TÜRKİYE CUMHURİYETİ
MİLLÎ SAVUNMA BAKANLIĞI

SAVUNMA SANAYİİ GÜVENLİĞİ YÖNERGESİ

UYGULAMA TALİMATI

Millî Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi güncellenerek yayımlanmıştır.

Bu Yönerge yayımı tarihinden itibaren yürürlüğe girecektir.

Bu Yönerge hükümlerini uygulamaktan ve işlem yapmaktan sorumlu makamlar, Yönerge'ye Bakanlık İç Ağından ve İnternet üzerinden ulaşabileceklerdir.

Savunma Sanayii Güvenliği faaliyetlerinde bu Yönerge kullanılacaktır. Bu kapsamda yürütülecek çalışma ve faaliyetlerle ilgili olarak uluslararası anlaşmalardan kaynaklanan yükümlülükler ve ilgili üst normlar hariç olmak üzere diğer düzenleyici işlemler arasında uyuşmazlık bulunması durumunda öncelikle bu Yönergede belirtilen esas, yöntem ve kurallar uygulanacaktır.

Bu Yönerge hükümlerine aykırı davrananlar veya hükümlerin uygulanmasında ihmal ya da kusur gösterenler hakkında idari ve adli işlem yapılacaktır.

31/01/2023

imza

Hulusi AKAR
Bakan

DEĞİŞİKLİK KAYIT ÇİZELGESİ

DEĞİŞİKLİK OLURUNUN TARİHİ	DEĞİŞEN,EKLENEN,İPTAL EDİLEN MADDE/FIKRA/BENT/KÜÇÜK BENT	YÜRÜRLÜĞE GİRİŞ TARİHİ
31 Ocak 2023	“Kontrole Tâbi Liste Kapsamında Üretim Yapacak İşletmelerin Kuruluş İzni İşlemleri” başlıklı 4. bölümün “Kuruluş İzninin İptali veya Yeniden Düzenlenmesi” konulu 4. Maddesine “c” alt bendi eklenmiştir.	31.01.2023
	“Kişi Güvenlik Belgeleri” başlıklı 5. Bölümün “Kişi Güvenlik Belgesi Verilmeyecek Hâller” konulu 4.a.1 Maddesine “(7)” alt bendi eklenmiştir.	31.01.2023
	“Tesis Güvenlik Belgeleri” başlıklı 6. Bölümün “Tesis Güvenlik Belgesi için Aranan İstek ve Özellikler” konulu “3.ı.(13)” maddesi değiştirilmiş ve EK-T olarak “Savunma Sanayi Firmalarının Uzaktan Çalışma Siber Güvenlik Esasları” eklenmiştir.	31.01.2023
	“Kontrole Tâbi Malzemenin İhraci ve İthali” başlıklı 8. bölümün “İhracat veya yurt dışına çikarma” konulu 3. maddesinin “b.1” alt bendi ile “g” alt bendi değiştirilmiştir.	31.01.2023
	“Kontrole Tâbi Malzemenin İhraci ve İthali” başlıklı 8. bölümün “İthalat veya yurt içine sokma:” konulu 4. maddesinin “g” alt bendi değiştirilmiştir.	31.01.2023
	“Tesis Güvenlik Belgeleri” başlıklı 6.bölümün “Genel” konulu 1. maddesine “j” fıkrası ve j.(1), j.(2), j(3), j(4) alt bentleri eklenmiştir. “EK-J Tesis Güvenlik Belgesi Protokolü”nde yer alan 5. maddesinin “b” alt bendi, “ç” alt bendi ve “e” alt bendi değiştirilmiştir.	31.01.2023
	“Kontrole Tâbi Malzemenin Üretimi” başlıklı 7. bölümün “Genel” konulu 1. maddesine “e” fıkrası ve e.1”, “e.2”, “e.3” ve “e.4” alt bentleri eklenmiştir. “EK-N Üretim İzin Belgesi Protokolü”nde yer alan 5. maddenin “b” alt bendi, “c” alt bendi ve “d” alt bendi değiştirilmiştir.	31.01.2023

İÇİNDEKİLER

EKLER

EK-A	Tanımlar
EK-B	Kısaltmalar
EK-C	Kurye Yetkilendirme Formu
EK-Ç	Proje Güvenlik Talimatı
EK-D	Toplantı Katılım Formu
EK-E	Kuruluş İzni Başvuru Yazısı
EK-F	(İptal edilmiştir)
EK-G	(İptal edilmiştir)
EK-Ğ	Kişi Güvenlik Belgesi Başvuru Yazısı
EK-H	Beyanname
EK-I	(İptal edilmiştir)
EK-İ	Tesis Güvenlik Belgesi Başvuru Yazısı
EK-J	Tesis Güvenlik Belgesi Protokolü
EK-K	(İptal edilmiştir)
EK-L	Tesis Güvenlik Belgesi
EK-M	Üretim İzin Belgesi Başvuru Yazısı
EK-N	Üretim İzin Belgesi Protokolü
EK-O	Üretim İzin Belgesi
EK-Ö	(İptal edilmiştir)
EK-P	(İptal edilmiştir)
EK-R	Geçici İthal Belgesi
EK-S	Son Kullanıcı Belgesi
EK-Ş	Ziyaret Talep Formu
EK-T	Savunma Sanayi Firmalarının Uzaktan Çalışma Siber Güvenlik Esasları

BİRİNCİ BÖLÜM
GENEL ESASLAR

1. AMAÇ

Bu Yönergenin amacı;

a. 29 Haziran 2004 tarihli ve 5201 sayılı Harp Araç ve Gereçleri ile Silah, Mühimmat ve Patlayıcı Madde Üreten Sanayi Kuruluşlarının Denetimi Hakkında Kanun kapsamında üretim yapan veya yapacak olan kamu kurum ve kuruluşları ile gerçek kişilere ve özel hukuk tüzel kişilerine ait sanayi kuruluşlarının kurulması, işletilmesi, denetimi ve yükümlülükleri ile Kontrole Tâbi Liste kapsamındaki malzemelerin ithalat ve ihracat izin işlemlerini,

b. Savunma sanayii kapsamında yapılan andlaşmalarda yer verilen ve doğrudan satın alma, müşterek proje programlarına katılım, teşvik veya yatırım yolu ile tedarik edilecek veya savunma sanayii, teknoloji ve teçhizatı sahasında araştırma, geliştirme, imalat ve montaj yapan gerçek ve tüzel kişilerle bu konularda çalışan şahıslara ait her türlü gizlilik dereceli bilgi, belge, proje, malzeme ve hizmetlerin ve bunlarla ilgili yerlerin güvenliğinin ve korunmasının sağlanmasına ilişkin yapılacak işlemleri belirlemektir.

2. KAPSAM:

Bu Yönerge;

a. 5201 sayılı Kanun kapsamındaki her türlü harp araç ve gereçleri ile silah, mühimmat ve bunlara ait yedek parçalarla patlayıcı maddeleri ve bunlara ait teknolojileri üretmek üzere kurulan veya işletilen kamu kurum ve kuruluşları ile gerçek kişilere ve özel hukuk tüzel kişilerine ait kuruluşları ve bu kuruluşlardaki personeli,

b. Savunma sanayiine ait gizlilik dereceli her türlü andlaşma ile bilgi, belge, proje, malzeme veya hizmetlerin alımını, satımını, üretimini, araştırma ve geliştirmesini, muhafazasını ve depolanmasını yapacak veya yaptıracak bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişileri ve bunların faaliyet gösterecekleri tesisler ile 26 Haziran 2001 tarihli ve 4691 sayılı Teknoloji Geliştirme Bölgeleri Kanununa göre kurulan tesisleri kapsar.

3. TANIMLAR VE KISALTMALAR:

Bu Yönergede kullanılan tanımlar EK-A'da, kısaltmalar ise EK-B'dedir.

4. ESASLAR:

a. 5201 sayılı Kanun gereğince her yıl ocak ayında veya gerektiğinde yıl içerisinde, Savunma Sanayii Millî Güvenlik Makamı (Millî Savunma Bakanlığı adına Teknik Hizmetler Genel Müdürlüğü) tarafından Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Sanayi ve Ticaret Bakanlığı ve ihtiyaç duyulan kamu kurum ve kuruluşlarının görüşleri alınarak tespit edilen Kontrole Tâbi Liste Resmî Gazetede yayımlanır. Ancak, herhangi bir nedenle Kontrole Tâbi Liste yayımlanmamışsa, en son yayımlanan liste esas alınır.

b. Kontrole Tâbi Listede yer alan malzemeyi üretecek kuruluşların kurulması ve işletilmesi için Savunma Sanayii Millî Güvenlik Makamına yapılan başvuruları müteakip, Savunma Sanayii Millî Güvenlik Makamınca Genelkurmay Başkanlığı, İçişleri Bakanlığı, Sağlık Bakanlığı, Çevre ve Orman Bakanlığı ve Sanayi ve Ticaret Bakanlığının görüşü alınır. Alınan görüşlerin uygun olması ve üretim yapılacak tesisin 2565 sayılı Askerî Yasak Bölgeler ve Güvenlik Bölgeleri Kanunu kapsamında yer almayan alanlarda bulunduğunun tespit edilmesi durumunda, üretim yapmayı talep eden kuruluşa, Kuruluş İzni verilir.

c. Kontrole Tâbi Listede yer alan malzemenin yurt içinde üretilebilmesi Savunma Sanayii Millî Güvenlik Makamının vereceği Üretim İznine bağlıdır.

ç. Üretim İzin Belgesi talep eden kuruluşların Kontrole Tâbi Listede yer alan malzemeyi üreteceği tesisler, Savunma Sanayii Millî Güvenlik Makamınca Üretim İzin Belgesi tanzim edilmeden önce veya eş zamanlı olarak 5202 sayılı Kanun kapsamında Tesis Güvenlik Belgesi, ilgili personeli ise Kişi Güvenlik Belgesi ile belgelendirilir.

d. 5202 sayılı Kanun kapsamında Tesis Güvenlik Belgesine sahip olan veya sahip olmayı talep eden kuruluşlar tarafından, faaliyette bulunulacak tesislerinde 10 Haziran 2004 tarihli ve 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun çerçevesinde gerekli fiziki güvenlik önlemleri alınır.

e. Kontrole Tâbi Listede yer alan malzemenin ihracatı ve ithalatı işlemlerinde, Savunma Sanayii Millî Güvenlik Makamından izin alınır.

f. Kontrole Tâbi Listede yer alan malzemenin ithalat işlemlerinde Son Kullanıcı Belgesi talep edilmesi durumunda, Son kullanıcı Belgesi Savunma Sanayii Millî Güvenlik Makamı tarafından onaylanır.

g. Kontrole Tâbi Listede yer alan malzemeyi üretmeyi ve/veya savunma sanayii konusunda hizmet vermeyi talep eden kuruluşların faaliyette bulunacağı tesisler, 5202 sayılı Kanun kapsamında Tesis Güvenlik Belgesi ile, bu kuruluşların gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz etmesi öngörülen personeli ise Kişi Güvenlik Belgesi ile belgelendirilir.

ğ. Kontrole Tâbi Listede yer alan malzemenin tedarik faaliyetlerinde ve savunma sanayii konusunda yürütülen gizlilik dereceli projelerde, istekli kişi ve kuruluşlara gizlilik dereceli bilgi, belge veya malzeme açıklanmadan veya verilmeden önce, bu kişi ve kuruluşlardan 5202 sayılı Kanun kapsamında tanzim edilmiş uygun gizlilik dereceli Tesis Güvenlik Belgesi ve Kişi Güvenlik Belgesi talep edilir. İstekli kişilerin Türkiye Cumhuriyeti vatandaşı olmaması veya kuruluşların Türkiye Cumhuriyeti sınırları içerisinde kurulmuş olmaması durumunda, bu kişi ve kuruluşlardan kendi ülkelerinin yetkili makamlarınca tanzim edilmiş Tesis Güvenlik Belgesi veya muadili belgeler istenir.

h. Savunma sanayii ile ilgili bilgi, belge, malzeme ve projeye, bu Yönergenin EK-A'sında tanımlanan gizlilik derecelerinden uygun olan gizlilik derecesi verilir. Bu gizlilik dereceleri ile sınıflandırılmasına ihtiyaç duyulmayan bilgi, belge, malzeme ve proje TASNİF DIŞI olarak adlandırılır ve işaretlenir. TASNİF DIŞI olarak nitelendirilen bilgi, belge, malzeme veya projenin, savunma sanayii güvenliği ile ilgili mevzuatta belirlenen usul ve esaslar çerçevesinde korunması gerekmez; bu tür bilgi, belge, malzeme ya da projeye erişim için güvenlik belgesi talep edilmez.

ı. Savunma sanayii ile ilgili bilgi, belge ve malzemeye gizlilik derecesi verilmesi ve verilen gizlilik derecesinin değiştirilmesi veya iptal edilmesi, bilgi, belge ve malzemeyi üreten veya bunlara sahip olan kişi, kurum veya kuruluşun yetki ve sorumluluğundadır. Savunma sanayii projelerinde gizlilik derecesi verilmesi ve verilen gizlilik derecesinin değiştirilmesi veya iptal edilmesi ise Proje Makamının yetki ve sorumluluğundadır.

i. Savunma sanayii ile ilgili projenin gizlilik derecesinin ÖZEL veya daha yukarı seviyede belirlenmesi durumunda, Proje Makamı koordinatörlüğünde ilgili makamların katılımıyla, savunma sanayii güvenliği mevzuatı kapsamında alınacak güvenlik önlemleri ile uygulamaya yönelik esasların yer aldığı Proje Güvenlik Talimatı oluşturulur. Proje Makamı koordinatörlüğünde hazırlanan Proje Güvenlik Talimatı, Savunma Sanayii Millî Güvenlik Makamı tarafından onaylanmasını müteakip yürürlüğe girer.

j. Tesis Güvenlik Belgesi ile belgelendirilen ve gizlilik dereceli proje yürütülen veya gizlilik dereceli bilgi, belge veya malzeme bulundurulan tesislere, yerli veya yabancı şahıslar tarafından gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz edilecek şekilde yapılacak ziyaretler, ziyaret tarihinden 21 iş günü öncesinden Savunma Sanayii Millî Güvenlik Makamından izin alınarak gerçekleştirilir ve ziyaretin tamamlanmasını müteakip Savunma Sanayii Millî Güvenlik Makamına bilgi verilir.

k. Savunma sanayii güvenliğinin sağlanmasına yönelik olarak ihtiyaç duyulabilecek ikili veya çok taraflı uluslararası güvenlik andlaşması akdedilme çalışmaları, uluslararası andlaşmaların akdedilmesi ile ilgili mevzuat çerçevesinde yürütülür, andlaşmanın yürürlüğe girmesini müteakip uygulama direktifi hazırlanarak ilgili makam ve kuruluşlara yayımlanır.

l. Tesis Güvenlik Belgesi bulunan tesislerde çalışacak yabancı uyruklu kişilerin kendi ülkelerinin yetkili makamlarından alınmış uygun gizlilik dereceli Kişi Güvenlik Belgeleri Savunma Sanayii Millî Güvenlik Makamına ibraz edilir. Savunma Sanayii Millî Güvenlik Makamınca, bu şahıslara ilişkin bilgiler, ilgili ülke yetkili makamları ile temas edilerek doğrulanabilir.

5. YETKİ, GÖREV VE SORUMLULUKLAR:

a. Savunma Sanayii Millî Güvenlik Makamı, Millî Savunma Bakanlığı adına Teknik Hizmetler Genel Müdürlüğüdür.

b. 5201 sayılı Kanun gereğince her yıl Ocak ayında veya gerektiğinde yıl içerisinde Resmî Gazetede yayımlanan Kontrole Tâbi Listede yer alan malzemenin ihracat ve ithalatı için gerekli izinlerin verilmesi ve Son Kullanıcı Belgesi onay işlemleri konusunda Savunma Sanayii Millî Güvenlik Makamı yetkilidir.

c. 5202 sayılı Kanun kapsamındaki Millî ve NATO gizlilik dereceli Kişi Güvenlik Belgesi, Millî gizlilik dereceli Tesis Güvenlik Belgesi ve 5201 sayılı Kanun kapsamındaki Üretim İzin Belgesi düzenlenmesine ilişkin faaliyetlerde Savunma Sanayii Millî Güvenlik Makamı yetkilidir. Anılan belgelerden Kişi Güvenlik Belgesi Savunma Sanayii Millî Güvenlik Makamınca, Tesis Güvenlik Belgesi Millî Savunma Bakanlığı Müsteşar Teknoloji ve Koordinasyon Yardımcısınca, Üretim İzin Belgesi ise Millî Savunma Bakanının onayını müteakip Millî Savunma Bakanlığı Müsteşar Teknoloji ve Koordinasyon Yardımcısınca imzalanır.

ç. 5202 sayılı Kanun kapsamındaki NATO gizlilik dereceli Tesis Güvenlik Belgesi başvuru işlemleri ile denetim ve raporlama faaliyetlerinden Savunma Sanayii Millî Güvenlik Makamı, tanzim edilmesi konusunda ise, Kuzey Atlantik Antlaşması Teşkilatı Merkez Kurulu Başkanlığı yetkilidir.

d. 5201 ve 5202 sayılı Kanunlar kapsamında yer alan faaliyetlerin gerçekleştirilebilmesi için; Savunma Sanayii Millî Güvenlik Makamı, İhtiyaç Makamı, Proje Makamı, Kuruluş, Kuruluş Güvenlik Koordinatörü ve görev üstlenebilecek diğer kuruluş personeli tarafından yapılacak işlemler, bu Yönergede belirtilen hususlar çerçevesinde yürütülür. Bunların görev ve sorumlulukları müteakip maddelerde belirtilmiştir.

6. SAVUNMA SANAYİİ MİLLÎ GÜVENLİK MAKAMININ GÖREV VE SORUMLULUKLARI:

a. 5201 sayılı Kanun gereğince her yıl Resmî Gazetede yayımlanan Kontrole Tâbi Liste hakkında ilgili makamlarla koordineyi müteakip gerekli tetkiki yapmak, hazırlanan listenin Resmî Gazetede yayımlanmasını sağlamak.

b. 5201 sayılı Kanun kapsamında faaliyet gösteren veya göstermek isteyen kuruluşların, Kontrole Tâbi Listede yer alan malzemeyi üretmek üzere kurulmalarına yönelik yapacakları talepleri ilgili makamlarla koordineli olarak incelemek, uygun bulunanlara Kuruluş İzni verilmesini sağlamak.

c. Tesis Güvenlik Belgesi ile belgelendirilen ve gizlilik dereceli proje yürütülen veya gizlilik dereceli bilgi, belge veya malzeme bulundurulan tesislere, yerli veya yabancı şahıslar tarafından gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz edilecek şekilde yapılacak ziyaretler, ziyaret tarihinden 21 iş günü öncesinden Savunma Sanayii Millî Güvenlik Makamından izin alınarak gerçekleştirilir ve ziyaretin tamamlanmasını müteakip Savunma Sanayii Millî Güvenlik Makamına bilgi verilir.

ç. Savunma sanayii güvenliğinin sağlanmasına yönelik olarak ihtiyaç duyulabilecek ikili veya çok taraflı uluslararası güvenlik andlaşması akdedilme çalışmaları, uluslararası andlaşmaların akdedilmesi ile ilgili mevzuat çerçevesinde yürütülür, andlaşmanın yürürlüğe girmesini müteakip uygulama direktifi hazırlanarak ilgili makam ve kuruluşlara yayımlanır.

d. Tesis Güvenlik Belgesi bulunan tesislerde çalışacak yabancı uyruklu kişilerin kendi ülkelerinin yetkili makamlarından alınmış uygun gizlilik dereceli Kişi Güvenlik Belgeleri Savunma Sanayii Millî Güvenlik Makamına ibraz edilir. Savunma Sanayii Millî Güvenlik Makamınca, bu şahıslara ilişkin bilgiler, ilgili ülke yetkili makamları ile temas edilerek doğrulanabilir.

e. İhracat ve ithalat işlemlerinin gerçekleştirilebilmesi için gerekli olan Son Kullanıcı Belgesi işlemlerini takip etmek, Kontrole Tâbi Listede yer alan malzemeleri ithal etmek isteyen kuruluşların talep edebilecekleri Son Kullanıcı Belgelerinin incelenmesini müteakip uygun bulunanları onaylamak.

f. Türkiye'nin taraf olduğu uluslararası ihracat kontrol rejimleri çerçevesinde düzenlenen toplantılar için gerekli hazırlıkları yapmak, ilgili makamlarla koordineyi müteakip görüş oluşturmak ve gerektiğinde söz konusu toplantılarda Millî Savunma Bakanlığını temsiletmek.

g. Türkiye'nin taraf olduğu ve Millî Savunma Bakanlığınca takip edilen uluslararası ihracat kontrol rejimleri ve savunma sanayii konusunda üye olunan uluslararası organizasyonların yürüttüğü faaliyetler ve gelişmelere yönelik olarak ilgili makamları bilgilendirmek.

ğ. Savunma sanayii güvenliği konusunda yürürlükte bulunan mevzuat çerçevesinde, alınan güvenlik tedbirlerini gözden geçirmek ve ihtiyaç duyulması hâlinde ilgili makamlarla koordine ederek gerekli mevzuat değişikliklerini hazırlamak, güncellenen mevzuat doğrultusunda güvenlik standartlarını oluşturmak ve bunlar hakkında ilgili tarafları bilgilendirmek amacıyla brifingler vermek, toplantı ve konferanslar düzenlemek.

h. 5202 sayılı Kanun kapsamındaki Millî gizlilik dereceli belgelendirme başvuruları ile Kuzey Atlantik Andlaşması Teşkilâtı Merkez Kurulu Başkanlığının yaptığı yetki devri çerçevesinde, NATO gizlilik dereceli belgelendirme başvurularını kabul etmek, anılan talep kapsamında başvuru evraklarını inceleyerek eksiklikleri tamamlatmak.

ı. Millî/NATO gizlilik dereceli Kişi Güvenlik Belgesi talep edilen personel hakkında Millî İstihbarat Teşkilâtı Müsteşarlığı, Emniyet Genel Müdürlüğü veya mahallî mülkî idare amirlikleri vasıtasıyla, güvenlik soruşturması ve arşiv araştırması yaptırmak.

i. Güvenlik soruşturması ve arşiv araştırması sonucunda, personel hakkında belgelendirmeye engel teşkil edebileceği değerlendirilen tereddütlü hususlara ilişkin, Millî Savunma Bakanlığı Hukuk Müşavirliği ve Davalar Dairesi Başkanlığından hukukî mütalaa almak.

j. Güvenlik soruşturması, arşiv araştırması ve inceleme sonucunun uygun olması durumunda, Millî/NATO gizlilik dereceli Kişi Güvenlik Belgesi talep edilen personele

geçerlilik süresi de belirlenerek uygun gizlilik dereceli Kişi Güvenlik Belgesi tanzimetmek.

k. Kuruluşlarca yapılan Millî/NATO gizlilik dereceli Tesis Güvenlik Belgesi taleplerinin ve başvuru evraklarının mevzuat açısından ön incelemesini yapmak, belirlenen eksiklikleri tamamlatmak, bu eksiklikleri üç ay içinde tamamlamayan kuruluşların başvuru evraklarını iade ederek, talebini iptal etmek.

l. Başvuru belgelerini tamamlayan kuruluşlara ait tesislerin Denetim Heyeti vasıtasıyla denetlenmesini sağlayarak, uygun bulunan kuruluşlara talep edilen gizlilik derecesi de göz önünde bulundurularak, uygun Millî gizlilik dereceli Tesis Güvenlik Belgesini tanzim etmek ve Tesis Özel Güvenlik El Kitabını onaylamak, uygun NATO gizlilik dereceli Tesis Güvenlik Belgesinin tanzimi maksadıyla Kuzey Atlantik Andlaşması Teşkilâtı Merkez Kurulu Başkanlığını bilgilendirmek, belge verilen kuruluşlara ait Tesis Özel Güvenlik El Kitabını onaylamak.

m. Kuruluşlara ait tesislerde, yılda en az bir defa haberli veya habersiz denetim yapmak, bu denetimlere ilişkin denetim kriterlerini belirlemek, güncellemek ve alınması gereken ilâve güvenlik önlemlerini tespit etmek.

n. Türkiye Cumhuriyeti vatandaşlarının veya yabancı kişilerin, Millî/NATO gizlilik dereceli Tesis Güvenlik Belgesine sahip kuruluşlara ait tesislere yapacakları ziyaret taleplerini incelemek, ilgili makamlarla koordine etmek ve uygun bulunanlara izin vermek.

o. Millî/NATO gizlilik dereceli Kişi Güvenlik Belgesine sahip olan şahısların, diğer ülkelerin savunma sanayi kuruluşlarına yapacakları ziyarete ilişkin taleplerini ilgili ülkedeki askerî ataşelik vasıtasıyla, o ülkedeki yetkili makamlar ile koordine etmek, sonuçları talep sahibine bildirmek.

ö. Yerli ve yabancı basın organlarının, Tesis Güvenlik Belgesine sahip savunma sanayii kuruluşlarına ait tesislerde röportaj, program ve çekim yapma talepleri ile Kontrole Tâbi Listede yer alan malzeme ve teçhizat ile ilgili bilgilerin yayım organlarında yayınlanması hususunu ilgili makamlarla koordine ederek incelemek, uygun bulunanlara izin vermek.

p. Millî/NATO gizlilik dereceli Tesis Güvenlik Belgesine sahip kuruluş tarafından kabul edilen stajyer personel listesi esas alınarak, stajyerlerin gizlilik dereceli bilgi, belge veya malzemeye ulaşmasını engellemek için gerekli önlemlerin alınıp alınmadığını gerektiğinde yapılacak denetimlerde kontrol etmek.

r. Savunma sanayii güvenliğinin sağlanmasına yönelik olarak ihtiyaç duyulabilecek ikili veya çok taraflı uluslararası güvenlik andlaşması akdedilme çalışmalarını yürütmek ve andlaşmanın yürürlüğe girmesini müteakip uygulama esaslarını ilgili makam ve kuruluşlara yayımlamak.

s. ÖZEL veya üzeri gizlilik derecesine sahip savunma sanayii projelerinde güvenliğin sağlanması amacıyla hazırlanan projeye özgü Proje Güvenlik Talimatını, savunma sanayii güvenliği ile ilgili mevzuat kapsamında incelemek, uygun bulunanları onaylamak.

ş. Gizlilik dereceli bilgi, belge ve malzemenin taşıma planlarını savunma sanayii güvenliği ile ilgili mevzuat kapsamında incelemek, uygun bulunanları onaylamak.

t. 5202 sayılı Kanun kapsamında NATO gizlilik dereceli belgelendirme taleplerini, Kuzey Atlantik Andlaşması Teşkilâtı Merkez Kurulu Başkanlığının yaptığı yetki devri çerçevesinde, ilgili makamlar ile koordineli olarak incelemek, inceleme sonuçlarını belge tanzim edecek yetkili makam olan Kuzey Atlantik Andlaşması Teşkilâtı Merkez Kurulu Başkanlığına göndermek.

u. Verilen belgelerin usulüne uygun olarak kullanılması, belgenin veriliş koşullarının değişmesi hâlinde durumun yeniden incelenmesi ve değerlendirme sonucuna göre Millî gizlilik dereceli belgeyi iptal etmek, NATO gizlilik dereceli belgelerin iptali için sorumlu makam olan Kuzey Atlantik Andlaşması Teşkilâtı Merkez Kurulu Başkanlığına bilgi vermek.

ü. Gizlilik ihlalleri ile ilgili şikayetleri inceleyerek, yapılacak işlemleri belirlemek.

7. İHTİYAÇ MAKAMININ GÖREV VE SORUMLULUKLARI:

a. Tedarik faaliyeti sürecinde, savunma sanayii güvenliği ile ilgili işlemler hakkında Proje Makamı ve Savunma Sanayii Millî Güvenlik Makamı ile iş birliği içinde bulunmak.

b. Proje için özel güvenlik önlemleri uygulanması gerekli görüldüğü takdirde, bu hususu ilgili makamlara bildirmek.

c. Son Kullanıcı Belgesinde yer alan "End User-Son Kullanıcı" bölümünü onaylamak.

8. PROJE MAKAMININ GÖREV VE SORUMLULUKLARI:

a. Tedarik faaliyeti sürecinde, savunma sanayii güvenliği ile uygulamalar bakımından, Savunma Sanayii Millî Güvenlik Makamı ile iş birliği içinde bulunmak.

b. Proje için aranacak savunma sanayii güvenliği ile ilgili belge ve bilgileri belirlemek, bunları proje dokümanlarına yansıtmak.

c. Projede görev almak isteyen kişi ve kuruluşlara herhangi bir bilgi vermeden veya açıklamadan önce, bu kişi veya kuruluşların uygun gizlilik dereceli Kişi Güvenlik Belgesine ve/veya Tesis Güvenlik Belgesine sahip olup olmadıklarını kontrol etmek, projeyi gerçekleştirmek amacıyla kullanılacak tesisin/tesislerin, uygun gizlilik dereceli Tesis Güvenlik Belgesi olup olmadığını araştırmak.

ç. Projede görev üstlenebilecek kuruluşlardan, görevleri gereği gizlilik dereceli bilgi, belge veya malzemeye nüfuz etmeleri gerekecek personel için Kişi Güvenlik Belgesi temin edilmesini istemek veya Savunma Sanayii Millî Güvenlik Makamından, bu kişilerin durumunun araştırılması hususunda talepte bulunmak.

d. Savunma Sanayii Millî Güvenlik Makamı ile koordine ederek, sözleşme ve/veya protokollere, savunma sanayii güvenliği uygulamalarını düzenleyen hükümlerkoymak.

e. Kontrole Tâbi Listede yer alan ve en az ÖZEL veya üzeri gizlilik derecesine haiz projelerin yürütülmesi sırasında alınması gerekli tüm güvenlik tedbirlerini içeren Proje Güvenlik Talimatının hazırlanması çalışmalarını koordine etmek, hazırlanan dokümanın Savunma Sanayii Millî Güvenlik Makamı tarafından onaylanmasını ve onayı müteakip ilgili makam ve kuruluşlara dağıtılmasını sağlamak.

f. Yürütülen/yürütülecek projelerin gizlilik derecesini belirlemek, değiştirmek veya ihtiyaç kalmadığı durumlarda gizlilik derecesini kaldırmak.

g. Sözleşmeye bağlanmış projelerde yurt dışından ithal edilecek malzemeler ile Son Kullanıcı Belgesi onay taleplerini değerlendirmek, uygun bulunanları Savunma Sanayii Millî Güvenlik Makamı onayına göndermek.

9. KURULUŞLARIN GÖREV VE SORUMLULUKLARI:

a. Bu Yönergede belirtilen esas ve usuller çerçevesinde hareket ederek, Tesis Güvenlik Belgesi ve Kontrole Tâbi Liste kapsamında üretim yapılacaksa Üretim İzin Belgesi almak üzere başvuruda bulunmak.

b. Savunma Sanayii Millî Güvenlik Makamınca istenebilecek bilgi, belge, form ve taahhütnameleri usulüne uygun olarak düzenlemek.

c. Savunma sanayii ile ilgili yürütülecek gizlilik dereceli projelerde gizlilik dereceli bilgi, belge veya malzemenin ana yüklenici veya alt yüklenici olan diğer bir kuruluşla paylaşılması durumunda; bilgi, belge ve/veya malzeme paylaşılacak kuruluşun uygun gizlilik dereceli Tesis Güvenlik Belgesine sahip olması şartını aramak.

ç. Kontrole Tâbi Liste kapsamında üretim yapılması sürecinde, üretimi yapılan malzemenin bir kısmının yurt içinde yerleşik başka bir kuruluştan tedarik edilmesi ve tedarik edilecek kısmın da Kontrole Tâbi Listede yer alması durumunda; malzemenin tedarik edileceği kuruluşun uygun Üretim İzin Belgesine sahip olması şartını aramak.

d. Kontrole Tâbi Listede yer alan malzemeyi üretmek amacıyla kurulması planlanan tesislerinin kurulmasına ilişkin olarak Savunma Sanayii Millî Güvenlik Makamından Kuruluş İzni talep etmek.

e. Kontrole Tâbi Listede yer alan malzemenin ihracat ve ithalat işlemlerinde Savunma Sanayi Millî Güvenlik Makamından ihracat izni ve/veya ithalat izni almak.

f. Kontrole Tâbi Liste kapsamında üretecekleri maddelerin cinsleri ile senelik üretim miktarlarını Savunma Sanayii Millî Güvenlik Makamına bildirmek.

g. İmal ettikleri harp araç ve gereçleri, silâh, mühimmat ve patlayıcı madde cinsleri ile stoklarını ve üretim tesislerinde kendi denetim ve sorumlulukları altında imâl edecekleri veya üçüncü şahıslara imâl ettirecekleri Kontrole Tâbi Liste kapsamındaki malzemeleri her yıl ocak ayı içerisinde Savunma Sanayii Millî Güvenlik Makamına bildirmek.

ğ. Kontrole Tâbi Liste kapsamında aldıkları siparişlerin cins ve miktarları ile sipariş verenlerin kimliklerini bir ay içerisinde Savunma Sanayii Millî Güvenlik Makamına bildirmek.

h. Tesis Güvenlik Belgesi talep edilen tesisinde, 10 Haziran 2004 tarihli ve 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun ile bu Kanun gereğince Resmî Gazetede yayımlanan Özel Güvenlik Hizmetlerine Dair Kanunun Uygulanmasına İlişkin Yönetmelikte yer alan hükümlere göre gerekli fizikî koruma önlemlerini ve İçişleri Bakanlığınca istenebilecek diğer tedbirleri almak.

ı. Tesis Güvenlik Belgesi talep edilen tesisinde uygulamaya konulmak üzere, tesise özgü Olağanüstü Hâl Planı ve Sabotaja Karşı Koyma Planı hazırlamak, tesiste meydana gelebilecek herhangi bir güvenlik ihlâlini, sabotajı veya olağanüstü hâli Savunma Sanayii Millî Güvenlik Makamına bildirmek.

i. Tesis Güvenlik Belgesi düzenlenmesi için başvuruda bulunulan tesisinde, gizlilik dereceli bilgi, belge ve malzemenin saklanması ve depolanması maksadıyla Savunma Sanayii Millî Güvenlik Makamınca belirlenen kriterleri sağlayacak şekilde Kontrollü Oda oluşturmak.

j. Tesis Güvenlik Belgesi düzenlenmesi için başvuruda bulunulan tesisinde, gizlilik dereceli proje çalışmalarının yürütüleceği veya Kontrole Tâbi Listede yer alan malzemenin üretileceği alanları Savunma Sanayii Millî Güvenlik Makamınca belirlenen kriterleri sağlayacak şekilde Kontrollü Bölge hâline getirmek.

k. Gizlilik dereceli projelere ilişkin imzalanan sözleşmelerde yer alan güvenlikle ilgili hükümler ile Tesis Güvenlik Belgesi ve Üretim İzin Belgesi alınması sırasında yapılan protokollerde belirtilen hükümlere uygun hareket etmek.

l. Tesis Güvenlik Belgesi talep edilen tesisinde savunma sanayi güvenliğinin sağlanması amacıyla, fiziki güvenlik, yangın güvenliği, evrak, doküman ve malzeme güvenliği, bilgi güvenliği, personel güvenliği, kurye hizmetleri, Kontrollü Oda, Kontrollü Bölge vb. güvenlikle ilgili tüm hususlardan sorumlu kişi ve birimlerden oluşan güvenlik organizasyonu oluşturmak ve görevlendirmeleri yapmak.

m. Tesis Güvenlik Belgesi ile belgelendirilen veya belgelendirilmesi talep edilen tesisinde savunma sanayii güvenliği ile ilgili uygulamaları yürütmek üzere oluşturulan güvenlik organizasyonunu koordine edecek bir Kuruluş Güvenlik Koordinatörü görevlendirmek.

n. Tesis Güvenlik Belgesi ile belgelendirilen veya belgelendirilmesi talep edilen tesisin savunma sanayii güvenliği ile ilgili uygulamalarının açıklandığı Tesis Özel Güvenlik El Kitabını hazırlamak, Savunma Sanayii Millî Güvenlik Makamınca onaylanmasını müteakip, Tesis Özel Güvenlik El Kitabında belirtilenleri uygulamak.

o. Tesis Güvenlik Belgesi ile belgelendirilen veya belgelendirilmesi talep edilen tesisinde, Savunma Sanayii Millî Güvenlik Makamının belirlediği ilâve güvenlik önlemlerini almak ve geliştirmek.

ö. Gizlilik dereceli proje yürütülen/yürütülecek veya gizlilik dereceli bilgi, belge ve/veya malzeme bulundurulan/bulundurulacak tesisinde, gerek Tesis Güvenlik Belgesi verilmesi amacıyla yapılan gerekse Tesis Güvenlik Belgesi ile belgelendirilmesini müteakip yapılan ara denetimlerde tespit edilen güvenlik zafiyetlerini giderici önlemleri almak.

p. Gizlilik dereceli bilgi, belge, malzeme ve projelere nüfuz edebilecek yönetim kurulu başkanı ve üyeleri, genel müdür ve genel müdür yardımcıları ile diğer üst düzey yöneticileri, kuruluş hissedarları (hissedarın tüzel kişilik olması hâlinde tüzel kişiliğin temsilcisi/temsilcileri), bilgi işlem merkezinde çalışacak personel, gelen-giden evrak bölümünde çalışacak personel, kurye ve gizlilik dereceli bilgiye ulaşabilecek diğer personeli için Kişi Güvenlik Belgesi başvurusu yapmak.

r. Tesis Güvenlik Belgesi ile belgelendirilen tesisin sahibi olan kuruluşun adı tüzel kişiliği veya hisse yapısı, yönetim kurulu başkanı veya üyelerinden herhangi birinin değişmesi durumunda, değişikliği içerecek şekilde Savunma Sanayii Millî Güvenlik Makamına bilgi vermek.

s. Tesisinde bulunan gizlilik dereceli bilgi, belge veya malzemeye ya da yürütülen gizlilik dereceli projeye, Kişi Güvenlik Belgesine sahip olup Bilmesi Gereken Kişiler dışındaki diğer şahıslar tarafından nüfuz edilmesini engellemek.

ş. Tesisinde görevli olup Kişi Güvenlik Belgesi ile belgelendirilmiş personeli ile ilgili değişiklikleri Savunma Sanayii Millî Güvenlik Makamına bildirmek.

t. Kişi Güvenlik Belgesi ile belgelendirilen personeli için altı ayda bir adli sicil takibi yapmak, personel ile ilgili kayıtları tutmak, adli sicil kaydına rastlanan personelinin durumunu Savunma Sanayi Millî Güvenlik Makamına bildirmek.

u. Tesisinde görevli olup Kişi Güvenlik Belgesi ile belgelendirilmiş personelinin işten ayrılması durumunda, zaman gözetmeksizin personelin sahip olduğu Kişi Güvenlik Belgesini Savunma Sanayii Millî Güvenlik Makamına iade etmek.

ü. Kendisine verilen gizlilik dereceli bilgi, belge ve malzemenin, tesisinde bulunduğu sürece savunma sanayii güvenliği ile ilgili mevzuat çerçevesinde korunmasını sağlamak, projenin tamamlanması veya sözleşmenin herhangi bir nedenle feshedilmesi durumunda dahi, kendisine verilmiş veya proje kapsamında üretilmiş gizlilik dereceli bilgi, belge ve malzemeyi gerektiği şekilde korumak veya usulüne uygun olarak imha edip kayıt altına almak.

v. Savunma Sanayii Millî Güvenlik Makamı veya Proje Makamınca verilebilecek bilgi, belge veya malzemenin üçüncü şahıslara verilmesi veya güvenlik önlemlerinin yetersizliği nedeniyle oluşabilecek mağduriyetleri tazmin etmeyi kabul etmek.

y. Gizlilik dereceli bilgi, belge ve/veya malzemenin gerekli güvenlik önlemleri alınarak taşınması için taşıma planı hazırlamak, hazırlanan taşıma planını onaylanmak üzere Savunma Sanayii Millî Güvenlik Makamına göndermek, taşıma işleminin, onaylanan taşıma planına uygun olarak yapılmasını sağlamak.

z. Tesis Güvenlik Belgesi ile belgelendirilen tesisinde yürütülecek savunma sanayii ile ilgili projelere ilişkin olarak, projeye ait sözleşmenin imzalanmasını müteakip, projenin adı, gizlilik derecesi, proje yürütücüleri listesi ve projenin tahmini tamamlanma süresine ilişkin bilgileri Savunma Sanayii Millî Güvenlik Makamına göndermek.

aa. Görev alacağı savunma sanayii ile ilgili gizlilik dereceli projeler için Proje Makamı koordinatörlüğünde hazırlanacak Proje Güvenlik Talimatı hazırlama çalışmalarına katılmak.

bb. Türk Silahlı Kuvvetlerinin ihtiyacının karşılanmasına yönelik olmayıp, savunma sanayii ile ilgili konularda kuruluşun sahip olduğu kabiliyetlerin geliştirilmesi amacıyla yerli ve/veya yabancı kuruluşlarla iş birliği yapılacak olması ve bu iş birliği kapsamında gizlilik dereceli bilgi, belge veya malzemenin paylaşılacak olması durumunda, ilgili kuruluşların katılımıyla Proje Güvenlik Talimatı hazırlamak, hazırlanan Proje Güvenlik Talimatını onaylanmak üzere Savunma Sanayii Millî Güvenlik Makamına göndermek ve iş birliği sürecinde, Savunma Sanayii Millî Güvenlik Makamınca onaylanan Proje Güvenlik Talimatında yer alan hususlara uymak.

cc. Tesis Güvenlik Belgesi ile belgelendirilen tesisine, yerli veya yabancı şahıslar tarafından gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz edilecek şekilde gerçekleştirilecek ziyaretler için, ziyaret tarihinden 21 iş günü öncesinden Savunma Sanayii Millî Güvenlik Makamından izin almak/ izin alınmasını sağlamak ve ziyaretin gerçekleşmesini müteakip Savunma Sanayii Millî Güvenlik Makamına bilgi vermek.

çç. Tesis Güvenlik Belgesi ile belgelendirilen tesisine, yabancı şahıslar tarafından gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz edilmeyecek şekilde yapılacak ziyaretlerde Savunma Sanayii Millî Güvenlik Makamına bilgi vermek.

dd. Sözleşmeye bağlanmış projelerde ihtiyaç duyulacak parça ve malzemelerin ithalat izin talepleri ile Son Kullanıcı Belgesi onay işlemlerini, Proje Makamı vasıtasıyla Savunma Sanayii Millî Güvenlik Makamına ulaştırmak.

10. KURULUŞ GÜVENLİK KOORDİNATÖRÜNÜN GÖREV VE SORUMLULUKLARI:

a. Tesiste, fiziki güvenlik önlemleri, yangın, sabotaj ve olağanüstü hal hizmetleri, toplantı odaları, Kontrollü Oda ve Kontrollü Bölge güvenliği, evrak/doküman ve malzeme güvenliği, bilgi güvenliği, personel güvenliği vb. savunma sanayii güvenliği ile ilgili konularda alınan ve uygulanan tedbirleri koordine etmek, bu tedbirlerin uygulanmasını sağlamak, iç denetim faaliyetleri icra ederek kayıt altına almak, tespit ettiği güvenlik ihlallerini kuruluş üst yönetimine rapor etmek ve Savunma Sanayii Millî Güvenlik Makamına bilgi vermek.

b. Tesisin güvenlik sisteminde görev yapan tüm personelin temel ve uygulamaya yönelik güvenlik eğitimleri ile tüm çalışanların güvenlik sistemine uygun olarak hareket etmesini sağlamaya yönelik eğitim ihtiyaçlarını belirlemek, eğitim programları hazırlamak, eğitimlerin alınmasını sağlamak, alınan tüm eğitimleri izlenebilir şekilde kayıt altına almak.

c. Kuruluş tarafından tesise özgü olarak hazırlanan ve Savunma Sanayii Millî Güvenlik Makamı tarafından onaylanarak yürürlüğe giren Tesis Özel Güvenlik El Kitabının uygulanmasını sağlamak, uygulamada karşılaşılan aksaklıkları tespit etmek ve revize edilen Tesis Özel Güvenlik El Kitabını onaylanmak üzere değişiklik teklifleri ile birlikte Savunma Sanayii Millî Güvenlik Makamına göndermek.

ç. Savunma sanayii güvenliği ile ilgili mevzuatı takip etmek, mevzuatta meydana gelebilecek değişikliklerin Tesis Güvenlik Belgesine sahip tesiste uygulanmasını sağlamak.

d. Tesis Güvenlik Belgesi ile belgelendirilen tesiste yürütülen gizlilik dereceli proje çalışmalarına ve toplantılara, uygun gizlilik dereceli Kişi Güvenlik Belgesi bulunmayan şahısların katılmasını önlemek, toplantıya katılanların kayıtlarını tutmak, gerekli kontrolleri yapmak veya yapılmasını sağlamak.

e. Personelin sahip olduğu Kişi Güvenlik Belgesinin geçerlilik süresini takip etmek, yenilenmesi gerekiyorsa geçerlilik süresinin bitiminden altı ay öncesinde ilgili evraklarla birlikte Savunma Sanayii Millî Güvenlik Makamına başvuruda bulunulmasını sağlamak.

f. Tesisin sahip olduğu Tesis Güvenlik Belgesinin geçerlilik süresini takip etmek, yenilenmesi gerekiyorsa geçerlilik süresinin bitiminden altı ay öncesinde ilgili evraklarla birlikte Savunma Sanayii Millî Güvenlik Makamına başvuruda bulunulmasını sağlamak.

g. Tesis Güvenlik Belgesi ile belgelendirilen tesiste savunma sanayii güvenliğinin sağlanması amacıyla oluşturulan güvenlik organizasyonunda yer alan kişi ve birimler için görev talimatları hazırlamak, bu talimatların güncel olarak muhafaza edilmesini sağlamak, uygulamaları takip ve koordine etmek.

ğ. Belirli dönemlerde senaryolu alarm ve tatbikatlar yapılmasını sağlamak, tesisteki güvenlik sisteminin ve personelin reaksiyon durumunun istenilen düzeyde olup olmadığını kontrol etmek, yapılan tatbikatların izlenebilir şekilde kayıt altına alınmasını sağlamak.

h. Kuruluş bünyesinde çalışıp gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz etmesi öngörülen personel için Kişi Güvenlik Belgesi tanzim edilmesi maksadıyla Savunma Sanayii Millî Güvenlik Makamına başvuruda bulunulmasını sağlamak.

ı. Kişi Güvenlik Belgesi ile belgelendirilmiş personele altı ayda bir güvenlik brifingi vermek, verilen brifinglerin kaydını tutmak.

i. Kişi Güvenlik Belgesi ile belgelendirilen personel için altı aylık dönemlerde adli sicil takibi yaptırılmasını, adli sicili uygun olanların kayıtlarının personel dosyalarında muhafaza edilmesini, adli sicili uygun olmayan personelin durumunun ise Savunma Sanayii Millî Güvenlik Makamına bildirilmesini sağlamak.

j. Tesis Güvenlik Belgesi ile belgelendirilen tesise yerli veya yabancı şahıslar tarafından yapılacak ziyaretler için gerekli izinlerin alınmasını, gerçekleşen ziyaretlere ilişkin kayıtların tutulmasını ve ziyaretin gerçekleşmesini müteakip Savunma Sanayii Millî Güvenlik Makamına bilgi verilmesini sağlamak.

k. Tesis Güvenlik Belgesi ile belgelendirilen tesisle ilgili olarak, basın ve yayın organlarında yer alacak bilgi ve belgelerin verilmesi öncesinde Savunma Sanayii Millî Güvenlik Makamından izin alınmasını sağlamak.

11.SAVUNMA SANAYİİNDE GÖREVLİ PERSONELİN GÖREV VE SORUMLULUKLARI:

a. Bu Yönergede belirtilen bütün tanımları, hüküm, şartları ve açıklamaları aynen kabul etmek ve bunların Savunma Sanayii Millî Güvenlik Makamınca değiştirilmiş şekillerini duyuru tarihinden itibaren uygulamak.

b. Kendisine verilen gizlilik dereceli bilgi, belge ve malzemeyi veya görevin gerektirdiği bir planı, açıklamadan veya aktarmadan önce gerekli inceleme ve kontrolleri yapmak, önlem ve onayları almak.

c. Uygun gizlilik dereceli Kişi Güvenlik Belgesi bulunmayan veya Bilmesi Gereken Kişi dışındaki şahısların gizlilik dereceli bilgi, belge ve malzemeye ulaşmasını önlemek.

ç. Şahit olduğu güvenlik ihlalleri hakkında ilgilileri bilgilendirmek.

İKİNCİ BÖLÜM
BİLGİ, BELGE VE MALZEME GÜVENLİĞİ

1. GENEL:

a. Savunma sanayii ile ilgili gizlilik dereceli bilgi, belge veya malzemenin işaretlenmesi, kayıt, çoğaltım ve tercümesi, üçüncü kişi ve kuruluşlara aktarılması, açıklanması, taşınması ve imhası işlemleri, bu yönergede belirtilen esas ve usuller çerçevesinde, gizlilik seviyesine uygun güvenlik tedbirleri alınarak yapılır.

b. Projeye ilişkin gizlilik dereceli herhangi bir bilginin yükleniciye açıklanması proje makamının sorumluluğundadır. Savunma sanayii kuruluşlarınca gizlilik dereceli bir bilginin kamuya açıklanması ise, Millî Savunma Bakanlığınca ilgili makamlarla yapılacak koordinasyon sonrasında verilecek izne bağlıdır.

c. Savunma sanayii kuruluşları tarafından, gizlilik dereceli bilgi, belge veya malzemenin üçüncü kişi ve kuruluşlara aktarılması veya yurt içi/yurt dışı güzergâhlarda taşınmasına ihtiyaç olması durumunda yapılacak işlem için proje makamı koordinesiyle Savunma Sanayii Millî Güvenlik Makamından onay alınır. GİZLİ gizlilik dereceli bilgi ve dokümanın yabancı ülke sanayisine aktarılması gerektiğinde alıcı ülkenin resmî muhatap makamına iletilmek üzere devletten devlete esasına göre işlem yapılır.

ç. Bir evraka veya dokümana gizlilik derecesi verme yetki ve sorumluluğu, o evrakı veya dokümanı çıkartan makama aittir.

d. Gizlilik derecesi, bir projenin sadece zorunlu kısımlarına uygulanır; ancak, projenin gizlilik derecesi, en yüksek gizlilik derecesine sahip kısmın gizlilik derecesi ile belirlendiğinden, yüklenici ile proje bilgilerinin tamamına ulaşabilecek diğer kişi ve kuruluşlar, bu seviyeye uygun gizlilik dereceli güvenlik belgelerine sahip kişiler arasından seçilir.

2. GİZLİLİK DERECESİNİN İŞARETLENMESİ:

a. Uluslararası andlaşma hükümleri saklı kalmak kaydıyla; savunma sanayii alanında yer alan bilginin, belgenin ve malzemenin gizlilik derecesi, bunları üreten/sahip olan kişi, kurum veya kuruluş tarafından, bu Yönergede tanımlanan gizlilik derecelerine uygun olarak belirlenir. Gizlilik derecesi bulunmayan evrak ve doküman üretilemez.

b. Savunma sanayii alanında yürütülen projelerin gizlilik derecesinin belirlenmesi Proje Makamının yetki ve sorumluluğundadır.

c. TASNİF DIŞI olarak adlandırılan veya işaretlenen bilgi, belge, malzeme ya da projenin, taraf olunan uluslararası andlaşma hükümleri saklı kalmak kaydıyla, savunma sanayii ile ilgili mevzuatta belirtilen esas ve usuller çerçevesinde korunması gerekmez; bu tür bilgi, belge, malzeme ya da projeye erişim için güvenlik belgesi talep edilmez.

ç. Gizlilik derecesini değiştirme yetkisi gizlilik derecesini veren makama aittir. Sınıflandırılmış bilgi, belge veya malzemenin gizlilik derecesini düşürme işlemi, sistemin aşırı yüklenmesini önlemek amacıyla, mümkün görülen hâllerde gizlilik derecesini veren Proje Makamına teklif edilir ve uygun görülmesi durumunda hemen yapılır.

d. Herhangi bir belgenin gizlilik derecesi her sayfanın sol üst ve alt köşesine yazılır ve aynı gizlilik derecesi, her sayfanın üst ve alt kenar ortasına kırmızı ıstampa ile basılır. "HİZMETE ÖZEL"den daha yüksek gizlilik derecesi verilen herhangi bir belgeye, dağıtımı yapılacak her bir nüsha için farklı olacak şekilde özel bir güvenlik numarası verilir ve bunlar özel olarak işaretlenip kayıt altına alınır. Malzemelerde ise gizlilik derecesi, malzeme veya ambalajının üzerine kırmızı renkle görülecek ve çıkmayacak şekilde işaretlenir.

e. Farklı gizlilik dereceleri taşıyan bölümleri olan bir belge, en yüksek gizlilik derecesini taşıyan bölümün gizlilik derecesi ile sınıflandırılır. Ancak bu gizlilik derecesi, belgenin her sayfasına basılmayıp yalnız ilgili bölüm ile ilk sayfasının veya kabının üst ve alt kenarlarının ortasına basılır. Belgeye dâhil diğer bölümler, kendi gizlilik derecelerini taşır.

f. Üzerinde gizlilik dereceli bilgi bulunan CD, DVD, taşınabilir bilgisayar, flash bellek vb. bilgi depolama aygıtları Kontrollü Bölge dışındaki bilgisayarlarda kullanılmaz.

g. Bilgi sistem donanımlarının daha düşük gizlilik dereceli bir ağa bağlanması durumunda, üzerinde işlenecek bilgilerin gizlilik derecesinin düşürülmesi için aşağıdaki önlemler uygulanır.

(1) Sabit diskte yer alan veriler, güvenli silme yöntemleriyle silinerek, sabit disk formatlanır ve işletim sistemi yeniden kurulur.

(2) Donanımın üzerinde yer alan ve bağlanılan ağın üzerinde işlenen bilginin gizlilik derecesini vb. gösteren etiket ve işaretler çıkarılır/değiştirilir.

3. GİZLİLİK DERECELİ BİLGİ, BELGE VE MALZEMENİN VERİLMESİ VEYA AÇIKLANMASI:

a. Savunma sanayii alanındaki herhangi bir gizlilik dereceli bilgi, belge ve malzeme ya da gizlilik dereceli projeye; sadece bunların gizlilik derecesine uygun Kişi Güvenlik Belgesine sahip şahıslar tarafından bilmesi gereken prensibine göre nüfuz edilebilir. Ayrıca; bahse konu proje, uygun seviyeli Kişi Güvenlik Belgesi bulunmayan şahıslara ya da uygun seviyeli Tesis Güvenlik Belgesi olmayan kuruluşlara verilemez ve açıklanamaz.

b. Savunma sanayii alanındaki herhangi bir gizlilik dereceli bilgi, belge ve malzeme ya da gizlilik dereceli proje gizlilik derecesine uygun Tesis Güvenlik Belgesine sahip tesis veya yerde muhafaza edilir veya kontrollü bölgede işlem yapılır.

c. Uygun seviyede Kişi Güvenlik Belgesi ve Tesis Güvenlik Belgesi olmayan şahıs ya da kuruluşlar/kurumlar, savunma sanayii alanındaki herhangi bir gizlilik dereceli bilgi, belge ve malzeme ya da gizlilik dereceli projeye erişemez, bunların bulunduğu ya da yürütüldüğü gizlilik dereceli yerlere ve tesislere giremez ve bunlarla ilgili andlaşma, sözleşme veya alt sözleşme çalışmalarına ve uygulamalarına iştirak edemez.

ç. Uluslararası gizlilik dereceli projelerde yer almaya istekli kuruluşların, Türkiye Cumhuriyeti sınırları içerisinde kurulmuş olmayan yabancı bir kuruluş olması ya da istekli kişilerin yabancı olması hâlinde; istekli kuruluş ve kişilerden kendi ülkelerinin yetkili makamlarınca tanzim edilmiş ve onaylanmış uygun gizlilik dereceli güvenlik belgeleri istenir. Bu kuruluş ve kişilerin gizlilik dereceli bilgi, belge ve malzeme ya da gizlilik dereceli projeye erişimine, sadece, temin edilen güvenlik belgelerinin geçerliliğinin Savunma Sanayii Millî Güvenlik Makamı tarafından ilgili ülke yetkili makamları ile teyit edilmesini müteakip izin verilir.

d. Askerî personel (Jandarma Genel Komutanlığı ile Sahil Güvenlik Komutanlığı dâhil olmak üzere Türk Silahlı Kuvvetleri personeli) ve Millî Savunma Bakanlığı personeli için Kişi Güvenlik Belgesi tanzim edilmez, bu personelin nüfuz edeceği gizlilik dereceli bilgi, belge ve malzeme seviyesi, kurum/komutanlık tarafından belirlenir.

e. Uluslararası faaliyetlerin bir gereği olarak Türk Silahlı Kuvvetleri envanterinde bulunan veya savunma sanayii kuruluşları tarafından Türk Silahlı Kuvvetleri için üretilen veya modernize edilen silah ve destek sistemleri ve/veya gizlilik gerektiren bir faaliyet hakkındaki bilgi, belge ve malzemenin, yerli veya yabancı ülke mensuplarıyla paylaşılacak bilgi düzeyi ve yapılacak açıklama düzeyi hakkında Genelkurmay Başkanlığınca karar verilir.

f. Savunma sanayii alanındaki herhangi bir gizlilik dereceli bilgi, belge ve malzemenin yurt dışına verilmesi gerektiğinde, taraf olunan uluslararası andlaşma hükümleri saklı kalmak kaydıyla, Savunma Sanayii Millî Güvenlik Makamı tarafından, konuyla ilgili olarak Genelkurmay Başkanlığı ile yapılacak koordine sonrasında, açıklanacak ve paylaşılacak bilgi düzeyi tespit edilerek, bilgi ve belgeyi açıklayacak makama ulaştırılır ve sonucu takip edilir.

g. Proje makamlarınca, yurt dışından tedarik edilecek, gizliliğe haiz mal ve hizmet alımlarında, gizlilik ve güvenlik ihtiyaçları Savunma Sanayii Millî Güvenlik Makamı ile koordineli olarak belirlenir.

ğ. Proje Makamlarınca, bir malzeme veya hizmetin üretime dayalı olarak yurt içinden temin edilmesi sürecinde, tedarik projesinin gizlilik derecesi ihtiva etmesi durumunda, söz konusu malların ihalesine katılacak olan istekli kuruluşlardan, Kişi Güvenlik Belgesi, Tesis Güvenlik Belgesi ile ARGE Projeleri hariç olmak üzere Üretim İzin Belgesi istenir.

h. Yabancı firma ve kuruluşlara açık olan ve İhtiyaç Makamınca gizlilik derecesi verilen uluslararası ihalelerde, ülkeler ile yapılan andlaşma hükümleri saklı kalmak koşuluyla, bu ihalelere katılmaya istekli kuruluşlar ve kişilerden kendi ülkelerinin yetkili makamlarınca tanzim edilmiş ve onaylanmış uygun gizlilik dereceli Kişi Güvenlik Belgesi ve Tesis Güvenlik Belgesi veya bunların yerine geçen muadili belgeler istenir. Yerli firmalardan ise Savunma Sanayii Millî Güvenlik Makamı tarafından verilen Kişi Güvenlik Belgesi ile Savunma Sanayii Millî Güvenlik Makamı veya Kuzey Atlantik Andlaşması Teşkilâtı Merkez Kurulu Başkanlığınca verilen Tesis Güvenlik Belgesi istenir.

4. SATIŞ VE DEVİR İŞLEMLERİ:

a. Gizlilik dereceli bilgi, belge, proje ve malzemenin andlaşmalarda belirlenenlerin dışındaki ülke ve kişiler ile yurt içinde açıklanması veya satışı, devri, aşağıda belirtilen esaslar çerçevesinde yapılır:

(1) Yurt dışından, herhangi bir andlaşma dâhilinde temin edilmiş ise, andlaşmada yer alan hükümler geçerlidir.

(2) Yurt içinde geliştirme ve üretilme durumunda, 29 Haziran 2004 tarihli ve 5201 sayılı Kanun ile bu Kanuna göre çıkarılan Yönetmelik kapsamında işlem yapılır.

(3) NATO projelerinde, andlaşmada yer alan hükümler uygulanır.

(4) Yukarıda belirtilen hususlar ve diğer kanunlarda yer alan yetkiler dışında kalan gizlilik dereceli bilgi, belge, proje ve malzemenin satış ve devir işlemlerine, Genelkurmay Başkanlığı ile koordineli olarak gerektiğinde, Dışişleri Bakanlığı ve diğer ilgili kurum ve kuruluşların görüşleri ile NATO ve Birleşmiş Milletler kararları dikkate alınarak Savunma Sanayii Millî Güvenlik Makamı tarafından izin verilir.

5. GİZLİLİK DERECELİ BELGE VEYA MALZEMENİN MUHAFAZASI:

a. TASNİF DIŞI olarak adlandırılan veya işaretlenen bilgi, belge, malzeme ya da projenin, taraf olunan uluslararası andlaşma hükümleri saklı kalmak kaydıyla, savunma sanayii güvenliği ile ilgili mevzuatta belirtilen esas ve usuller çerçevesinde korunması gerekmez; bu tür bilgi, belge, malzeme ya da projeye erişim için güvenlik belgesi talep edilmez.

b. ÇOK GİZLİ, GİZLİ ve ÖZEL gizlilik dereceli belge ve malzeme, Kontrollü Odalarda kasa, çelik masa veya demir kuşaklı çelik dolaplar içinde muhafaza edilir. Kontrollü oda ve dolaplar, çift kilit sistemi ile donatılır. Kuruluşa ait tesislerde bu iş için ayrılmış özel bir yer bulundurulur.

c. Savunma sanayii kuruluşlarında bulunan HİZMETE ÖZEL bilgi ve belgeler Kontrollü Bölgelerde çift kilitli dolaplarda muhafaza edilebilir.

ç. Kontrollü odalara giriş çıkış yapan personel ile giriş nedeni her işlem için kayıt altına alınır.

d. Gizlilik dereceli hiç bir belge, ilgisiz ve yetkisiz kişilerin görebileceği şekilde açıkta bırakılmaz.

e. Gizlilik dereceli bilgi, belge ve malzemenin kaybolması hâlinde, rapor ile kayıt altına alınır, durum derhâl belgeyi gönderen makama bildirilir ve Savunma Sanayii Millî Güvenlik Makamına bilgi verilir.

f. ÖZEL ve üzeri gizlilik dereceli askerî ve ulusal güvenlik amaçlı yazılım üretenler ile en az ÖZEL gizlilik dereceli bilgi üreten, bu seviyeli bilgi ile çalışan veya elektronik ortamda depolayan kuruluşlar tarafından, bilginin üretildiği ve depolandığı bilgi sistem odalarında ve bilgisayar sistemlerinde kullanılan, enerji iletim, iletişim ve veri hatlarına dışarıdan müdahaleye ve bilgi sızmasına engel olacak güvenlik tedbirleri alınır ve bu sistemlere yönelik TEMPEST koruması sağlanır.

6. GİZLİLİK DERECELİ BELGENİN KAYDI, ÇOĞALTIMI VE TERCÜMESİ:

a. Kuruluşların gelen ve giden evrak, bilgi ve belgeleri için merkezi bir kayıt ve takip sistemi, gizlilik derecesi ihtiva eden Millî ve NATO evrak, bilgi ve belgeler için gelen ve giden olmak üzere ayrıca kayıt sistemi oluşturulur.

b. Gizlilik dereceli belgenin kaydının yapıldığı gelen ve giden evrak kayıt defterinde; gizlilik derecesi, konusu, geldiği makam, gönderildiği makam, ekleri, sıra numarası, gönderildiği tarih, giriş tarihi ve kayıt numarası, teslim alanın kimliği, teslim aldığı tarih ve imzası, kaldırıldığı dosya vb. bilgiler yer alır.

c. ÇOK GİZLİ, GİZLİ ve ÖZEL gizlilik derecesi taşıyan belgeler, kuruluş güvenlik sistemi içinde izlenebilir kayıt sistemi oluşturulmadan çoğaltılmaz ve tercüme edilmez. HİZMETE ÖZEL gizlilik derecesi taşıyan belgelerin çoğaltılması durumunda kopya numarası verilmez.

ç. Kurye ile gönderilecek GİZLİ ve ÖZEL gizlilik dereceli belge veya malzeme için bir adet zarf veya uygun ambalaj ile dört adet senet hazırlanır. Senetlerin iki adedi belge veya malzeme ile beraber zarfın/ambalajın içine konur, zarf/ambalaj ek yerleri bantlanır, imzalanır ve mühürlenir. Diğer iki adet senet, zarfa/ambalaja iliştirilir ve evrak bürosuna teslim edilir. Evrak bürosu ilgilisince, zarf/ambalaj üzerindeki bilgiler kayıt edilir, senedin bir sureti imzalanır ve belgeyi getiren personele iade edilir.

d. Şahsa hitaben yazılan yazılarla, ÖZEL işaretli gizlilik dereceli belgelerin zarfı veya ambalajı açılmaz, bu gibi bilgilere nüfuz etme girişiminde bulunulmaz. Kayıt ve kontrol işlemi, zarf üzerindeki bilgilerden veya gönderme bilgilerinden yararlanılarak yapılır.

e. Gizlilik dereceli bilgiler belgegeçer ve elektronik posta ilegönderilemez.

7. GİZLİLİK DERECELİ BİLGİ, BELGE VE MALZEMENİN TAŞINMASI:

a. Gizlilik dereceli bilgi, belge ve malzemenin taşınması sırasında güvenliklerinin ve korunmalarının sağlanması için gereken fiziki koruma önlemlerinin gönderici ve alıcı tarafından alınması veya aldırılması zorunludur. Taşınması öngörülen gizlilik dereceli bilgi, belge ve malzemenin göndericisi ve alıcısı, uygun gizlilik derecesinde Tesis Güvenlik Belgesine ve taşımada görev alacak personeli ise, uygun gizlilik derecesinde Kişi Güvenlik Belgesine sahip olmalıdır.

b. Gizlilik dereceli bilgi, belge ve malzemenin taşınmasında görev alacak kurye hizmeti veren savunma sanayii kuruluşlarından uygun gizlilik dereceli Tesis Güvenlik Belgesi, taşımada görev alacak kurye personelinden ise uygun gizlilik derecesinde Kişi Güvenlik Belgesi istenir.

c. Yurt içinden yurt dışına veya yurt dışından yurt içine taşınacak ÖZEL ve daha yüksek gizlilik dereceli bilgi, belge ve malzemenin sahibi olan kişi, kuruluş ya da makamlar tarafından hazırlanan taşıma planlarına ilişkin EK-C'de yer alan Kurye Yetkilendirme Formu, taşıma yapılmadan önce, Proje Makamı koordinesiyle, Savunma Sanayii Millî Güvenlik Makamına onaylatılır. Hazırlanacak taşıma planlarında en az;

(1) Gizlilik dereceli gönderiyi teslim alacak ve gönderecek makam ve personelin açık adı ve adresi,

(2) Gizlilik dereceli gönderinin gönderilme gerekçesi ve varsa ana proje bilgileri,

(3) Gönderiye ait ağırlık, hacim, miktar bilgileri ve gizlilik derecesi,

(4) Taşımanın yapılacağı tarihler, izlenecek rota ve kullanılacak ulaşım vasıtaları ile Kurye veya güvenlik personelinin kimlikleri ve bağlı oldukları kuruluş bilgileri,

(5) Gönderiye ilişkin gümrük işlemleri ile varsa ihracat izinlerine ilişkin bilgiler yer almalıdır.

ç. ÖZEL'den daha düşük gizlilik dereceli bilgi, belge ve malzemenin taşınmasına ilişkin alınacak önlemler, kuruluş tarafından hazırlanacak Tesis Özel Güvenlik El Kitabında tanımlanır.

d. Taraf olunan uluslararası andlaşma hükümleri saklı kalmak kaydıyla, uluslararası taşıma işlemleri aşağıda belirtilen esaslar çerçevesinde yürütülür.

(1) "ÖZEL" ve daha yüksek gizlilik dereceli bilgi, belge ve malzemenin yurt dışına yapılacak taşıma işlemi, imkânlar ölçüsünde Dışişleri Bakanlığının diplomatik kuryeleri vasıtasıyla yapılır. Bunun mümkün olmadığı hâllerde, "ÖZEL" ve daha yüksek gizlilik dereceli bilgi, belge ve malzemenin yurt dışına transferi, Savunma Sanayii Millî Güvenlik Makamınca onaylanan ve ilgili ülke yetkili makamlarına iletilen kurye yetkilendirme formu çerçevesinde, kuruluşlarca görevlendirilecek uygun gizlilik dereceli Kişi Güvenlik Belgesi bulunan kurye vasıtasıyla yapılır. Taşımaya ilişkin masraflar alıcı veya gönderici tarafından karşılanır.

(2) Yurt dışına posta veya taşıma firmaları vasıtasıyla sadece "HİZMETE ÖZEL" gizlilik dereceli bilgi, belge ve malzeme gönderilebilir.

e. Görevin tamamlanmasını takiben sonucu Savunma Sanayii Millî Güvenlik Makamına rapor edilir.

f. TSK tarafından kriptolanmış ve karşılıklı belgegeçer cihazlarına enteğre edilmiş kripto cihazları olması halinde, HİZMETE ÖZEL doküman, bu belgegeçer cihazlar ile gönderilebilir.

8. GİZLİLİK DERECELİ BİLGİ, BELGE VE MALZEMENİN İMHASI:

a. Belirli bir zaman sonra veya herhangi bir olayı müteakip, gizlilik dereceli bir bilgi, belge veya malzemenin kıymetinin kalmadığı kanaati hasıl olduğunda; bu bilgi, belge ve malzemeler ilgili talimatlar çerçevesinde imha edilir ve izlenebilir şekilde kayıt altına alınır.

b. Bu durumda söz konusu bilgi, belge ve malzeme, üç kişilik bir heyet teşkil edilerek imha edilir ve imha tutanağı tanzim edilir. Kuruluş üst düzey yöneticileri tarafından onaylanan imha tutanağının bir sureti proje makamına gönderilir, diğer sureti dosyalanarak muhafaza edilir.

ÜÇÜNCÜ BÖLÜM
PROJE UYGULAMALARI

1. GENEL:

a. Savunma projelerinin uygulama sürecinde, planlama safhasından uygulama safhasına geçilmeden önce ihtiyaç makamlarınca belirlenen gizlilik derecesi esas alınır.

b. Tedarik, modernizasyon ve AR-GE dahil savunma projelerinin gizlilik derecesi, uluslararası andlaşma hükümleri saklı kalmak kaydıyla; gerektiğinde Savunma Sanayii Millî Güvenlik Makamı ile koordine edilerek ve bu Yönergede tanımlanan gizlilik derecelerine uygun olarak Proje Makamı tarafından gizlilik derecesinin uygulanacağı süre ve indirileceği veya kaldırılacağı tarih için de Proje Makamınca işlem yapılır.

c. ÖZEL veya üzeri gizlilik derecesine sahip savunma sanayii projelerinde güvenliğin sağlanması amacıyla Proje Makamı koordinatörlüğünde ilgili makam ve kuruluşların katılımıyla örneği EK-Ç'de yer alan Proje Güvenlik Talimatı hazırlanır. Proje Güvenlik Talimatı Savunma Sanayii Millî Güvenlik Makamının onayını müteakip yürürlüğe girer. Projenin, Proje Güvenlik Talimatı esaslarına uygun olarak yürütülmesi ve kontrolü proje makamı yetki ve sorumluluğundadır.

ç. Proje ile ilgili şartname hazırlıkları, teklife çağrı hazırlıkları ve teklif alınacak kişi veya kuruluşları belirleme hazırlıkları, projeye verilen gizlilik derecesinin seviyesine göre yürütülür. Ayrıca, Proje Makamlarınca şu önlemler alınır:

(1) Projenin gizlilik derecesi kontrol edilir, buna göre önce teklif alınabilecek kişi veya kuruluşlar belirlenir. Alınacak güvenlik tedbirleri gözden geçirilir.

(2) Proje üzerinde çalışacak personel belirlenir.

(3) Uygun gizlilik dereceli Kişi Güvenlik Belgesi ve Tesis Güvenlik Belgesi bulunmayan kişilere ve kuruluşlara, gizlilik dereceli bilgi ve belge açıklanmaz veya verilmez.

(4) Gizlilik derecesinin seviyesine göre bu bilgilerin verilmesinden önce gerekli görülen diğer ilave tedbirler alınır ve bilmesi gereken prensibi uyarınca hareket edilir.

d. Proje Makamlarınca hazırlanacak sözleşme ve eklerinde; projenin gizlilik seviyesi ile uyumlu Kişi Güvenlik Belgesi ve Tesis Güvenlik Belgesine sahip olmayan kişi, kuruluşların, projede üretilen/verilen gizlilik dereceli bilgi, belge ve malzemeye erişememesi için bu Yönergede yer alan güvenlik tedbirlerinin alınmasına, gizlilik dereceli bilgi, belge ve malzemenin, proje gizlilik derecesine uygun Tesis Güvenlik Belgesine sahip tesis veya yerde muhafaza edilmesine, projenin genel güvenlik ve gizlilik ihtiyaçları ile gizlilik dereceli bilgi, belge ve malzemenin taşınması sırasında bu Yönergede tanımlanan güvenlik önlemlerinin alınmasına yönelik hükümlere ve projede görev alan yüklenici ve alt yüklenici tesislerine yapılacak ziyaretlere ilişkin düzenlemelere yer verilir.

e. Proje Makamınca, yürütülecek projenin gizlilik derecesi dikkate alınarak, teklif isteme ve teklife çağrı dosyalarının gönderilmesi süreci de dâhil olmak üzere, ilgili şahıs ve kuruluşlardan Kişi Güvenlik Belgesi, Tesis Güvenlik Belgesi ile ARGE projeleri hariç olmak üzere, ÜİB istenir.

f. Proje Makamınca; teklif veren ve sözleşme yapan kişi ve kuruluşlara ilişkin güvenlik belgeleri arşivi, Savunma Sanayii Millî Güvenlik Makamı ile koordineli olarak oluşturulur ve yapılan ihlâller veya şüpheli durumlar hakkında Savunma Sanayii Millî Güvenlik Makamına bilgi verilir.

g. Proje uygulama aşamasına ilişkin gizlilik dereceli hususlar, barış dönemi faaliyetlerine paralel olarak, seferberlik ve savaş hâline yönelik çalışmaları da kapsar. Yürürlükte bulunan"Seferberlik ve Savaş Hâline İlişkin Harp Sanayii Faaliyetlerinin Yürütülmesi Yönergesi" esaslarına göre görev verilecek kuruluşlar tespit edilirken, bu Yönergede belirtilen esaslara uygun olarak teşkilâtlanmış kuruluşlara öncelik verilir.

2. TEKLİF İSTEME/TEKLİFE ÇAĞRI DOSYALARININ GÖNDERİLMESİ:

a. Savunma projeleri için hazırlanmış şartname veya teklife çağrı dosyaları, gizlilik derecelerine uygun biçimde ilgili kişi veya kuruluşlara gönderilir ve tekliflerin ihlâle meydan vermeyecek şekilde hazırlanarak Proje Makamına iletilmesi sağlanır.

b. Gerek Proje Makamı ve gerekse projeye teklif veren kişi veya kuruluş; gizlilik dereceli bilgi, belge ve malzemenin, karşı tarafa güvenli şekilde ulaştırılmasından sorumludur.

3. GİZLİLİK DERECELİ SÖZLEŞME GÖRÜŞMELERİ VE PROJE TOPLANTILARI:

a. Toplantıya gizlilik derecesi uygun olan personel ile toplantıda yüklenici taraf olabilecek kişi veya kuruluşun, toplantının gizlilik derecesine eşdeğer veya daha üst gizlilik derecesinde Kişi Güvenlik Belgesi sahibi olan bilmesi gereken personeli katılır.

b. Görüşülecek konunun gizlilik derecesine göre; projede görev almak isteyen kişi veya kuruluşun mal veya hizmet üretimini yapacağı tesisi için, uygun gizlilik dereceli Tesis Güvenlik Belgesi bulunup bulunmadığı kontrol edilir.

c. Toplantının gizlilik derecesi, toplantıyı düzenleyen makam tarafından önceden tayin edilir ve toplantı başlamadan önce katılımcılara gerekli güvenlik açıklaması yapılır. Toplantıda, projeyi ilgilendiren hususlar dışında gizlilik dereceli konular konuşulmaz.

ç. Sözleşme görüşmelerinde, proje uygulamasında göz önüne alınacak güvenlik tedbirleri ile yüklenici kişi veya kuruluşun uyması gereken güvenlik kuralları ve yüklenici kişi veya kuruluşun proje üzerindeki güvenlik sorumlulukları açıklanır.

d. Sözleşme görüşmelerinde, ihtiyaç olması durumunda Savunma Sanayii Millî Güvenlik Makamını temsil eden bir personel talep edilebilir.

e. Proje uygulamasına yönelik olarak, Proje Makamı veya yüklenici kişi veya kuruluş tarafından planlanabilecek her tür toplantı için, toplantı salonu veya yerinin emniyeti, toplantıyı düzenleyen kişi veya kuruluş tarafından sağlanır. Toplantı başlamadan önce, toplantıya katılan kişilerin uygun Kişi Güvenlik Belgesi olup olmadığı kontrol edilir ve bilmesi gerekenler dışında kalan kişilerin toplantıya katılması önlenir.

f. Gerçekleştirilen gizlilik dereceli toplantılardan ÖZEL ve üzeri gizlilik derecesine haiz olanlar için EK-D'de yer alan Toplantı Katılım Formu düzenlenir ve en az iki yıl muhafaza edilir. Proje Makamınca uygun görülen hallerde, Toplantı Katılım Formunun bir sureti, katılımcılara da verilebilir.

4. GİZLİLİK DERECELİ SÖZLEŞME UYGULAMALARI:

a. Proje Makamlarınca, sözleşme görüşmeleri sırasında yapılan açıklamalar ve sözleşmede yer verilen güvenlik hükümleri çerçevesinde ve belirlenen proje uygulama sürecinde; yüklenici kişi veya kuruluşun sorumluluk aldığı konulardaki güvenlik tedbirleri, kontrol altında tutulur. Uygulamada karşılaşılabilecek ihlaller hakkında yüklenici kişi veya kuruluş veya temsilcileri uyarılır ve gerekli tedbirlerin alınması sağlanır.

b. Herhangi bir uyarı yapılmamış olsa dahi uygulamada gizlilik ihlali tespit edildiği takdirde yasal tedbirlere başvurulur. Proje Makamı veya Savunma Sanayii Millî Güvenlik Makamının ikazına rağmen önlem alınmaması halinde Kanunda öngörülen yasal tedbirler uygulanır.

5. YÜKLENİCİ KİŞİ VEYA KURULUŞUN SORUMLULUKLARI:

Yüklenici kişi veya kuruluş, gizlilik dereceli sözleşmelerde belirtilen hükümlere uygun şekilde hareket etmek zorundadır. Bu çerçevede yüklenici kişi veya kuruluşların özellikle yerine getirmek zorunda oldukları güvenliğe ilişkin hususlar şunlardır:

a. Sözleşme, ek sözleşme veya alt sözleşme öncesi ve sonrasında gerekli güvenlik önlemlerini almak.

b. Tesis Güvenlik Belgesinin temel şartları çerçevesinde sözleşme gereklerini yerine getirmek, varsa güvenlik ihlallerini ve/veya uygunsuzluklarını gidererek Proje Makamı ile Savunma Sanayii Millî Güvenlik Makamını bilgilendirmek.

c. Gizlilik dereceli bilgilere nüfuz edebilecek personeli için uygun gizlilik dereceli Kişi Güvenlik Belgesi almak, bunlarla ilgili kayıtları tutmak ve varsa sakıncalı personel için gerekli önlemleri almak.

ç. Ana, alt ve ek sözleşmeler gereği gizlilik dereceli bilgiyi alt yükleniciye vermek söz konusu olduğunda, proje makamı ve Savunma Sanayii Millî Güvenlik Makamı ile ön koordinasyonda bulunmak ve alınacak sonuca göre işlem yapmak.

d. Projenin gerçekleştirilmesi sürecinde alt yüklenici kullanılması durumunda, Proje Makamı bilgisi dâhilinde, yapılacak alt sözleşme ve protokollere ana sözleşmede yer verilen güvenlik ile ilgili hususları dâhil etmek.

e. Proje ile ilgili bilgilerin korunmasına ilişkin kendisine verilecek herhangi bir talimat veya usule uymak, projenin tamamlanması veya herhangi bir nedenle sözleşmenin feshi durumunda dahi, kendisine verilmiş veya proje kapsamında üretilmiş gizlilik dereceli bilgi veya malzemeyi usulünce korumaya devam etmek.

6. SÖZLEŞME GÜVENLİK HÜKÜMLERİ:

Proje Makamınca hazırlanan tüm sözleşmelere uygun gizlilik derecesi verilir. Gizlilik dereceli proje sözleşmelerinde, gerekli görülecek koruyucu güvenlik önlemlerini içeren idarî veya teknik istek ve özelliklere ilaveten, duruma uyan düzenlemelerin yapılması suretiyle aşağıda belirtilen tanım, tarif ve hükümlere de yer verilir:

a. İhtiyaç Makamı (Türk Silahlı Kuvvetlerinin söz konusu mal veya hizmet ihtiyacını belirleyen biriminin adı yazılır).

b. Proje Makamı (Türk Silahlı Kuvvetleri adına sözleşmeyi hazırlayan ve imzalayan makamın ilgili dairesinin adı yazılır).

c. Savunma Sanayii Millî Güvenlik Makamı (Millî Savunma Bakanlığı Teknik Hizmetler Genel Müdürlüğüdür).

ç. Sözleşme kapsamında verilen veya üretilen gizlilik dereceli bilgi, belge ve malzeme şu şekilde korunur:

(1) Alıcı; gönderenin yazılı izni olmaksızın gizlilik dereceli bilgi, belge ve malzemeyi, üçüncü kişilere ya da kuruluşlara veya bunların temsilcilerine açıklayamaz. Bu izin, Savunma Sanayii Millî Güvenlik Makamı ile koordine edilerek verilebilir.

(2) Alıcı; gizlilik dereceli bilgi, belge veya malzemeyi, uygun güvenlik önlemleri alınmış ortamlarda muhafaza eder veya kullanabilir.

(3) Alıcı; gizlilik dereceli bilgi, belge veya malzemeyi, gönderenin yazılı izni olmaksızın, planlanan veya onaylanan amaçlar dışında herhangi bir nedenle kullanamaz (Proje Makamınca gerek görülürse, bu izni almak için takip edilecek usuller bu paragrafta belirtilir).

(4) Sözleşme kapsamında verilen veya üretilen gizlilik dereceli bilgi, belge veya malzemenin, uluslararası alanda transferi, sadece hükümetten hükümete prensibiyle ve yazılı olarak belirtildiği şekilde yapılır.

(5) Gizlilik dereceli bilgi, belge, malzeme ve proje, sadece Savunma Sanayii Millî Güvenlik Makamınca uygun gizlilik dereceli Kişi Güvenlik Belgesi tanzim edilmiş şahıslara Bilmesi Gereken Prensibine uygun olarak açıklanabilir.

(6) Sözleşme kapsamında verilen veya üretilen gizlilik dereceli bilgi, belge ve malzeme uygun gizlilik derecesi ile işaretlenir.

(7) Sözleşme kapsamında verilen veya üretilen gizlilik dereceli bilgi, belge veya malzemenin kaybolması veya yetkisiz kişilere açıklanması durumu ile karşılaşıldığında, konu hemen ve tam olarak Proje Makamına ve Savunma Sanayii Millî Güvenlik Makamına rapor edilir.

(8) Yüklenici tarafından, sözleşme kapsamında verilen veya üretilen gizlilik dereceli bilgi, belge veya malzeme, diğer potansiyel yüklenicilere veya uygun gizlilik dereceli Kişi Güvenlik Belgesi ve Tesis Güvenlik Belgesi bulunmayan alt yüklenicilereverilemez.

(9) Potansiyel yüklenicilerin ya da alt yüklenicilerin yabancı bir ülkede yerleşik olması durumunda, bu kişi veya kuruluşlardan kendi ülkelerinin Yetkili Güvenlik Makamı tarafından tanzim edilmiş uygun gizlilik dereceli Kişi Güvenlik Belgesi ve Tesis Güvenlik Belgesi veya muadili belgeleri istenebilir.

(10) Proje Makamı, gerek gördüğünde, potansiyel yüklenicilerin ya da alt yüklenicilerin uygun gizlilik dereceli Kişi Güvenlik Belgesi ve Tesis Güvenlik Belgesi olup olmadığını, Savunma Sanayii Millî Güvenlik Makamı kanalıyla tetkik eder. Kişi veya kuruluşun beyanının doğru olmadığının belirlenmesi durumunda ilgili kişi veya kuruluş hakkında yasal işlem başlatır.

(11) Sözleşme çerçevesinde verilen veya üretilen bütün gizlilik dereceli bilgi, belge ve malzemenin, sözleşmenin sona ermesi ya da mevzuata uygun fesih durumunda dahi, alıcı tarafından korunmasına devam edilir.

(12) Alıcı tarafından, sözleşme çerçevesinde verilen veya üretilen gizlilik dereceli bilgi, belge ve malzemeye nüfuzu gerektiren bütün alt sözleşmelere, bu hükümler de dâhil olmak üzere, güvenliği sağlayıcı hükümler ve gerek görülecek diğer şartlar ilave edilir.

(13) Alıcı tarafından, yabancı uyruklu kişilerin gizlilik dereceli bilgi, belge ve malzemeye nüfuzunu zorunlu kılan durumlarda, bu personelden, edindikleri bilgi, belge ve malzemeyi başka amaçlar için kullanmayacakları ve üçüncü kişi ve kuruluşlara aktarmayacakları hususunda taahhütname alınır.

DÖRDÜNCÜ BÖLÜM
KONTROLE TÂBİ LİSTE KAPSAMINDA ÜRETİM YAPACAK İŞLETMELERİN KURULUŞ İZNİ İŞLEMLERİ

1. GENEL:

a. 5201 sayılı Kanunun 3'üncü maddesinde "Harp araç ve gereçleri ile silah, mühimmat ve bunlara ait yedek parçalar ve patlayıcı maddeleri üretecek kuruluşların kurulması ve işletilmesi, Sanayi ve Ticaret Bakanlığının görüşü alınmak suretiyle Millî Savunma Bakanlığının iznine bağlıdır." ifadesi mevcuttur. Bu Kanun kapsamında "Kontrole Tâbi Liste"nin nelerden ibaret olduğu, ilgili makamlar, kamu kurum ve kuruluşları ile koordineli olarak Millî Savunma Bakanlığınca belirlenir ve her yıl Ocak ayında Resmî Gazetede tebliğ olarak yayımlanır.

b. Kontrole Tâbi Liste kapsamında bulunan bir malzemenin üretimini yapacak isteklilerin, öncelikle Savunma Sanayii Millî Güvenlik Makamından Kuruluş İzni almaları gerekir. Bu kapsamda faaliyet göstermek isteyen kuruluşlar, Millî Savunma Bakanlığınca aranan istek ve özellikleri en kısa süre içinde tamamlar ve Kuruluş İzni verilmesi talebiyle başvuruda bulunur.

c. Kurulması plânlanan tesisin bulunduğu arazinin 2565 sayılı "Askerî Yasak Bölgeler ve Güvenlik Bölgeleri Kanunu"nda belirtilen araziler içerisinde yer almaması güvence altına alınmış olmalıdır.

2. KURULUŞ İZNİ İÇİN BAŞVURU:

a. Kontrole Tâbi Liste kapsamında üretim yapmak isteyen kişi veya kuruluşlarca, EK-E'de yer alan yazı ile, bu ürünlerden hangisinin üretileceği hakkında bilgi verilerek Kuruluş İzni talebinde bulunulur.

b. Savunma Sanayii Millî Güvenlik Makamı tarafından yapılan inceleme sonunda, üretimi planlanan malzemenin Kontrole Tâbi Liste kapsamında olduğunun belirlenmesini müteakip, kuruluş tarafından, aşağıda belirtilen bilgi ve belgeler dokuz nüsha dosya halinde Savunma Sanayii Millî Güvenlik Makamına gönderilir. Belgelerin, yetkili kişiler tarafından onaylanmış fotokopileri de kabul edilir.

(1) Kuruluş İzni talep eden işletmenin 29 Haziran 1956 tarihli ve 6762 sayılı Türk Ticaret Kanununa göre kurulmuş şirket olduğunu gösterir Ticaret Sicil Gazetesinin onaylı örneği.

(2) Tesisi kuracak ve işletecek olanlar ile sermaye sahiplerinin açık kimlikleri ve bu iş için koyacakları sermaye miktarı.

(3) Tesisin kurulacağı alanın; ada, pafta, parsel numaraları ve arazinin kayıtlı olduğu il ile tesise ait depo, satış merkez ve şubeleriyle idare merkezi ve bürolarının bulunacağı yerlerin adresleri.

(4) Tesisin kurulacağı alanın mülkiyeti kuruluşa ait değil ise, taşınmazın sahibi ile kuruluş arasındaki sözleşmenin onaylı sureti.

(5) Varsa üretilecek ürüne ait bilgi, belge, ürünlerin proses iş akım şemaları, tesiste olabilecek atıklar ve bertaraf yöntemlerine ilişkin bilgi ile Kapasite Raporu.

(6) Varsa ilgili Makamdan alınacak İşyeri Açma ve Çalışma Ruhsatı.

(7) Firmanın kuruluş İzni almak için başvuru yapması halinde eksik evrakları için 3 ay ek süre verilir. 3 ay içinde eksik evraklarının tamamlanmaması halinde talep iptal olur.

3. KURULUŞ İZNİ VERİLMESİ:

a. Kontrole Tâbi Liste kapsamında yer alan malzemeyi üretmeyi talep eden kuruluşların başvuru belgelerinin alınmasını müteakip, Savunma Sanayii Millî Güvenlik Makamı tarafından inceleme başlatılır.

b. Yapılan inceleme sonucunda; kuruluşun verdiği belgeler ile tesisin kurulacağı araziye ait bilgilere ilişkin olarak Genelkurmay Başkanlığının görüşü alınır ve arazinin 2565 sayılı Kanunda belirtilen ve yurt savunması bakımından stratejik önem taşıyan araziler içerisinde yer alıp almadığı tespit edilir.

c. Arazinin, 2565 sayılı Kanun kapsamında olmadığının belirlenmesi durumunda, kuruluş ile ilgili bilgi ve belgeler, Bilim Sanayi ve Teknoloji Bakanlığı, İçişleri Bakanlığı, Sağlık Bakanlığı ve Çevre ve Orman Bakanlığına gönderilerek görüşleri alınır.

ç. Alınan görüşlerin olumlu olması durumunda, Kuruluş izni için Millî Savunma Bakanının onayı alınır ve sonuç, ilgili kuruluşa bildirilir.

d. Sermaye sahiplerinin veya hissedarlarının değişmesi, başka kuruluşlarla ortaklık kurulması veya kuruluşun isminin değişmesi durumunda; Savunma Sanayii Millî Güvenlik Makamının yapacağı değerlendirme ve alacağı karara bağlı olarak Kuruluş İzni yeni isim ve unvana göre yeniden düzenlenebilir.

e. Genelkurmay Başkanlığı ile İçişleri Bakanlığının olumsuz görüş bildirmesi durumunda Kuruluş İzni verilmez ve bu husus talep eden kuruluşa bildirilir.

f. Kuruluş İzni yazısı, Millî Savunma Bakanının onayının alınmasını müteakip Millî Savunma Bakanlığı Müsteşar Teknoloji ve Koordinasyon Yardımcısı tarafından imzalanır.

g. Kuruluş İzni için herhangi bir ücret talep edilmez.

ğ. Kuruluş izni için Makam tarafından kamu yararı dikkate alınarak diğer meri mevzuatlara uyulması istenebilir ve bu hususlara uyulacağına dair taahhüt alınır.

4. KURULUŞ İZNİNİN İPTALİ VEYA YENİDEN DÜZENLENMESİ:

a. 5201 sayılı Kanunun 5'inci maddesi gereğince, sermaye sahiplerinin veya hissedarlarının değişmesi, başka kuruluşlarla ortaklık kurulması veya kuruluşun isminin değişmesi durumunda, yeni isim ve unvana göre Kuruluş İzni verilebilir.

b. Kuruluş İzninin iptalini gerektiren hususlar şunlardır:

(1) Kuruluşun tasfiyesi veya iflas etmesi.

(2) Tesisinin yerinin değişmesi.

(3) Kuruluş İzninin veriliş tarihinden itibaren 18 ay içerisinde, üretim tesisinin kurulup, Tesis Güvenlik Belgesi gereklerine hazır hale getirilememesi.

c. Kuruluş izni verildikten sonra kuruluş tarafından Kontrole Tabi Listenin askerî patlayıcılar ve piroteknik malzeme, roketatar, roket, füzeler ve torpidolar ile bunların ana parçaları hariç yeni bir ürün üretilmesi istenirse, ilgili kurum ve kuruluşların daha önceki görüşleri dikkate alınarak Makam tarafından yapılacak değerlendirmeyi müteakip Kuruluş İzni verilebilir.

BEŞİNCİ BÖLÜM
KİŞİ GÜVENLİK BELGELERİ

1. GENEL:

a. Kişi Güvenlik Belgesi; kişinin, görevi gereği bilmesi gereken gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz edebilmesini sağlayan ve/veya bu gibi gizlilik dereceli bilgi, belge ve malzemenin bulunduğu Kontrollü Oda veya gizlilik dereceli projelerin yürütüldüğü Kontrollü Bölgelere veya gizlilik dereceli yerlere giriş iznini gösteren bir belgedir. Savunma sanayii alanında faaliyet gösterecek kuruluşlarda çalışan, kuruluş ve proje güvenliğinin sağlanması amacıyla, hakkında yapılan Güvenlik Soruşturması ve Arşiv Araştırması sonucunda durumu uygun bulunan kişiler için Savunma Sanayii Millî Güvenlik Makamınca tanzim edilir.

b. Görevlendirilen kişinin nüfuz edebileceği en üst gizlilik derecesinin seviyesi, tanzim edilen Kişi Güvenlik Belgesinde belirtilir. Burada konu edilen şahıslar, savunma sanayii projelerinde görev üstlenecek/görevlendirilecek, proje üzerinde görüşme ve çalışma yapabilecek, proje toplantılarına veya gizlilik dereceli konuların görüşüldüğü brifing ve demonstrasyonlara katılabilecek kişiler veya bunların temsilcileridir.

c. Belgelendirme işlemleri, şahısların görev aldığı kuruluşların talebi ile başlatılabileceği gibi, Proje Makamının talebi ile de başlatılabilir. Kuruluş tarafından yapılan başvurularda, gizlilik dereceli bilgi, belge ve malzemeye nüfuz etmesi gerekli her personel listeye dâhil edilir. Gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz etmeyecek personel (5188 sayılı Kanun kapsamında görevlendirilen güvenlik görevlisi, bahçıvan, temizlik görevlisi, yemekhane görevlisi, şoför, stajyer, bekçi, sağlık görevlisi, muhasebe personeli vs.) için başvuru yapılmaz.

ç. Bilmesi Gereken Prensibi gereği, Kişi Güvenlik Belgesi bulunsa dahi ilgisi olmayan şahısların gizlilik dereceli projelerde görev üstlenmesine veya gizlilik dereceli herhangi bir bilgi, belge veya malzemeye nüfuz etmesine müsaade edilmez. Güvenlik önlemleri ve gerekli kontroller, çalışmayı planlayarak yürüten, toplantı veya brifingi tertipleyen makamın sorumluluğunda alınır ve yapılır.

d. Çifte vatandaşlığı olan Türkiye Cumhuriyeti uyruklu kişiler için gerekli tahkikat sonucunda Kişi Güvenlik Belgesi verilebilir.

e. Kuruluşlarca Tesis Güvenlik Belgesi alınan/alınacak tesislerinde Millî Güvenlik Makamı izni olmaksızın yabancı uyruklu personel çalıştırılmaz.

f. Kuruluşlarda çalışan yabancı uyruklu kişilerin kimlikleri ve varsa kendi ülkelerinin yetkili makamlarından alınmış Kişi Güvenlik Belgeleri veya muadili belgeler hakkında Savunma Sanayii Millî Güvenlik Makamına bilgi verilir. Bu bilgiler, Savunma Sanayii Millî Güvenlik Makamınca, gerekli görülen durumlarda, zamana bağlı olmaksızın, uygun görülecek yollardan ve yerlerden araştırılabilir. Araştırma sonucunun olumsuz çıkması durumunda, derhâl ilgili kuruluş uyarılır, yabancı şahsın gizlilik dereceli projede görev alması ve gizlilik dereceli bilgi, belge veya malzemeye erişmesi engellenir.

g. NATO gizlilik dereceli Tesis Güvenlik Belgesi bulunan kuruluşlarca talep edilen NATO gizlilik dereceli Kişi Güvenlik Belgeleri, Kuzey Atlantik Antlaşması Teşkilâtı Merkez Kurulu Başkanlığı adına Savunma Sanayii Millî Güvenlik Makamınca düzenlenir. Anılan Kişi Güvenlik Belgeleri yurt içi kullanım için geçerli olup, yurt dışı Kişi Güvenlik Belgesi ihtiyaçları, Kuzey Atlantik Antlaşması Teşkilâtı Merkez Kurulu Başkanlığınca değerlendirilir.

ğ. Kişi Güvenlik Belgesine sahip personelin, her altı ayda bir olmak üzere, kuruluşlar tarafından adli sicil takibi yaptırılır (Adli sicil takibinde ilgili personelin "adli sicil ve arşiv kaydı" olmadığına dair yazılı beyanı yeterli kabul edilebilir.). Kişi Güvenlik Belgesine sahip personelin adli kovuşturmaya maruz kalması veya herhangi bir sebeple hüküm giymesi ve/veya adli sicil takibi sonrasında bir problemle karşılaşılması durumunda, bu durum ivedilikle Savunma Sanayii Millî Güvenlik Makamına bildirilir. Savunma Sanayii Millî Güvenlik Makamının görüşü alınana kadar geçen süre içinde söz konusu personelin gizlilik dereceli bilgi, belge, malzeme ve projeye nüfuz etmesi engellenir.

h. Kişi Güvenlik Belgesinin süresinin dolması veya kişinin kuruluştan ayrılması halinde, kuruluş tarafından Kişi Güvenlik Belgesinin iptal edilmesine yönelik ivedilikle Savunma Sanayii Millî Güvenlik Makamına bilgi verilir. Fiziki olarak düzenlenmiş olan NATO Kişi Güvenlik Belgesi Kuzey Atlantik Antlaşması Teşkilatı Merkez Kurulu Başkanlığına iade edilir.

ı. Genelkurmay Başkanlığınca yaptırılan güvenlik soruşturması sonucunda Kripto Güvenlik Belgesi ile belgelendirilen kuruluş personeli için, güvenlik soruşturması yapılmaksızın Kişi Güvenlik Belgesi verilmesi hususunda Savunma Sanayii Millî Güvenlik Makamı yetkilidir. Benzer şekilde Savunma Sanayii Millî Güvenlik Makamınca yaptırılan güvenlik soruşturması sonucunda Kişi Güvenlik Belgesi verilen personele, Kripto Güvenlik Belgesi verilmesi hususunda Millî Savunma Bakanlığı yetkilidir.

i. Tesis Güvenlik Belgesi başvurusunda bulunmayan kuruluşlar, Kişi Güvenlik Belgesi başvurusu yapamaz. Kuruluşlar tarafından, Tesis Güvenlik Belgesi ve Kişi Güvenlik Belgesi almak için eş zamanlı başvuru yapılır.

j. (İptal edilmiştir)

k. (İptal edilmiştir)

l. Birden fazla kuruluşta hissedar ve yönetim kurulu üyesi görevlerinde bulunan kişilere sadece bir kuruluş üzerinden Kişi Güvenlik Belgesi verilir. Söz konusu Kişi Güvenlik Belgesi'nin diğer kuruluşlarda da geçerliliği Millî Güvenlik Makamınca kayda alınarak sağlanır.

m. NATO ve Millî gizlilik dereceli Tesis Güvenlik Belgesi bulunan kuruluş personeline sadece Millî gizlilik dereceli Kişi Güvenlik Belgesi, sadece NATO gizlilik dereceli Tesis Güvenlik Belgesi bulunan kuruluş personeline ise Kuzey Atlantik Antlaşması Teşkilatı Merkez Kurulu Başkanlığı adına NATO gizlilik dereceli Kişi Güvenlik Belgesi tanzim edilir.

2. KİŞİ GÜVENLİK BELGESİ İÇİN BAŞVURU:

a. Şahıs şirketi statüsünde olan kuruluşların hissedarlarının tamamı, anonim şirket statüsünde olan kuruluşların ise ortaklarından, gizlilik dereceli bilgi, belge ve malzemeye nüfuz etmesine yönetim kurulu kararı ile izin verilen hissedarlar ile bu kuruluşların yönetim kurulu üyeleri, genel müdür ve genel müdür yardımcıları, güvenlik koordinatörü ile gizlilik dereceli bilgi, belge ve malzemeye nüfuz etmesi muhtemel personeli için Kişi Güvenlik Belgesi alınması maksadıyla, başvuru evrakları ile birlikte, kuruluş tarafından Savunma Sanayii Millî Güvenlik Makamına başvuru yapılır.

b. 5201 sayılı Kanunun 4'üncü maddesi gereğince yayımlanan Kontrole Tâbi Liste kapsamında yürütülen AR-GE projelerinde, ön fizibilite ve fizibilite etüdü hazırlama çalışmalarında, danışmanlık faaliyetlerinde veya panel, komisyon çalışmalarında görev alması öngörülen ve bir kuruluşa bağlı olarak çalışmayan, gizlilik dereceli bilgi, belge ve malzemeye nüfuz etmesi muhtemel akademisyen personelin Kişi Güvenlik Belgesi alması maksadıyla;

(1) Söz konusu faaliyetlerin Tesis Güvenlik Belgesine sahip bir kuruluş marifetiyle gerçekleştirilmesi durumunda, akademisyen personelin Kişi Güvenlik Belgesi başvurusu, Tesis Güvenlik Belgesine sahip kuruluş tarafından, başvuru evrakları ve Proje Makamı oluru ile Savunma Sanayii Millî Güvenlik Makamına gönderilir.

(2) Gizlilik dereceli proje faaliyetlerinin üniversite/enstitünün Tesis Güvenlik Belgesi olan bir bölgesinde gerçekleştirilmesi durumunda, ilgili akademisyen personel için Kişi Güvenlik Belgesi alınması maksadıyla, başvuru evrakları ile birlikte, Tesis Güvenlik Belgesi alan üniversitenin/enstitünün ilgili birimi tarafından Savunma Sanayii Millî Güvenlik Makamına başvuru yapılır.

(3) Gizlilik dereceli proje faaliyetlerinin doğrudan, Tesis Güvenlik Belgesi olmayan bir bölgede akademisyen personel tarafından gerçekleştirilmesinin ve gizlilik dereceli bilgi, belge ve malzemeye nüfuz edilmesinin söz konusu olması durumunda, gizlilik dereceli çalışmaların tamamının Proje Makamı kontrol ve sorumluluğunda Proje Makamınca belirlenecek Kontrollü Bölgede yapılması sağlanır. Anılan personel için Kişi Güvenlik Belgesi alınması maksadıyla gerekli başvuru, ilgili evraklarla birlikte, Proje Makamı tarafından Savunma Sanayii Millî Güvenlik Makamına yapılır.

c. Güvenlik soruşturması ve arşiv araştırması yapılması istenen her bir şahıs için,

(1) İçişleri Bakanlığının yürürlükteki Güvenlik Soruşturması ve Arşiv Araştırması Yönetmelik esaslarına göre aynı sayfada olacak şekilde tanzim edilmiş, fotokopi olmayan fotoğraflı ve ıslak imzalı "Güvenlik Soruşturması ve Arşiv Araştırması Formu" ve "Nüfus Cüzdanı Sureti",

(2) Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'nden temin edilecek 15 günü geçmemiş Adli Sicil Belgesi/Sabıka Kaydı (Biri asıl, ikisi onaylı fotokopi olabilir. Kişinin kaydına rastlanmışsa, kayıtla ilgili mahkeme kararı gibi açıklayıcı bilgi ve belge eklenir.),

(3) T.C. Kimlik Numarası bulunan nüfus cüzdanı aslının arkalı önlü bir adet fotokopisi sıraya konularak zımbalanır ve bu şekilde üç takım hazırlanarak EK-Ğ'de yer alan başvuru yazısına eklenir.

ç. Adli Sicil Belgesinde yer alan bilgiler nüfus cüzdanının aslına uygunluğu kontrol edilerek başvuru evraklarına eklenir, Resmî Kuruma hitaben alınmayan ve nüfus cüzdanı bilgileri ile örtüşmeyen Adli Sicil Belgeleri başvuru evrakları ile birlikte kuruluşa iade edilir.

d. Güvenlik soruşturması sırasında, ilgili personelin ikamet (oturma) adresinin değişmesi veya bu adreste bulunamaması durumunda; Savunma Sanayii Millî Güvenlik Makamı tarafından, Kişi Güvenlik Belgesi talep eden kuruluştan ihtiyaç duyulan bilgiler/evraklar yeniden istenir.

e. Güvenlik Soruşturması ve Arşiv Araştırması Formunun her bir suretine 4,5x6 cm ebadında, son altı ay içinde ön cepheden çekilmiş renkli vesikalık fotoğraf yapıştırılır. Fotoğrafların kenarındaki fazlalıklar uygun bir şekilde kesilerek ince bir katı alındıktan sonra sadece zamkla veya benzeri bir yapıştırıcı ile yapıştırılır ve kesinlikle tel zımba veya toplu iğne kullanılmaz. Fotoğraflar, kuruluş yetkilisi tarafından mühür veya kaşe ile onaylanır. Resimli formların fotokopi ile çoğaltılmış suretleri kabul edilmez.

f. (İptal edilmiştir)

g. Güvenlik Soruşturmasına ilişkin başvuru evrakları eksik doldurulmuşsa üç ay süre verilerek başvuru evrakları iade edilir, bu süre sonunda kuruluş tarafından geri bildirim olmadığı takdirde, söz konusu başvuru iptal edilmiş sayılır.

ğ. Kişi Güvenlik Belgesi alınması için hazırlanan başvuru evrakları üçer takım olacak şekilde harmanlanarak ve EK-Ğ'de yer alan başvuru yazısına eklenerek siyah klasörde gönderilir. Kargo ile kişi adına gönderilen başvurular ve/veya evraklar kabul edilmez.

h. İstenilen bilgiler, güvenlik soruşturması yapacak kurumlar için gerekli bilgiler olup, bunun dışında hiç bir nedenle açıklanmaz ve kullanılmaz.

3. KİŞİ GÜVENLİK BELGESİ VERİLMESİ:

a. Kuruluşlar tarafından Kişi Güvenlik Belgesi talep edilen personel için, 5202 sayılı Kanunun dördüncü maddesinin birinci fıkrasının (b) bendi gereğince, güvenlik soruşturması ve arşiv araştırması, Savunma Sanayii Millî Güvenlik Makamının talebi üzerine, mevzuata uygun olarak Millî İstihbarat Teşkilâtı Müsteşarlığı, Emniyet Genel Müdürlüğü veya mahalli mülki idare amirlikleri tarafından yaptırılır. Sonuç, Savunma Sanayii Millî Güvenlik Makamına bildirilir. Güvenlik soruşturması ve arşiv araştırması sonucu uygun olanlar ile hakkında belgelendirmeye engel teşkil edebileceği değerlendirilen tereddütlü hususlar bulunan personel için Kişi Güvenlik Belgesi tanzim edilip edilemeyeceğine ilişkin gerektiğinde hukuki mütalaa sonrası uygun bulunan kişilere, Savunma Sanayii Millî Güvenlik Makamı tarafından istenilen gizlilik derecesinde, en fazla beş yıl süreyle geçerli Kişi Güvenlik Belgesi tanzim edilir.

b. Beş yıl sonunda yenilenmesi talep edilecek Kişi Güvenlik Belgesi için altı ay önceden yenileme talebinde bulunulur. Yenilemede de ilk başvuru gibi bütün işlemler aynen tekrar edilir. Savunma Sanayii Millî Güvenlik Makamınca, yenileme süreci başlatılan, süresi dolan Kişi Güvenlik Belgesi yenisi tanzim edilene kadar kullanıma devam edilir.

c. Kuruluşlarca süresi dolan Kişi Güvenlik Belgesinin yenilenmemesi durumunda ise belgenin süresinin bitimini müteakip en geç 15 gün içinde Savunma Sanayii Millî Güvenlik Makamına iade edilir.

ç. ÇOK GİZLİ gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz etmelerine izin verilecek Türkiye Cumhuriyeti vatandaşlarının söz konusu gizlilik derecesine uygun olarak Kişi Güvenlik Belgesi ile belgelendirilmesi, Proje Makamlarının oluru ve teklifi çerçevesinde Savunma Sanayii Millî Güvenlik Makamı yetkisindedir.

d. Kuruluş yetkilisince, Savunma Sanayii Millî Güvenlik Makamınca Kişi Güvenlik Belgesi tanzim edilip kuruluşa gönderilmesini müteakip, kuruluş tarafından, EK-H'de yer alan beyanname, Kişi Güvenlik Belgesi verilen şahıslara asgari olarak büyük harfle yazılmış kısımları elle yazdırılarak imzalatılır ve kuruluş tarafından onaylanır. Beyannameler, kuruluş tarafından muhafaza edilir.

e. Kişi Güvenlik Belgesi süresi dolmadan ayrılan kişinin, bir başka kuruluşta çalışması ve kuruluşun anılan personel için yeni kuruluşta başladığı tarihten itibaren iki ay içinde kalan süreyi kullanmak üzere talepte bulunması halinde Adli Sicil Belgesi, nüfus cüzdanının arkalı önlü fotokopisi ve adli sicil kaydının da uygun olması durumunda, yeni bir soruşturma yapılmaksızın, Kişi Güvenlik Belgesini, kalan süre kadar yeni kuruluş üzerinden kullandırmaya Savunma Sanayii Millî Güvenlik Makamı yetkilidir.

f. Kişi Güvenlik Belgesi, kimlik kartı yerine kullanılamaz, Kuruluş Güvenlik Koordinatörü tarafından Kontrollü Odada muhafaza edilir. Gizlilik dereceli bilgi, belge ve malzemenin bulunduğu Kontrollü Oda ve gizlilik dereceli proje çalışmalarının yürütüldüğü Kontrollü Bölgelere veya gizlilik dereceli yerlere girecek ve ilgili makamlar tarafından düzenlenen toplantı, brifing, demonstrasyon vs. gibi gizlilik dereceli faaliyetlere katılacak personelden talep edilmesi durumunda, Kuruluş Güvenlik Koordinatörü tarafından ilgili personele zimmet karşılığı belirli süreyle Kişi Güvenlik Belgesi teslim edilebilir.

g. Kişi Güvenlik Belgesinin geçerlilik süresi içinde evlilik ve boşanma nedeniyle olabilecek soyadı değişikliklerinde, Güvenlik Koordinatörünce Makama yazılı olarak bilgi verilir.

ğ. Kişi Güvenlik Belgeleri, Tesis Güvenlik Belgesinin gizlilik derecesi seviyesinden daha üst seviyede gizlilik derecesinde tanzim edilmez. Kişi Güvenlik Belgesinin gizlilik derecesi seviyesi Tesis Güvenlik Belgesinin eşiti ve/veya alt seviyesinde tanzim edilebilir. Özel durumlarda Savunma Sanayii Millî Güvenlik Makamı yetkilidir.

h. Makamca Kişi Güvenlik Belgesi tanzim edilen kuruluş personelinin daimi giriş kartına, Tesis Güvenlik Koordinatörü tarafından Güvenlik Belgesinin gizlilik derecesi ve geçerlilik tarihi bilgilerinin işlenmesi veya bandrol/etiket şeklinde yapıştırılması sağlanır.

4. KİŞİ GÜVENLİK BELGESİ VERİLMEYECEK HÂLLER:

a. Durumları aşağıdaki bentlere uyanlara Kişi Güvenlik Belgesi verilmez.

(1) Kasıtlı bir suç nedeniyle bir yıl veya daha fazla süreli hapis cezası alanlarla, cezası ya da mahkûmiyeti ertelenmiş, seçenek yaptırımlara çevrilmiş veya affa uğramış olsa bile; cinsel dokunulmazlığa karşı suçlar, her türlü sahtecilik, Devletin egemenlik alametlerine ve organlarının saygınlığına karşı suçlar, Devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, milli savunmaya karşı suçlar, Devlet sırlarına karşı suçlar ve casusluk suçları ile hırsızlık, yağma, nitelikli mala zarar verme, güveni kötüye kullanma, dolandırıcılık, hileli iflas, uyuşturucu veya uyarıcı madde kullanma, kullanmak amacıyla bulundurma, kabul etme, satın alma, kullanılmasını kolaylaştırma, imal ve ticaretini yapma, fuhuş, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, zimmet, irtikâp, rüşvet, görevi kötüye kullanma, göreve ilişkin sırrın açıklanması, iftira, suç uydurma, yalan tanıklık, suçtan kaynaklanan mal varlığı değerlerini aklama, kaçakçılık, suç işlemek amacıyla örgüt kurma, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanuna muhalefet suçlarından mahkûm olanlar,

(2) Yukarıdaki bentte sayılan suçlar nedeniyle haklarında soruşturma veya kovuşturma yürütülenlerle hükmün açıklanmasının geri bırakılması kararı verilmiş olanlardan; mevcut bilgi, belge delil, görev safahatı gibi hususlar da dikkate alınarak yapılacak değerlendirme sonucunda kişi güvenlik belgesi verilmesi sakıncalıgörülenler,

(3) 5901 sayılı Türk Vatandaşlığı Kanununda belirtilen mavi kart uygulaması kapsamında olanların hakları saklı kalmak kaydıyla, Türkiye Cumhuriyeti vatandaşlığından çıkanlar veya çıkarılanlarla yabancı uyruklu olanlar,

(4) Herhangi bir sabotaj, isyan, casusluk, vatana ihanet hareketine katılanlar ve bu hareketlere katılanlara yardımda bulunanlarla, görevi olmaksızın ya da haklı bir sebebe dayanmaksızın herhangi sabotör veya casusla ya da hasım bir devletin temsilcileriyle temas kurmuş olanlar,

(5) Sır saklayamamak, akıl hastalığı, alkoliklik, unutkanlık ve sara gibi güvenliği tehlikeye düşürecek durumları tespit edilenler,

(6) Atatürk İlke ve İnkılâplarına aykırı davranışta bulunanlar.

b. Durumları (1) ve (2) numaralı bentler kapsamında değerlendirilen ve haklarındaki tereddütler giderilemeyen kişiler hakkında Bakan onayı alınır.

c. (İptal edilmiştir)

ç. (İptal edilmiştir)

(7) Millî güvenliğe tehdit oluşturduğu tespit edilen yapı, oluşum veya gruplara ya da terör örgütlerine üyelik veya iltisakın ya da bunlarla irtibatı tespit edilenler.

5. KİŞİ GÜVENLİK BELGESİ KAYITLARI:

Kuruluşlarca, gizlilik dereceli projede görev alan personel ile ilgili kayıtlar tutulur. Bu kayıtlar, Savunma Sanayii Millî Güvenlik Makamınca planlı veya plansız olarak gerek görüldükçe gözden geçirilir. Savunma Sanayii Millî Güvenlik Makamınca bir şahsın gizlilik dereceli görevde çalışmasının güvenlik açısından uygun olmadığı yönünde bir duyum alındığı takdirde o şahsın güvenlik tahkikatı yeniden, yaptırılabilir.

6. KİŞİ GÜVENLİK BELGESİNİN İPTALİ:

a. Kişi Güvenlik Belgesinin iptalini gerektiren hususlar aşağıda belirtilmiştir:

(1) Kişi Güvenlik Belgesinin kaybedildiğine ilişkin hususun, Kişi Güvenlik Belgesinin hükümsüzlüğüne ilişkin olarak ülke genelinde yayınlanan tirajı yüksek üç gazeteden birinde yer alan ilan ve kaybetme gerekçeleri ve kuruluş tarafından tutulacak tutanak ile birlikte Savunma Sanayii Millî Güvenlik Makamına bildirilmesi,

(2) Savunma Sanayii Millî Güvenlik Makamı tarafından, Kişi Güvenlik Belgesi bulunan personel hakkında, belgenin geçerlilik süresi içinde yaptırılacak güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlanması,

(3) Kişi Güvenlik Belgesi verilmesi için aranan şartlardan herhangi birini sağlamadığının sonradan anlaşılması veya bu şartlardan birinin sonradan kaybedilmesi,

(4) (İptal edilmiştir)

(5) Kişi Güvenlik Belgesi verilmiş bir şahsın, bu belgenin verilmesini takiben güvenlik ile ilgili usul ve kurallara uymadığına yönelik olarak kuruluş tarafından, Savunma Sanayii Millî Güvenlik Makamına bilgi verilmesi,

(6) Kişi Güvenlik Belgesi verilen akademisyen personelin görev aldığı projenin bittiğine ilişkin Proje Makamınca geri bildirim sağlanması ve personelin, çalıştığı kuruluştan veya Kişi Güvenlik Belgesi almasını gerektiren görevinden ayrılması,

(7) Kuruluşta görevli Kişi Güvenlik Belgesi sahibi personelin tamamını kapsayacak şekilde, kuruluşa ait Tesis Güvenlik Belgesinin ve/veya Üretim İzin Belgesinin iptal edilmesi,

(8) Kişi Güvenlik Belgesinin süresinin dolması ve zamanında yenileme talebinde bulunulmaması halinde personele verilmiş Kişi Güvenlik Belgesi iptaledilir.

b. Kişi Güvenlik Belgesinin gizlilik derecesi seviyesinin indirilmesi, yükseltilmesi veya Kişi Güvenlik Belgesinin iptali, Proje Makamı veya kuruluş tarafından talep edilebilir. Ancak belgenin seviyesinin değiştirilmesi ve iptali, Savunma Sanayii Millî Güvenlik Makamınca yapılacak değerlendirme sonucuna göre yapılır.

c. Kişi Güvenlik Belgesi ile ilgili hususların Bilmesi Gereken Prensibi çerçevesinde uygulanmasından ve yürütülmesinden Kuruluş Üst Yöneticisi ile birlikte Kuruluş Güvenlik Koordinatörü Savunma Sanayii Millî Güvenlik Makamına karşı sorumludur. Savunma Sanayii Millî Güvenlik Makamı tarafından görevlendirilen Denetim Heyetince yapılacak tüm haberli veya habersiz denetimlerde bu hususlar yerinde incelenir.

ALTINCI BÖLÜM
TESİS GÜVENLİK BELGELERİ

1. GENEL:

a. 5202 sayılı Kanunun 6'ncı maddesinde "Makamdan; gizlilik dereceli bilgi, belge, proje veya malzemeye nüfuzu gerektiren savunma sanayii konuları ile ilgisi olan her kişi için Kişi Güvenlik Belgesi ve projenin uygulanacağı tesis veya yer için de Tesis Güvenlik Belgesi alınması zorunludur. Bu belgeler temin edilmeden, ilgililere, gizlilik dereceli bilgi, belge, proje veya malzeme açıklanamaz ve verilemez; bunların bulunduğu yerlere ve tesislere girilemez; gizlilik dereceli bilgi ihtiva eden anlaşma, sözleşme veya alt sözleşme çalışmalarına ve uygulamalarına iştirak edilemez." ifadesi mevcuttur.

b. 5202 sayılı Kanun kapsamında, Savunma Sanayii Millî Güvenlik Makamınca yapılan belgelendirmenin amacı, her türlü casusluk, sabotaj, baskın, yıkıcı faaliyet, hırsızlık, yangın, iş kazalarına karşı tesis, personel, bilgi, doküman, araç, gereç, makine güvenliğini sağlamak, gizlilik dereceli bilgi, belge ve malzemeye yetkisiz şahısların ulaşmasını engellemek, proje çalışmaları için güvenilir bir ortam hazırlamaktır.

c. Yürürlükte bulunan NATO Güvenlik Talimatı, NATO ile ilgili faaliyet gösteren kurum ve kuruluşların, Tesis Güvenlik Belgesi almak zorunda olduklarınıbelirtmektedir.

ç. Tesis Güvenlik Belgesi, savunma sanayii güvenliği uygulamaları bakımından gerçek veya tüzel bir kişiye ait bir tesisin, belgede belirtilen gizlilik derecesine uygun durumda olduğunu gösteren idarî bir tespit niteliğinde olup, kuruluşun talebi üzerine ve sadece Türkiye Cumhuriyeti sınırları içinde mal ve hizmet üretmek üzere ve Türkiye Cumhuriyeti şirketler hukuku mevzuatına uygun olarak kurulmuş, Savunma Sanayii Millî Güvenlik Makamınca aranan şartları sağlayan kuruluşlar için tanzim edilir.

d. Belgenin gizlilik derecesi, diğer istek ve özelliklerin yanı sıra, kuruluşun millî veya yabancı ortaklı oluşu da dikkate alınarak belirlenir.

e. Yabancı ortaklı veya yönetim kurulu başkanı ile üyelerinin bir veya birkaçı yabancı uyruklu olan kuruluşlara, Denetim Heyetince yapılacak denetim sonucunun uygun olması durumunda Savunma Sanayii Millî Güvenlik Makamı tarafından sadece MİLLÎ HİZMETE ÖZEL gizlilik dereceli Tesis Güvenlik Belgesi verilir.

f. Yabancı ortak veya yönetim kurulu başkanı, üyeleri ile diğer yöneticilerin NATO üyesi ülke mensubu olması durumunda, personelin ülkesinden alınmış uygun gizlilik dereceli Kişi Güvenlik Belgesinin bulunması ve Denetim Heyetince yapılacak denetim sonucunun uygun olması durumunda, Millî Güvenlik Makamınca MİLLÎ HİZMETE ÖZEL Tesis Güvenlik Belgesi ve/veya Kuzey Atlantik Andlaşması Teşkilâtı Merkez Kurulu Başkanlığınca NATO gizlilik dereceli Tesis Güvenlik Belgesi verilir. Yabancı olan ortak veya yönetim kurulu başkanı, üyeleri ile diğer yöneticilerin NATO üyesi olmayan ülke mensubu olması durumunda NATO TGB verilip verilemeyeceğine Dışişleri Bakanlığınca karar verilir. MİLLÎ belge için görüşü alınır.

g. İlk defa olarak kuruluşlara Millî ve/veya NATO gizlilik dereceli Tesis Güvenlik Belgesi verilebilmesi için; şahıs şirketi statüsünde olan kuruluşların hissedarlarının tamamı, anonim şirket statüsünde olan kuruluşların ise ortaklarından, gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz etmesine yönetim kurulu kararı ile izin verilen hissedarlar ile bu şirketlerin yönetim kurulu üyeleri, genel müdür ve genel müdür yardımcıları, güvenlik koordinatörü ile gizlilik dereceli bilgi, belge ve malzemeye nüfuz etmesi muhtemel personeli için yaptırılacak güvenlik soruşturması ve arşiv araştırmasının olumlu sonuçlanması zorunludur.

ğ. Tesis Güvenlik Belgesinin geçerlilik süresi beş yıldır. Tesis Güvenlik Belgesinin süresi dolduğunda (ve varsa süre uzatımı sonunda) geçerliliği sona erer. Tesis Güvenlik Belgesi sadece, verildiği adreste yer alan tesisler için geçerlidir.

h. Kişi Güvenlik Belgesi başvurusunda bulunmayan kuruluşlar, Tesis Güvenlik Belgesi başvurusu da yapamaz.

ı. Tesis Güvenlik Belgesinin süre bitiminin sonunda yenilenmesi maksadıyla altı ay önceden, 5202 sayılı Yönetmeliğin 21'inci maddesinde yer alan bilgi ve belgelerle Savunma Sanayii Millî Güvenlik Makamına başvuruda bulunulur.

i. Talep edilen, savunma sanayii, ticarî ve inşaat firmalarına ait NATO gizlilik dereceli Tesis Güvenlik Belgelerine ait işlemler, Kuzey Atlantik Antlaşması Teşkilâtı Merkez Kurulu Başkanlığı adına Savunma Sanayii Millî Güvenlik Makamınca yürütülür.

j. Tesis Güvenlik Belgesi başvurusu kapsamında;

(1) Firma dosyası ile Tesis Özel Güvenlik El Kitabının ve tesislerinin incelenmesi için ön inceleme ücreti olan 3000 TL ücretin,

(2) Yapılan inceleme ve denetlemeler sonunda, Tesis Güvenlik Belgesi verilmesi uygun bulunduğu takdirde; belgelendirme ücreti olan 6000 TL'yi,

(3) Tesis Güvenlik Belgesi verilmesi uygun bulunmadığı takdirde; denetim eksikliklerin tamamlanması durumunda ikinci denetimin yapılabilmesi için j.(1) maddesinde 3000 TL inceleme ücretini Millî Savunma Bakanlığı Merkez Saymanlık Müdürlüğünün ilgili hesabına yatırır ve makbuzun bir suretini, Savunma Sanayii Millî Güvenlik Makamına gönderir.

(4) j (1), j (2) ve j (3) maddesinde belirtilen ücretler takvim yılı başından geçerli olmak üzere her yıl bir önceki yıla ilişkin olarak 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerleme oranında artırılarak uygulanır. İlgili hesap numarası ve güncel ücretler Millî Savunma Bakanlığı'nın resmî internet sayfasında yayımlanır.

2. TESİS GÜVENLİK BELGESİ İÇİN BAŞVURU:

a. 5201 sayılı Kanun gereğince yayımlanan Kontrole Tâbi Liste kapsamında faaliyet göstermek isteyen kuruluşlar ile bu Yönergede tanımlı Gizlilik Dereceli projelerde yer almak isteyen kuruluşlarca; ofisleri, iş yerleri veya tesisleri için Tesis Güvenlik Belgesi düzenlenebilmesi amacıyla, EK-İ'de yer alan bir yazı ile Savunma Sanayii Millî Güvenlik Makamına başvuruda bulunulur.

b. Kuruluş tarafından; Tesis Güvenlik Belgesi talebinde bulunma amacı, talepte bulunulan Tesis Güvenlik Belgesinin gizlilik derecesi ve faaliyette bulunulacak tesisin fizikî yerleşim durumu belirtilerek, aşağıdaki bilgi ve belgelerden oluşan dosya ile Savunma Sanayii Millî Güvenlik Makamına başvuru yapılır.

(1) Tesis Güvenlik Belgesi talep edilen tesiste, 10 Haziran 2004 tarihli ve 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun kapsamında özel güvenlik teşkilatı oluşturulmasına izin verildiğini gösterir belge ile birlikte, Özel Güvenlik Teşkilatı İl Koordinasyon Kurulu Kararının onaylı fotokopisi, özel güvenlik firmasından özel güvenlik hizmeti alınıyorsa firma ile yapılan hizmet sözleşmesinin fotokopisi,

(2) Tesiste savunma sanayii güvenliğinin sağlanmasına yönelik uygulamaları içeren, alt maddelerde belirtilen bölümlerden oluşan ve kuruluş tarafından kendi tesislerine özgü hazırlanan iki adet Tesis Özel Güvenlik El Kitabı,

(a) Kuruluş Tanıtım Bölümü

(I) Kuruluş adı

(II) Tesis Güvenlik Belgesi talep edilen tesisin açık adresi

(III) Kuruluşun hissedarları, hisse oranları, yönetim kurulu başkanı ve üyeleri ile şirketi temsil ve ilzama yetkili kişi bilgileri

(IV) Kuruluşu temsil ve ilzama yetkili kişileri ile Kuruluş Güvenlik Koordinatörünün imza sirkülerinin onaylı sureti

(V) Kuruluşun hissedarları, yönetim kurulu başkanı ve üyeleri ile şirketi temsil ve ilzama yetkili kişileri gösteren güncel tarihli Ticaret Sicili Gazetesi'nin onaylı sureti

(VI) Kuruluş güvenlik koordinatörü kimlik ve iletişim bilgileri

(VII) Kuruluş Güvenlik Koordinatörü yetkileri

(b) Fiziki Güvenlik Bölümü

(I) Çevre Güvenlik

(II) Giriş-Çıkış Güvenlik

(III) Kontrollü Bölge Güvenlik

(IV) Tesis Fiziki Emniyet Tedbirlerini Gösterir Kroki

(c) Yangın Güvenlik Bölümü

(I) Yangın Emniyet Sistemi

(II) Yangın Emniyet Tedbirlerini Gösterir Kroki

(ç) Bilgi Güvenlik Bölümü

(I) Evrak Güvenlik

(II) Toplantı Güvenlik

(III) Malzeme Güvenlik

(IV) Elektronik Bilgi Güvenlik

(V) Kurye Güvenlik

(d) Denetlemeye Esas Kontrol Formu Bölümü

(3) (İptal edilmiştir.)

(4) (İptal edilmiştir.)

(5) (İptal edilmiştir.)

(6) EK-J'de yer alan, Millî ve/veya NATO gizlilik dereceli Tesis Güvenlik Belgesi verilebilmesi ve belgelendirmeyi müteakip Savunma Sanayii Millî Güvenlik Makamı ve kuruluş tarafından yerine getirilmesi gerekli hususları içeren, Savunma Sanayii Millî Güvenlik Makamı tarafından 30 Mayıs 1985 tarihli ve 3212 sayılı Kanun ve savunma sanayii güvenliği ile ilgili mevzuata göre hazırlanan ve şirketi temsil ve ilzama yetkili kişi tarafından başlığında gizlilik derecesi belirtilerek hazırlanıp imzalanmış iki/ikişer adet protokolsureti,

(7) Millî ve/veya NATO gizlilik dereceli Tesis Güvenlik Belgesi ile ilgili olarak hazırlanan protokolde belirtilen ön inceleme ücretinin talep edilen her bir belge için ayrı ayrı Millî Savunma Bakanlığı Merkez Saymanlık Müdürlüğünün ilgili hesabına yatırıldığını gösterir makbuz/makbuzların sureti,

(8) (İptal edilmiştir.)

3. TESİS GÜVENLİK BELGESİ İÇİN ARANAN İSTEK VE ÖZELLİKLER:

a. Kuruluş Tesis Güvenlik Sisteminde bu yönergede belirtilen hususlar dışında, teknolojik gelişmelerden yararlanılarak geliştirilmiş daha üstün bir koruma sağlayan yeni bir yöntemle karşılaşılması durumunda bu durum denetlemeyi yapan heyet tarafından hazırlanan sonuç raporunda belirtilir ve Savunma Sanayii Millî Güvenlik Makamı inisiyatifiyle uygulanabilir.

b. 5188 Sayılı Kanun hükümlerine uygun olarak Kuruluş tesisinin silahlı ve silahsız korunması hususunda İl Güvenlik Koordinasyon kurulunun vereceği karargeçerlidir.

c. Belgelendirme veya kontrol maksadıyla yapılacak denetlemelerde Tesis Özel Güvenlik El Kitabı (TÖGEK)'nda yer alan ve kuruluşun faaliyet alanına, büyüklüğüne göre aşağıda belirtilen esaslar dahilinde hazırlanmış güvenlik tedbirleri, TÖGEK'te yer alan kontrol formuna göre tetkik edilir.

ç. Fizikî Güvenlik: TÖGEK'te yer alan önlemler, tesise izinsiz girişleri önleyecek nitelikte caydırıcı ve engelleyici ve uygulanabilir, kontrol edilebilir özellikte tedbirler (çit, duvar, parmaklık, kamera, güvenlik elemanı, elektronik tedbirler, araç giriş çıkış kontrolü vb.) içermelidir.

(1) (İptal edilmiştir).
(2) (İptal edilmiştir).
(3) (İptal edilmiştir).
(4) (İptal edilmiştir).
(5) (İptal edilmiştir).
(6) (İptal edilmiştir).
(7) (İptal edilmiştir).
(8) (İptal edilmiştir).
(9) (İptal edilmiştir).
(10) (İptal edilmiştir).
(11) (İptal edilmiştir).
(12) (İptal edilmiştir).
(13) (İptal edilmiştir).
(14) (İptal edilmiştir)
(15) (İptal edilmiştir)
(16) (İptal edilmiştir)
(17) (İptal edilmiştir).
(18) (İptal edilmiştir).
(19) (İptal edilmiştir).
(20) (İptal edilmiştir).
(21) (İptal edilmiştir).
(22) (İptal edilmiştir).

(23) Kuruluşun Tesis Güvenlik Sistemi bu yönergede belirtilen tüm güvenlik sistem elemanlarını ihtiva edecek şekilde, tepe yönetici ve Güvenlik Koordinatörü sevk ve idaresinde oluşturulmalı ve alınan önlemler ile güvenliğe yönelik uygulama esasları Tesis Özel Güvenlik El Kitabında (TÖGEK) tanımlanmalıdır.

d. *Yangın Güvenlik:* TÖGEK'te yer alan önlemler, tesiste yangın riskini önleyecek, yangın çıkması durumunda yayılmadan önlenmesini sağlayacak, kritik malzemeleri ve belgeleri ortamdan uzaklaştıracak uygulanabilir, kontrol edilebilir özellikte tedbirler, yöntemler (yangın söndürme uyarı cihazları / sistemleri, patlayıcı / parlayıcı / yanıcı malzemelerin kontrolü,vb.) içermelidir.

(1) (İptal edilmiştir).
(2) (İptal edilmiştir).
(3) (İptal edilmiştir).
(4) (İptal edilmiştir).
(5) (İptal edilmiştir).
(6) (İptal edilmiştir).
(7) (İptal edilmiştir).

e. *Bilgi Güvenlik:* TÖGEK'te yer alan önlemler, gerek kuruluş yetkili personelinin gerekse kuruluş dışı ilgili personelinin bilgi güvenliği konusunda uyması gereken yöntemleri, bilgi ve belgelerin güvence altına alınması, kayıt alınması vb. uygulanabilir, kontrol edilebilir özellikte tedbirler, yöntemler (ziyaretçi/katılımcıların güvenlik kleranslarının kontrol edilmesi, toplantı katılım formunun tutulması, ortam güvenliğinin sağlanması, gizlilik dereceli evrakın çoğaltılmasının kayıtlı ve kontrollü yapılması. vb.) içermelidir.

(1) (İptal edilmiştir).
(2) (İptal edilmiştir).
(3) (İptal edilmiştir).
(4) (İptal edilmiştir).
(5) (İptal edilmiştir).
(6) (İptal edilmiştir).

f. (İptal edilmiştir).

(1) (İptal edilmiştir).
(2) (İptal edilmiştir).
(3) (İptal edilmiştir).

g. (İptal edilmiştir).

(1) Gelen ve giden evrak, MİLLÎ ve NATO olacak şekilde farklı kayıt sistemlerinde ayrı ayrı numaralandırma yöntemiyle kayıt altına alınmalı, ÖZEL ve üzeri gizlilik dereceli evrak ve dokümanların Kontrollü Odada, HİZMETE ÖZEL evrak ve dokümanların ise kontrollü bölge içinde çiftkilitli dolaplarda muhafaza edilmesi sağlanmalıdır.

(2) Gelen evraka, gizlilik derecesine uygun işlem yapılmalı ve bu evraka istinaden yapılacak yazışmalarda aynı gizlilik derecesi korunmalıdır.

(3) Şirket/kuruluş tarafından başlatılabilecek bir proje veya hazırlanacak yazı için uygun bir gizlilik derecesi verilmelidir.

(4) Gizlilik dereceli bilgi ihtiva eden evrak üzerine gizlilik derecesi işaretlenmelidir.

(5) Gizlilik dereceli evrakın çoğaltılması önlenmeli, zorunlu hâllerde belirlenen prosedürler çerçevesinde işlem yapılmalıdır.

(6) Gizlilik dereceli bilgi ve malzeme transferi gerektiğinde öncelikle Proje ve Savunma Sanayii Millî Güvenlik Makamından izin alınmalı ve transfer özel önlemler alınarak gerçekleştirilmelidir.

(7) Kurye hizmetleri için özel talimatlar hazırlanmalı ve kurye olarak görevlendirilecek personel için, uygun gizlilik dereceli Kişi Güvenlik Belgesi alınmalıdır. Kişi Güvenlik Belgeli kurye/kuryeler Makama bildirilmelidir.

(8) Gizlilik dereceli evraklar imha edilirken imha tutanağı tutulmalı ve bu tutanak muhafaza edilmelidir.

ğ. Kontrollü Bölge Güvenliği İçin Alınacak Önlemler:

(1) Gizlilik dereceli proje çalışmalarının yapıldığı bölümler, kontrollü malzemelerin bulunduğu depolar ile anılan malzemelerin üretildiği alanlar için, yetkisiz kişilerin girişine engel olacak fizikî önlemler alınmalıdır.

(2) Giriş bölgelerine girilmez işaretleri asılmalıdır.
(3) Giriş ve çıkışlar kayıt ve kontrol altına alınmalıdır.
(4) Elektronik ve sair iletişim imkânları ile nüfuz edilmesine karşı tedbir alınmalıdır.
(5) Kontrollü bölge çalışma talimatları oluşturulmalı ve personele duyurulmalıdır.

h. Kontrollü Oda Güvenliği İçin Alınacak Önlemler:

MİLLÎ/NATO ÇOK GİZLİ, GİZLİ ve ÖZEL gizlilik dereceli evrak ve doküman ile diğer materyalin muhafazası için aşağıda belirtilen özelliklere sahip bir kontrollü oda hazırlanmalıdır:

(1) Giriş kapısında en az iki kilit sistemi bulunmalı, çelik kapılı olmalı ve odaya girmek için yetkilendirilmiş personel belirlenmelidir.

(2) (İptal edilmiştir).

(3) Varsa pencereler, sızmayı önleyecek sıklık ve mukavemette demir parmaklıklarla donatılmalıdır.

(4) Dolap ve dosyalar, NATO ve MİLLÎ gizlilik dereceli doküman için ayrı ayrı işaretlenmelidir.

(5) (İptal edilmiştir).

(6) (İptal edilmiştir).

(7) (İptal edilmiştir).

(8) Kontrollü oda ve bölgelere girmeye yetkili Kişi Güvenlik Belgesine sahip şahıslar için resimli imza örnekli personel tanıtım kartları hazırlanarak kapı girişlerine asılmalıdır.

ı. Bilgisayar ve Bilgi Güvenliği İçin Alınacak Önlemler:

Özel ve üzeri gizlilik dereceli askerî ve/veya ulusal güvenlik amaçlı yazılım üretenler ile en az ÖZEL gizlilik dereceli bilgi üreten, bu bilgi ile çalışan veya elektronik ortamda depolayan kuruluşlar tarafından, bilginin üretildiği ve depolandığı bilgi sistem odalarında ve bilgisayar sistemlerinde kullanılan, enerji iletim, iletişim ve veri hatlarına dışarıdan müdahaleye ve bilgi sızmasına engel olacak güvenlik tedbirleri alınır. Bu sistemlere yönelik TEMPEST koruması sağlanır. TEMPEST korumasının sağlanmasına yönelik alınan tedbirler, akredite kuruluşlarca belgelendirilir ve alınan belge, kuruluş tarafından Savunma Sanayii Millî Güvenlik Makamına gönderilir. Ayrıca aşağıdaki tedbirler alınır.

(1) Otomatik bilgi işlem sistemlerinin kullanılacağı ortamın fizikî ve elektronik güvenliği sağlanmalı ve bu ortam, casuslukların ve dışarıya sızmaların önlenmesi için emniyet çemberi ile çevrilmeli ve kontrollü giriş-çıkış yapılmalıdır.

(2) Otomatik bilgi işlem merkezi, elektronik dinlemeye karşı bir tedbir olarak, binanın veya kontrol altındaki sahanın mümkün olduğu kadar ortasına yakın bir yere kurulmalıdır. Gizlilik dereceli bilgi bulunan sunucu ile diğer sunucu ve elektronik cihazlar arasında en az bir metre, kablolar arasında ise en az 15 cm mesafe bulunmalıdır.

(3) Otomatik bilgi işlem sisteminde, kullanıcı işlemleri ile yönetim işlemleri birbirinden kesin olarak ayrı olmalıdır.

(4) Sistemin yönetim ve kontrol yazılımı, kullanıcılara sadece ihtiyaç duydukları imkânları sağlayacak şekilde kontrol edilebilir olmalıdır.

(5) Otomatik bilgi işlem birimlerinde çalışacak personel, uygun gizlilik dereceli Kişi Güvenlik Belgesine sahip şahıslar olmalı, bilgi işlem birimi ile sunucu mahalleri Kontrollü Bölge olmalıdır.

(6) Bilgisayarlar, bilgiye erişmek isteyen kullanıcının yetkili olup olmadığını test edecek şekilde programlanmalı, bu durumun sistem tarafından kontrolü sağlanmalıdır. Sistem üzerinde kullanıcıların kullanacakları alanlar için yetkilendirme yapılmalıdır.

(7) Merkezi bilgisayar sisteminin tek bir yetkilinin kontrolüne bırakılması önlenmelidir.

(8) Otomatik bilgi işlem birimlerine yetkisiz kişilerin girişini engelleyecek güvenlik tedbirleri alınmalı, bu birimlere girmesi gerekenler için güvenlik koordinatöründen izin alınmalıdır.

(9) Bilgisayarlarda kullanıcıların yetki ve sorumluluklarının yer aldığı bilgisayar kullanma talimatı oluşturulmalıdır.

(10) Yedekleme (back-up) yapılmalı ve kayıtlar saklanmalıdır.

(11) Sistem ve kullanıcılara ait kayıtlar (log) tutulmalı ve kayıtlara yapılan işlemler tanımlanmalıdır.

(12) Disket, harici disk, CD, flash bellek vb. yardımcı bilgi depolama araçlarının kuruluş içinde kullanımıile kuruluş dışına çıkarılmasına yönelik önlemler alınmalıdır.

(13) Tesisteki internet bilgisayarları için ayrı bir ağ kurulmalı, gizlilik dereceli bilgi bulunan ve üzerinde gizlilik dereceli (Hizmete Özel hariç) çalışma yapılan bilgisayarların internet bağlantısı engellenmeli, tesiste kablosuz intranet erişimi bulunmamalıdır. Kuruluşun yerel internet ağındaki Hizmete Özel gizlilik dereceli bilgiye yönelik olarak; Kişi Güvenlik Belgesine sahip ve bilmesi gereken prensibi dâhilinde konuyla ilgili kuruluş çalışanları; internet üzerinden kuruluş tarafından oluşturulacak Milli Sanal Özel Ağ (Virtual Private Network - VPN) vasıtasıyla ve Milli Elektronik Sertifika ile kimlik doğrulaması yapılarak, kuruluş içerisindeki Hizmete Özel gizlilik dereceli bilgiye uzaktan erişebilir veya işleyebilir. Söz konusu uzaktan erişim sistemine yönelik alınan tedbirlerin uygun olup olmadığı ve en az EK-T'de belirtilen güvenlik esaslarını sağladığı hususunda TÜBİTAK BİLGEM Başkanlığınca düzenlenecek belge/rapor, Milli Savunma Bakanlığı Muhabere ve Bilgi Sistemleri Dairesi Başkanlığının onayını müteakip Kuruluş tarafından Savunma Sanayii Millî Güvenlik Makamına gönderilir. Uzaktan erişim altyapısı en az EK-T'de sunulan güvenlik esaslarına uygun olmalıdır.

(14) İnternet ortamından alınan bilgilerin virüs kontrolleri yapılmalıdır.

(15) Üzerinde gizlilik dereceli bilgi bulunan CD, DVD, taşınabilir bilgisayar, flash bellek vb. bilgi depolama aygıtları Kontrollü Bölge dışındaki bilgisayarlarda kullanılmamalıdır.

4. TESİS GÜVENLİK BELGESİ VERİLMESİ:

a. Savunma Sanayii Millî Güvenlik Makamınca, başvuru bilgi ve belgelerinin alınmasını müteakip yapılan inceleme sonucunda, varsa belirlenen eksiklikler kuruluşa bildirilir. Savunma Sanayii Millî Güvenlik Makamı tarafından başvuru dokümanında belirlenen eksiklikleri üç ay içinde gidermeyen veya altı aya kadar verilebilen ek süreyi talep etmeyen kuruluşun başvurusu iptal edilir ve kuruluşa bilgi verilir.

b. Yapılan inceleme sonucunda herhangi bir olumsuzluk veya eksiklik olmadığının belirlenmesini müteakip kuruluşa ait tesis, Savunma Sanayii Millî Güvenlik Makamı tarafından yapılacak planlamaya uygun bir tarihte Denetim Heyetincedenetlenir.

c. Tesiste yapılan denetimde; Savunma Sanayii Millî Güvenlik Makamı tarafından belirlenen denetim kriterlerinin sağlanıp sağlanmadığı, Kuruluş tarafından hazırlanan Tesis Özel Güvenlik El Kitabında yer alan hususların uygulanıp uygulanmadığının kontrolü yapılarak, denetim raporu tanzim edilir.

ç. Denetim raporunun olumlu olması durumunda; kuruluş tarafından hazırlanan ve Savunma Sanayii Millî Güvenlik Makamı tarafından onaylanan Tesis Özel Güvenlik El Kitabı ile Savunma Sanayii Millî Güvenlik Makamı tarafından tanzim edilen Tesis Güvenlik Belgesi kuruluşa gönderilir.

d. NATO gizlilik dereceli Tesis Güvenlik Belgesi için, Denetim Heyetince yapılan denetim sonucu tanzim edilen denetim raporunun olumlu olması durumunda, Kuzey Atlantik Andlaşması Teşkilatı Merkez Kurulu Başkanlığına denetim raporu gönderilerek bilgi verilir. Kuzey Atlantik Andlaşması Teşkilatı Merkez Kurulu Başkanlığı tarafından, NATO gizlilik dereceli Tesis Güvenlik Belgesi tanzim edilerek ilgili kuruluşa gönderilir ve Savunma Sanayii Millî Güvenlik Makamına bilgi verilir.

e. Denetim sonucunun olumsuz olması durumunda; kuruluşa ait tesiste yapılan denetimde tespit edilen ve denetim raporunda belirtilen eksiklikler, yazılı olarak kuruluşa bildirilir ve belirtilen eksikliklerin tamamlanması için kuruluşa altı aya kadar süre verilir. Kuruluş tarafından, denetim esnasında tespit edilen eksikliklerin tamamlandığının yazılı olarak Savunma Sanayii Millî Güvenlik Makamına bildirilmesini müteakip, tesis, Savunma Sanayii Millî Güvenlik Makamınca yapılacak planlamaya uygun bir tarihte ikinci kez Denetim Heyetince denetlenir. İkinci kez yapılan denetim sonucunun olumlu olması durumunda; bu fıkranın ç. ve d. bentlerinde düzenlenen hükümler çerçevesinde gerekli işlemler yapılır.

f. İlk denetim sonucunda tespit edilen ve yazılı olarak kuruluşa bildirilen eksikliklerin, kuruluş tarafından, Savunma Sanayii Millî Güvenlik Makamınca belirtilen süre içerisinde tamamlandığının yazılı olarak bildirilmemesi ya da tesiste yapılan ikinci denetimin de olumsuz sonuçlanması durumunda başvuru iptal edilir. Tesis Güvenlik Belgesi başvurusu iptal edilen kuruluş tarafından, altı aydan önce aynı tesis için yeniden başvuruda bulunulamaz.

g. Tesis Güvenlik Belgesi verilmesi amacıyla yapılan denetimlerde, şu hususlar araştırılır:

(1) Tesisin sahiplerinin, yönetim kurulu başkanı ve üyelerinin, genel müdür ve yardımcılarının, güvenlik koordinatörü ile gizlilik dereceli konulara nüfuz edebilecek diğer personelin Kişi Güvenlik Belgelerinin olup olmadığı.

(2) Tesis güvenlik sisteminin oluşturulması ile sevk ve idaresinden sorumlu güvenlik koordinatörünün belirlendiği, güvenlik organizasyonu ile organizasyonda görevi olan güvenlik sistemi ile bağlantılı birim ve bireylerin görev tanımlarının ve hiyerarşik ilişki düzeyinin belirlenip belirlenmediği,

(3) Tesisin yürüttüğü faaliyetler ile gizlilik dereceli bilgilere nüfuz etmeye yönelik projelerde yer alma potansiyeli çerçevesinde Tesis Güvenlik Belgesine ihtiyacı olup olmadığı.

(4) Tesisin üretim veya hizmetlerinde diğer kurum ve kuruluşlar ile ilişkisi.

(5) Gizlilik dereceli bilgilere erişim potansiyeli olan personel için Kişi Güvenlik Belgesi almak üzere müracaatın yapılıp yapılmadığı.

(6) Tesisin gizlilik dereceli bilgileri depolama (saklama), kontrollü oda ve bölge güvenliği, ziyaretler, fiziki güvenlik, bilgi güvenliği, evrak ve dokümantasyon güvenliği, toplantı güvenliği konularında izlenebilir güvenlik kayıtlarının mevcudiyeti kontrol edilir.

ğ. Denetim Heyetinin, kuruluşun almış olduğu güvenlik önlemlerini yeterli bularak rapor etmesi ve diğer şartların da uygun olması durumunda, Savunma Sanayii Millî Güvenlik Makamınca, EK-L'de yer alan Tesis Güvenlik Belgesi Türkçe ve İngilizce olarak tanzim edilir. Müteakiben Savunma Sanayii Millî Güvenlik Makamının bağlı olduğu Müsteşar Yardımcısı tarafından imzalanır. Verilen belge, iptali gerektiren bir durumla karşılaşılmadığı takdirde, beş yıl süre ile geçerlidir.

h. Tesis Güvenlik Belgesinin yenilenmesi maksadıyla Kuruluş tarafından yapılan başvuru çerçevesinde, belgenin geçerlilik tarihine kadar Savunma Sanayii Millî Güvenlik Makamınca yeniden belgelendirme işlemleri tamamlanamamış ise, kuruluşun en üst düzeyli yöneticisi tarafından güvenlik zafiyeti oluşmadığına ilişkin verilecek bir taahhütname çerçevesinde belgenin bitim tarihinden itibaren bir yıla kadar süre uzatımı verilebilir. Yeniden belgelendirme sürecinde, Savunma Sanayii Millî Güvenlik Makamınca, Kuruluşların Kişi Güvenlik Belgesi taleplerinin sonuçlanması beklenmeden denetim yapılır ve sistemin uygun bulunması durumunda belgelendirme yapılabilir.

ı. ÇOK GİZLİ gizlilik dereceli bilgi, belge, malzeme veya projeye nüfuz etmelerine izin verilecek tesislerin, söz konusu gizlilik derecesine uygun olarak Tesis Güvenlik Belgesi ile belgelendirilmesi, ilgili makamlar ile yapılacak koordinasyonu müteakip, Savunma Sanayii Millî Güvenlik Makamı yetkisindedir.

5. ARA DENETLEMELER:

a. Ara denetlemeler, Tesis Güvenlik Belgesi olan ve savunma malzemesi üreten kuruluşların güvenlik uygulamalarının, bu Yönergede belirtilen esaslara uygun olup olmadığının gözden geçirilmesi amacıyla yapılan denetlemelerdir.

b. Tesis Güvenlik Belgesi verilen kuruluş, Savunma Sanayii Millî Güvenlik Makamı tarafından yılda en az bir defa olmak üzere haberli veya habersiz ara denetime Tâbi tutulur. Yapılacak ara denetimde eksik bulunan hususlar kuruluşa yazılı olarak bildirilir. Söz konusu eksikliklerin en geç üç ay içerisinde giderilerek sonucun Savunma Sanayii Millî Güvenlik Makamına bildirilmemesi veya bildirim sonucunda yapılacak doğrulama denetiminde eksikliklerin devam ettiğinin tespit edilmesi durumunda Savunma Sanayii Millî Güvenlik Makamı tarafından, kuruluşa ait Tesis Güvenlik Belgesi iptal edilir. Kuruluş, Tesis Güvenlik Belgesi iptal edilen tesis için altı aydan önce yeniden başvuruyapamaz.

c. Tesis Güvenlik Belgesi verilen kuruluşlar, yılda en az bir defa veya Savunma Sanayii Millî Güvenlik Makamınca gerek görüldüğünde denetlenir. Tespit edilecek eksik hususlar ve alınması gereken ilave tedbirler yazılı olarak kuruluşa bildirilir.

ç. Yapılan ara denetimlerde, kuruluşlara eksikliklerini tamamlamak üzere üç ay süre verilir, en geç üç ay içerisinde eksikliklerini tamamladığını bildirmeyen veya bildirmesini müteakip yapılan denetim sonucunda eksikliklerin devam ettiği tespit edilen kuruluşların TGB'si Makam tarafından iptal edilir. Tesis Güvenlik Belgesi iptal edilen kuruluş 6 aydan önce tesis için yeniden başvuruda bulunamaz**.**

6. TESİS GÜVENLİK BELGESİNİN İPTALİ VEYA YENİDEN DÜZENLENMESİ:

a. Tesis Güvenlik Belgesi süresinin dolması durumunda; kuruluşun müracaatı ve yeniden denetleme sonrasında sistemin uygun bulunması durumunda Tesis Güvenlik Belgesi tanzim edilir.

b. Tesiste aşağıda belirtilen değişikliklerden herhangi birinin meydana gelmesi durumunda Tesis Güvenlik Belgesi iptal edilir:

(1) Kuruluşun, millî güvenlik, kamu düzeni ve genel sağlık bakımından sakınca doğuran hâllerinin tespit edilmesi veya bu durumun bir Kamu kuruluşunca tevsik edilmesi,

(2) Kuruluşa ait tesisin yerinin veya adresinin değiştirilmesi, tasfiyesi, kuruluşun iflâs etmesi veya tüzel kişiliğinin değişmesi,

(3) Savunma sanayii alanındaki herhangi bir gizlilik dereceli bilgi, belge ve malzeme ya da gizlilik dereceli projenin uygun Kişi Güvenlik Belgesi bulunmayan şahıslara ya da Tesis Güvenlik Belgesi olmayan kuruluşlara verildiğinin veya açıklandığının tespit edilmesi,

(4) Kontrole Tâbi Listede yer alan malzemenin, diğer ülkelere ya da gerçek kişilere ve özel hukuk tüzel kişilerine izinsiz olarak satışı veya bunlara ait teknoloji transferi yapıldığının tespit edilmesi,

(5) Tesiste, tesis güvenliğini etkileyen grev veya lokavt hareketleri olduğunun tespit edilmesi,

(6) Tesis Güvenlik Belgesi ile belgelendirilen tesiste, basın ve yayım organları vasıtasıyla, Savunma Sanayii Millî Güvenlik Makamının izni olmaksızın çekim ve tanıtım yapılması,

(7) Kuruluşun tüzel kişiliğinde, sermaye yapısında ve ortaklık durumunda değişiklik olması durumunda, değişikliği takip eden bir ay içinde Savunma Sanayii Millî Güvenlik Makamına bilgi verilmemesi,

(8) Kuruluşun Tesis Güvenlik Belgesi ile belgelendirilen tesisinde, bir veya birden fazla farklı tüzel kişiliğin konuşlanması ve aynı adresin farklı tüzel kişilikler ile paylaşılması. Ancak hissedar yapısının belge sahibi kuruluş ile aynı olması, fiziki olarak belge sahibi kuruluşun tesisleri içinde ayrı bölüm/binalarda konuşlanması ve Millî Güvenlik Makamının onayının alınması koşuluyla farklı bir tüzel kişilik bulunabilir.

(9) Savunma Sanayii Millî Güvenlik Makamının planlı veya plansız olarak gerçekleştirdiği denetlemelerde tesis güvenlik uygulamalarının yetersiz bulunması ve kuruluşun anılan eksiklikleri belirtilen süre içinde gidermemesi,

(10) Tesis yetkililerinin, Savunma Sanayii Millî Güvenlik Makamı tarafından önerilebilecek ilave önlemleri almakta isteksiz davranması veya istenilen süre içinde gerekli düzenlemeleri yapmaması.

c. Tesis Güvenlik Belgesinin herhangi bir nedenle iptal edilmesi durumunda; iptal edilen Tesis Güvenlik Belgesinin aslı kuruluş tarafından Savunma Sanayii Millî Güvenlik Makamına iade edilir. Tesis Güvenlik Belgesinin iptal edilmesini müteakip Savunma Sanayii Millî Güvenlik Makamı tarafından, elektronik ortamda yer alan Tesis Güvenlik Belgesine Sahip Kuruluşlar listesinde gerekli güncelleme yapılır.

ç. Tesisin isminin değişmesi durumunda veya tesisin yeri değişmemekle birlikte yerel idare tarafından yapılan düzenleme neticesi meydana gelen adres değişikliklerinde, kuruluşun müracaatı üzerine Savunma Sanayii Millî Güvenlik Makamınca denetim yapılmaksızın belge yeniden düzenlenebilir.

YEDİNCİ BÖLÜM
KONTROLE TÂBİ MALZEMENİN ÜRETİMİ

1. GENEL:

a. 5201 sayılı Kanunun 2'nci maddesinde "Bu kanun, her türlü harp araç ve gereçleri ile silah, mühimmat ve bunlara ait yedek parçalarla patlayıcı maddeleri üretmek üzere kurulan veya işletilen kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere ait kuruluşları kapsar." ifadesi mevcuttur. Bu Kanun kapsamında Kontrole Tâbi Listenin nelerden ibaret olduğu, ilgili makamlar ve kamu kurum ve kuruluşları ile koordineli olarak Savunma Sanayii Millî Güvenlik Makamınca belirlenir ve her yıl Ocak ayında Resmî Gazetede tebliğ olarakyayımlanır.

b. Kontrole Tâbi Liste kapsamında bulunan bir malzemenin üretimi için, Savunma Sanayii Millî Güvenlik Makamından Üretim İzni alınır.

c. Kurulu durumda bulunan ancak savunma sanayii alanında faaliyet göstermek üzere iş değişikliği yapmak veya alt yüklenici olarak çalışmak isteyen kuruluşlar da Savunma Sanayii Millî Güvenlik Makamından izin alırlar. Kontrole Tâbi Liste kapsamındaki malzemelerin üretimi ile ilgili olmayıp üretimi destekleyici nitelikteki hizmet üretimi kapsamına giren, malzeme taşıma, sigorta gibi üretime yardımcı faaliyetler için Üretim İzin Belgesi alınmasına gerek yoktur.

ç. Belgelendirilen kuruluşlarca, belgelendirme tarihini takip eden dönem içindeki; sermaye ve hissedarlar, faaliyet alanları, yıllık üretim cins ve miktarları, personel adedi gibi bilgilerde olabilecek değişiklikler ile Kontrole Tâbi Liste kapsamındaki ürünler için alınan siparişler, siparişin cins ve miktarları ile sipariş veren kimlikleri gibi bilgiler, Savunma Sanayii Millî Güvenlik Makamına bildirilir.

d. (İptal edilmiştir).

e. Üretim İzin Belgesi başvurusu kapsamında;

(1) Dosyanın incelenmesi ve tesisin denetlenmesi için 4000 TL'yi,

(2) Yapılan inceleme ve denetlemeler sonunda, Üretim İzin Belgesi verilmesi uygun bulunduğu takdirde; belgelendirme ücreti olan 8000 TL'yi,

(3) Üretim İzin Belgesi verilmesi uygun bulunmadığı takdirde; denetim eksikliklerin tamamlanması durumunda ikinci denetimin yapılabilmesi için e.(1) maddesinde 4000 TL inceleme ücretini Millî Savunma Bakanlığı Merkez Saymanlık Müdürlüğünün ilgili hesabına yatırır ve makbuzun bir suretini, Savunma Sanayii Millî Güvenlik Makamına gönderir.

(4) e (1), e (2) ve e (3) maddesinde belirtilen ücretler takvim yılı başından geçerli olmak üzere her yıl bir önceki yıla ilişkin olarak 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerleme oranında artırılarak uygulanır. İlgili hesap numarası ve güncel ücretler Millî Savunma Bakanlığı'nın resmî internet sayfasında yayımlanır.

2. ÜRETİM İZNİ İÇİN BAŞVURU:

a. Kontrole Tâbi Liste kapsamında üretim yapmak isteyen kuruluşlarca, EK-M'de yer alan yazı ile, bu ürünlerden hangisinin üretilmekte olduğu veya üretileceği hakkında bilgi verilerek izin talebinde bulunulur.

b. Savunma Sanayii Millî Güvenlik Makamı tarafından yapılan inceleme sonunda, üretimi planlanan malzemenin Kontrole Tâbi Liste kapsamında olduğu belirlenirse kuruluştan aşağıda belirtilen bilgi ve belgeler istenir. İzin talep eden kuruluş tarafından, aşağıda belirtilen bilgi ve belgelerden oluşan iki nüsha dosya hazırlanarak Savunma Sanayii Millî Güvenlik Makamına gönderilir. Belgelerin, yetkili kişiler tarafından onaylanmış fotokopileri de kabul edilir:

(1) EK-N'de yer alan onaylanmış Üretim İzin Belgesi protokol sureti.

(2) Protokolde belirtilen, ön inceleme ücretinin ilgili hesaba yatırıldığını gösteren makbuzun fotokopisi. (Ücretin hangi amaçla yatırıldığı makbuz üzerinde belirtilecektir.)

(3) Üretimi yapılacak olan malzemenin, yürürlükte olan "Kontrole Tâbi Liste"nin hangi maddesi ve fıkrasına dâhil olduğunu belirtir bilgi. (Bu husus başvuru yazısında da belirtilerek, talep yapılacaktır.)

(4) Tesis Güvenlik Belgesinin veya belge almak üzere yapılmış başvurunun bir sureti (üretimin yapılacağı tesise ait).

(5) Üretimin yapılacağı kamu kurum kuruluşlarıile gerçek ve tüzel kişilere ait tesisin;

(a) Ayrıntılı kurucu kimlikleri,

(b) Hissedarları ve hisse oranları, (Yabancı ortaklık varsa, hisse oranı ayrıca belirtilir.)

(c) Güncel tarihli Ticaret Sicil Gazetesinin fotokopisi.

(ç) Üretim İzin Belgesi Talep edilen adresin, işyeri ünvanı ile (şube, merkez vb. belirtilecek biçimde) birlikte yayınlandığı güncel tarihli Ticaret Sicil Gazetesi.

(d) Kuruluşun isminin veya unvanının değiştiğinin bildirilmesi hâlinde; Makam tarafından gerektiğinde tekrar yapılacak denetim veya değerlendirmeyi müteakip Üretim İzin Belgesi yeniden tanzim edilebilir.

(6) Varsa ISO ve/veya eşdeğer Kalite Sistem Belgesi.(Üretimin yapılacağı tesise ait.)

(7) Varsa TSE veya TSEK belgeleri (Üretim İzin Belgesi talep edilen ürüne/ürünlere ait).

(8) Güncel tarihli kapasite raporu (Üretim İzin Belgesi istenen malzemeleri ihtiva edecek ve üretimin yapılacağı tesise ait olacak şekilde).

(9) Sanayi ve Ticaret Bakanlığından alınan ve yıllık vizeleri yapılmış Sanayii Sicil Belgesi.

(10) 6331 sayılı İş Sağlığı ve Güvenliği Kanunu kapsamında gerekli iş sağlığı ve güvenliği tedbirlerinin alındığına dair taahhütname.

(11) Üretilecek malzeme için kullanılacak olan mamul/yarı mamul malzemenin nereden tedarik edildiğine ilişkin ayrıntılı bilgi. Üretilecek malzeme için alt yüklenici kullanılacak ise, alt yüklenicilerden alınacak malzeme veya hizmete ilişkin ayrıntılı bilgi.

(12) Üretilecek malzemenin cins ve miktarı, işaretleme yöntemi, varsa stok numaraları.

(13) Üretilecek malzemeye ait arz, talep, ithalat, ihracat, üretime ilişkin yaratılacak yurt içi katma değer, off-set öngörüleri ile varsa tespit edilen sektörel bilgiler. Lisans altında üretim veya araştırma-geliştirme yöntemlerinden hangisiyle üretim yapıldığı, üretim bilgilerine (Üretim/Teknik Bilgi Paketi) sahip olunup olunmadığı, sahip olunması hâlinde, söz konusu bilgilerin kaynağı (ARGE, Lisans, Know-how, Konsorsiyum vb.), istihdam durumu, (Çalıştırılan ve çalıştırılması muhtemel personel bilgileri-Mühendis/İşçi vb.) üretimde kullanılacak kritik alt teknolojiler, ürünün tamamı üzerinden kuruluşun yerli katkı oranı. (Üretilen ürüne ait yurt dışından tedarik edilen parça/malzeme listesi.)

(14) Üretilecek her bir malzeme için ayrı ayrı üretim akış şeması.

(15) Üretim İzin Belgesi talep edilen üründen daha önce Türk Silahlı Kuvvetleri, diğer kamu/özel kuruluşlar ile yurt dışına üretim yapılmış ise bunlar hakkında açıklayıcı bilgi. (Üretim İzin Belgesi yenileme talebinde değerlendirilecektir.)

(16) Üretim İzin Belgesi talep edilen ürünün üretileceği tesislerde, Türk Silahlı Kuvvetleri için herhangi bir konuda üretim yapılmış ise, yapılan ürünlerin cins ve miktarları hakkında bilgi. (Üretim İzin Belgesi yenileme talebinde değerlendirilir.)

c. Kişi veya kuruluş ile Savunma Sanayii Millî Güvenlik Makamının karşılıklı olarak yerine getirmeleri gereken hususları düzenleyen ve protokolde belirtilen hususlar, kuruluş yetkililerince koşulsuz kabul edilmelidir.

3. ÜRETİM İZİN BELGESİ VERİLMESİ:

a. Savunma Sanayii Millî Güvenlik Makamı tarafından, istenen bilgi ve belgelerin alınmasını müteakip ön inceleme başlatılır.

b. Yapılan inceleme sonucunda kuruluş başvurusunun işleme alınmasının kararlaştırılması durumunda Sanayi ve Ticaret Bakanlığı ile ana platformlara yönelik olarak Savunma Sanayii Müsteşarlığı ve varsa ilgili diğer makamların konuyla ilgili görüşü istenir.

c. Alınan görüşün olumlu olması durumunda, Savunma Sanayii Millî Güvenlik Makamının koordinasyonunda, Sanayi ve Ticaret Bakanlığı personelinin de katılımıyla oluşturulan bir heyet teşkil edilir ve üretim tesisleri denetlenir.

ç. Bu denetlemede, tesisin, 5202 sayılı Kanun kapsamında verilen Tesis Güvenlik Belgesi için aranan şartları taşıması gerekir. Gerektiğinde tesiste Tesis Güvenlik Belgesi ve Üretim İzin Belgesi denetimi bir arada yapılabilir. Tesiste; Kontrole Tâbi Liste kapsamında üretilecek malzemelere ilişkin üretim hatlarında kullanılan ve kapasite raporunda belirtilen teçhizat ve makina parkında bulunan makinaların tetkiki, üretimin lisans veya araştırma-geliştirme ile yapılıp yapılmadığı, tesiste üretim esnasında kritik alt sistemlerin bulunup bulunmadığı, üretimdeki yerli katkı oranlarının belirlenmesi, üretimin sürekliliğine engel olma olasılığı bulunan darboğazlar, üretim akış şeması üzerinden üretimin izlenmesi veya gelişen teknoloji doğrultusunda bilgisayar ortamında üretimi gerçekleştirilen elektronik ürünlerin veya yazılımların ve benzeri hususların kontrolü yapılır.

d. Teşkil edilen heyet tarafından, yapılan inceleme ve üretim tesislerindeki denetlemeler, MSB internet sayfasında yer alan Denetlemeye Esas Kontrol Formundaki hususlara göre yapılır ve sonuç formda belirtilir ve denetim heyetince imzalanır.

e. Hazırlanan rapor, tespit niteliğinde olup Üretim İzni verilip verilmemesine ilişkin nihaî karar, Millî Savunma Bakanına aittir. Millî Savunma Bakanının onayının alınmasını ve Savunma Sanayii Millî Güvenlik Makamı ile kuruluş arasında imzalanan protokolde belirtilen belgelendirme ücretinin Millî Savunma Bakanlığı Merkez Saymanlık Müdürlüğünün ilgili hesabına yatırıldığına dair makbuzun bir suretinin Savunma Sanayii Millî Güvenlik Makamına ibraz edilmesini müteakip, Savunma Sanayii Millî Güvenlik Makamı tarafından EK-O'da yer alan Üretim İzin Belgesi tanzim edilir.

f. Üretim İzin Belgesinin geçerlilik süresinde herhangi bir kısıtlama yoktur. Savunma Sanayii Millî Güvenlik Makamı tarafından yapılacak ara denetimlerde Üretim İzin Belgesinin uygunluk durumu kontrol edilir. Kuruluş tarafından Üretim İzin Belgesinde yer alan malzemelerin üretiminin durdurulmasına karar verilmesi durumunda kuruluş tarafından Savunma Sanayii Millî Güvenlik Makamına bilgi verilir, Savunma Sanayii Millî Güvenlik Makamı tarafından yapılacak değerlendirmeye bağlı olarak Üretim İzin Belgesi yeniden düzenlenebilir veya alınacak onayı müteakip iptal edilebilir.

g. Yapılan inceleme ve denetlemede, kuruluşun verdiği bilgilerin doğruluğuna ya da üretimin gerçekleştirilemeyeceğine ilişkin bir uygunsuzluk belirlenirse, bu durum yazılı olarak kuruluşa bildirilir. Kuruluşun talep etmesi durumunda, tespit edilen hususların düzeltilmesi için, Savunma Sanayii Millî Güvenlik Makamı tarafından altı aya kadar ek süre verilebilir.

ğ. Ek süre verilen kuruluşun, eksikliklerini gidererek denetleme için hazırlıklarını tamamladığını Savunma Sanayii Millî Güvenlik Makamına verilen süre içinde, ikinci denetleme için yatırılan ön inceleme makbuzu ile birlikte, yazılı olarak bildirmesi durumunda, ikinci defa belgelendirme maksatlı denetim icra edilir.

h. İlk başvuru ile denetim sonrası bildirilen eksiklikleri bildirim tarihinden itibaren üç aylık süre içinde gidermeyen veya ek süre (altı aya kadar) talep etmeyen kuruluşların Üretim İzin Belgesi başvuruları iptal edilir.

ı. İkinci denetlemenin de olumsuz sonuçlanması ve işlemlerin iptal edilmesi sonrasında kişi veya kuruluşun yeniden talepte bulunması durumunda konu, yeni müracaat olarak ele alınır.

i. Üretim İzin Belgesi tanzim edilirken, Kontrole Tâbi Listede yer alan ilgili madde dikkate alınarak sadece üretim kabiliyeti bulunan ürünler veya ürün ailesi için üretim izni verilir. Üretim izni verildikten sonra eğer aynı ürünün farklı model ve konfigürasyonda ürün üretilmesi planlanıyorsa, Savunma Sanayii Millî Güvenlik Makamına başvuruda bulunulur. Savunma Sanayii Millî Güvenlik Makamı, gerekli gördüğü takdirde, yerinde denetleme yapabilir. Ürünün farklı olması durumunda yeniden Üretim İzin Belgesi için başvuru yapılır.

j. Kontrole Tâbi Listede yer alan herhangi bir malzemeyi üretmek üzere izin alan kuruluşlar tarafından, Kontrole Tâbi Liste kapsamındaki aynı malzeme kategorisinde olmayan diğer bir malzemenin üretilmesinin planlanması durumunda; Üretim İzin Belgesinin yenilenmesi için Savunma Sanayii Millî Güvenlik Makamına müracaat edilir. Söz konusu müracaat, bu Yönergenin Üretim İzin Belgesinin verilmesine ilişkin hükümlerine göre sonuçlandırılır.

k. Denetim Heyetince yapılan üretim izni denetimlerinde kuruluşun üretim izni talep ettiği ürüne yönelik üretim dokümantasyonu, kalite planları ve dokümantasyonu, üretim prosesi ve yetenekleri, test ve doğrulama altyapısı ve yetenekleri, girdi kontrolü, alt yüklenici kullanım durumu ile kalibrasyon altyapısı ve yetenekleri ile izlenebilirlik konularında inceleme ve değerlendirmeler yapılır ve bu hususlar rapor ile kayıt altına alınır.

l. 5202 sayılı Kanun kapsamında Tesis Güvenlik Belgesi olmayan veya Üretim İzin Belgesi denetimi ile birlikte yapılan Tesis Güvenlik Belgesi denetiminin sonucu uygun bulunmayan kuruluş için Üretim İzin Belgesi verilmez.

4. ARA DENETLEMELER:

a. Ara denetlemeler, Üretim İzin Belgesi olan ve savunma malzemesi üreten kuruluşların güvenlik uygulamaları ile üretim izni bulunan kontrollü ürünlerin üretilip üretilmediği ve kabiliyetin muhafaza edilip edilmediği hususlarının gözden geçirilmesi amacıyla Savunma Sanayii Millî Güvenlik Makamı kontrol ve sorumluluğunda yapılan denetlemelerdir.

b. Üretim İzin Belgesi verilen kuruluşlar, yılda en az bir defa veya Savunma Sanayii Millî Güvenlik Makamınca gerek görüldüğünde denetlenir. Bu denetlemelerde tespit edilen eksiklikler kuruluşa yazılı olarak bildirilir ve üç aylık süre sonunda doğrulama denetimi icra edilir. İlk defa üretim izni verilmesi esnasında raporla kayıt altına alınan hususların değiştirildiğinin tespit edilmesi ve anılan eksikliklerin kuruluş tarafından giderilmemesi durumunda Üretim İzin Belgesi Savunma Sanayii Millî Güvenlik Makamınca iptal edilebilir.

5. ÜRETİM İZİN BELGESİNİN İPTALİ VEYA YENİDEN DÜZENLENMESİ:

a. Kuruluş isminin değişmesi gerekçesiyle kuruluşun müracaat etmesi durumunda, mevcut belgenin kuruluşun yeni ismine göre yenilenmesi hususunda Savunma Sanayi Millî Güvenlik Makamı yetkilidir. Tesisin yeri değişmemekle birlikte yerel idare tarafından yapılan düzenleme neticesi meydana gelen adres değişikliklerinde, denetim yapılmaksızın belge yeniden düzenlenebilir.

b. Üretim İzin Belgesinin iptalini gerektiren hususlar şunlardır:

(1) Millî güvenlik, kamu düzeni ve genel sağlık bakımından sakınca doğuranhâller.

(2) İzinsiz olarak, diğer ülkelere ya da gerçek kişilere ve özel hukuk tüzel kişilerine her türlü harp araç ve gereçleri ile silah, mühimmat ve bunlara ait yedek parçalarla, patlayıcı maddelerin veya Kontrole Tâbi malzeme listesinde yer alan diğer malzeme ve donanımın satışı veya bunlara ait teknoloji transferi yapıldığının tespit edilmesi.

(3) Kuruluşun tasfiyesi veya iflâs etmesi.

(4) Kuruluşun sahibinin değişmesi. (Hissedarlık yapısının %51 ve üzerinde değişikliğe maruz kalması.)

(5) Kuruluşun sahipleri ile yönetim kurulu üyeleri ile Genel Müdür ve Genel Müdür Yardımcılarının değişmesi hâlinde anılan personele yönelik Savunma Sanayii Millî Güvenlik Makamı tarafından yaptırılacak güvenlik soruşturması ve arşiv araştırması neticesinin olumsuz olması.

(6) Tesisin yerinin değiştirilmesi.

(7) Üretim faaliyetini etkileyen grev veya lokavt hareketleri.

(8) Kuruluşun bağlı bulunduğu ana kuruluş veya şirket varsa, bununla ilişkisinde ortaklık veya statü değişikliği olması.

(9) Savunma Sanayii Millî Güvenlik Makamı tarafından gerçekleştirilen denetimde, kuruluş tarafından taahhüt edilen hususlara uymayan herhangi bir durumun tespit edilmesi.

(10) Savunma Sanayii Millî Güvenlik Makamı tarafından gerçekleştirilen denetim esnasında; tesiste, tesis güvenliğinin zafiyete uğradığı yönünde kanaat oluşması ve bunun bir raporla tespit edilmesi.

(11) Sınır Aşan Örgütlü Suçlarla Mücadele Sözleşmesi Ateşli Silahlar Protokolünde belirtilen işaretleme kriterlerinin yerine getirilmemiş olması.

(12) Kuruluş tarafından üretim izninin iptalinin talep edilmesi.

c. Kuruluş aleyhine, yürüttüğü faaliyetlerden dolayı yasal süreç başlatılması veya yasal olmayan bir faaliyet yürütüldüğüne dair alınan duyum/tespit üzerine idari soruşturma başlatılması durumunda, verilen Üretim İzin Belgesinin süreli veya süresiz olarak askıya alınması ve üretimin durdurulması hususunda Savunma Sanayi Millî Güvenlik Makamı yetkilidir.

SEKİZİNCİ BÖLÜM
KONTROLE TÂBİ MALZEMENİN İHRACI VE İTHALİ

1. GENEL:

a. Kontrole Tâbi Listede yer alan malzemenin ihracı veya yurt dışına çıkarılmasına, Genelkurmay Başkanlığı ve Dışişleri Bakanlığının görüşleri de alındıktan sonra Savunma Sanayii Millî Güvenlik Makamı tarafından izin verilebilir.

b. Kontrole Tâbi Listede yer alan malzemenin, satışı destekleme faaliyetleri kapsamında test, demonstrasyon, brifing, inceleme, sergileme, fuar, numune ya da benzeri amaçlarla yurt dışına çıkarılmasına Savunma Sanayii Millî Güvenlik Makamı tarafından izin verilebilir.

c. 5201 sayılı Kanun kapsamında faaliyet gösteren kuruluşlar tarafından, Kontrole Tâbi Listede yer almaması nedeniyle izne gerek görülmeden dış satış bağlantısı yapılmış veya Kontrole Tâbi Listede yer aldığı için ilgili mercilerden dış sipariş kabulüyle ilgili izin verilmiş malların, gelişen hükümet politikası, ülke menfaati ve benzeri şartlar dolayısıyla müşterisine teslimine mâni olunması durumunda; satıcının kusuru dışında maruz kalacağı zarar ve ziyan Bakanlar Kurulu kararı ile Hazine tarafından ilgili kuruluşa ödenir.

ç. Kontrole Tâbi Listede yer almayan ancak Tüm Hassas Maddelerin İhracatının Kontrolü uygulaması kapsamında, kitle imha silahlarının geliştirilmesinde kullanılabileceğinden şüphe duyulabilecek çift kullanımlı malzeme ve teknolojinin ihracatında; söz konusu malzeme ve teknolojinin kitle imha silahları geliştirdiğinden şüphe duyulan bir son kullanıcıya ihracının söz konusu olması, ihracatçı firma tarafından ihracata konu olan malzemenin tamamının veya parçasının kitle imha silahlarının geliştirilmesinde kullanılabileceğinden kuşku duyulduğu yönünde beyanda bulunulması, ulusal ve uluslararası güvenliğin tehlikeye düşebileceği ve insan haklarının ihlaline yol açabileceği durumlarda c. fıkrasında yer alan tazminat ile ilgili hükümler uygulanmaz.

d. Kontrole Tâbi Listede yer alan ve ihracatı diğer kurum ve kuruşların da iznine tâbi olan malzeme için, ihracatı gerçekleştirecek kuruluş tarafından, ilgili diğer kurum ve kuruluşlardan da gerekli izinler alınır.

e. Kuruluşlarca, Kontrole Tâbi Listede yer alan malzeme ve sistemlerin herhangi bir ülkeye veya yurt dışı kuruluşa tanıtım, pazarlama, sözleşme ve teklif maksadıyla faaliyet icra edilmeden önce, tanıtım, pazarlama, sözleşme ve teklif yapılacak kuruluş/ülke, paylaşılacak bilgi düzeyi, gizlilik derecesi, numune gönderimi ile ilgili bilgiler çerçevesinde başvurularak Millî Güvenlik Makamından izin alınır.

2. TÜM HASSAS İHRACATIN KONTROLÜ:

a. Kontrole Tâbi Listede yer almamakla birlikte; canlıların toplu imhasına yönelik tasarlanan nükleer, biyolojik ve kimyasal silahlardan oluşan kitle imha silahlarının ve bunları fırlatma vasıtalarının geliştirilmesinde kullanılabileceğinden şüphe duyulabilecek malzeme ve bunlara ait teknolojilerin ihracatı, aşağıda belirtilen durumlarda Savunma Sanayii Millî Güvenlik Makamının iznine tâbi tutulur:

(1) Bu tür silahları veya fırlatma vasıtalarını geliştirmesinden şüphe duyulan ülkeye veya son kullanıcıya ihraç edilmesine yönelik bir bilgi alınması.

(2) İhracatçı kuruluş tarafından, ihracata konu olan malzemenin tamamı veya parçasının kitle imha silahları ve bunları fırlatma vasıtalarının geliştirilmesinde kullanılabileceğinden kuşku duyulması yönünde beyanda bulunulması.

(3) Ulusal veya uluslararası güvenliğin tehlikeye düşebileceği ve insan haklarının ihlâline yol açabilecek durumların oluşması.

b. a fıkrası kapsamında yapılacak ihracat izni, Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Millî İstihbarat Teşkilatı Müsteşarlığı, Dış Ticaret Müsteşarlığı ve Türkiye Atom Enerjisi Kurumunun görüşleri alındıktan sonra Savunma Sanayii Millî Güvenlik Makamı tarafından verilir.

3. İHRACAT VEYA YURT DIŞINA ÇIKARMA:

a. Kontrole Tâbi Liste kapsamındaki herhangi bir malzemenin ihracatını yapacak olan kuruluş, ekinde MSB internet sayfasında yer alan (kuruluş antetli olması esastır) İhracat İzin Belgesi ve satıcı ülke yetkili makamlarının izni alınmaksızın üçüncü bir ülkeye her ne şekilde olursa olsun verilmeyeceğinin taahhüt edildiği ve Savunma Sanayii Millî Güvenlik Makamına karşılık gelen karşı ülkenin Millî Güvenlik Makamı tarafından imzalanmış ve mühürlenmiş Son Kullanıcı Belgesinin aslı (orijinal nüsha ve mühürlü olması esastır.) bulunan bir yazı ile Savunma Sanayii Millî Güvenlik Makamına başvurur.

b. Savunma Sanayii Millî Güvenlik Makamı, kuruluşun başvurusunu müteakip,

(1) İhracatçı kuruluşun Tesis Güvenlik Belgesi durumu, (Kuruluşun 5202 sayılı Kanun gereğince Tesis Güvenlik Belgesine sahip olması şartı aranır. İhracat ve yurt dışına çıkarılmasına ilişkin ihracat izni başvurusu kapsamında Tesis Güvenlik Belgesi olan Üretim İzin Belgesi bulunmayan kuruluş tarafından ihracata konu malzemenin, Üretim İzin Belgesine sahip kuruluştan tedarik edildiğine/edileceğine dair bilgi/belgenin Makama sunulması gerekmektedir.)

(1) Başvuru evraklarının yeterliliği,

(2) İhracata esas ürünün Türk Silahlı Kuvvetleri envanterinde mevcudiyeti ve varsa fikri mülkiyet hakkına ilişkin kısıtlamaları inceleyerek konu hakkında Genelkurmay Başkanlığı ile Dışişleri Bakanlığının görüşlerini alır. Savunma Sanayii Millî Güvenlik Makamı alınan görüşleri değerlendirerek kararını ilgili kuruluşa bildirir.

c. Malzemenin ihracatı uygun bulunduğu takdirde; kuruluşa, Savunma Sanayii Millî Güvenlik Makamı tarafından, kuruluş tarafından düzenlemiş İhracat İzin Belgesi onaylanarak bir yıl veya daha uzun süreli ihracat izni verilir. Bundan sonraki işlemler, yürürlükte bulunan İhracat Yönetmeliği esaslarına göre Ekonomi Bakanlığı tarafından kayda alınarak yürütülür. Bildirim ile ilgili hususlar yönetmelikte belirtildiğigibi uygulanır.

ç. Savunma Sanayii Millî Güvenlik Makamı tarafından, ihracat izni verilen kuruluşların kayıtları tutulur. Kuruluş tarafından, ihracatı gerçekleştirilecek malzemenin ihracat izninde tanımlı hususlarda herhangi bir değişiklik olması durumunda, bu değişiklik bir ay içerisinde Savunma Sanayii Millî Güvenlik Makamına bildirilir.

d. Savunma Sanayii Millî Güvenlik Makamı tarafından ihracat izni verilen kuruluşlar, ihracatın gerçekleşmesini müteakip, ihraç ettikleri malzemeye ilişkin Gümrük Beyannamesinin bir sureti, ihraç edilen malzemenin silah olması durumunda silahların seri numarasını belirtir yazı ile Konşimento Faturasının fotokopisini Savunma Sanayii Millî Güvenlik Makamına gönderir.

e. Kontrole Tâbi Listede yer alan sistem veya malzemenin, sergileme, tanıtım, pazarlama, test vb maksadıyla süreli olarak yurt dışına geçici ihracına, Millî Güvenlik Makamı tarafından, gerektiğinde ilgili makamlar ile koordine edilerek, geçici ihraç izni verilebilir.

f. Taşınma, yönetim kurulu değişikliği vb. nedenlerle Tesis Güvenlik Belgesi ve Üretim İzin Belgesi yenileme aşamasında olan firmaların ihracat izin başvuruları Makam tarafından değerlendirilir.

g. Süresinde ihracatı gerçekleştirilemeyen malzemelere ilişkin kati ve geçici ihraç izinleri, kuruluş tarafından gerekçeleri ile birlikte süre uzatımına yönelik başvuru yapılması kaydıyla uzatılabilir.

4. İTHALAT VEYA YURT İÇİNE SOKMA:

a. Kontrole Tâbi Liste kapsamında yer alan malzemeler, gerektiğinde Millî Savunma Bakanlığı tarafından veya Bakanlıkça yetki verilen kurum ve kuruluşlarca ithal edilebilir ve yurt içine sokulabilir.

b. Kontrole Tâbi Liste kapsamında bulunan bir malzemeyi ithal etmek isteyen kuruluş, ekinde MSB internet sayfasında yer alan (kuruluş antetli olması esastır) İthalat İzin Belgesi ve ithal edilmek istenen malzemenin Kontrole Tâbi Listenin hangi maddesinde yer aldığını belirten (malzeme Wassenaar Düzenlemesi Mühimmat Listesi ve Füze Teknolojisi Kontrol Rejimi Ek Listesinde yer alıyorsa bunu belirten) bir dilekçe ile Savunma Sanayii Millî Güvenlik Makamına başvurur.

c. Savunma Sanayii Millî Güvenlik Makamı tarafından, kuruluşun başvurusunu müteakip yapılan inceleme sonucunda, gerektiğinde İhtiyaç Makamı, Proje Makamı ve/veya ihtiyaç duyulabilecek diğer makamların görüşleri alınır. Uygun bulunması durumunda, kuruluş tarafından düzenlenmiş İthalat İzin Belgesi onaylanarak talepte bulunan kuruluşa bir yıl veya daha uzun süreli ithalat izni verilebilir.

ç. Millî Savunma Bakanlığı projeleri dışında kalan ancak, Kontrole Tâbi Listede yer alan malzemenin ithalatı için, 5202 sayılı Kanun kapsamında Tesis Güvenlik Belgesi ve 5201 sayılı Kanun kapsamında Üretim İzin Belgesi bulunan kuruluşlara izin verilebilir.

d. Savunma Sanayii Millî Güvenlik Makamı tarafından ithalat izni verilen kuruluş, ithalatın gerçekleşmesini müteakip ilgili gümrük müdürlüğünce onaylanmış gümrük beyannamesi ithalatçı nüshasının bir suretini, ithal edilen malzemenin silah olması durumunda silahın seri numarasını belirtir yazının, ithal edilen malzemenin mühimmat olması durumunda ise kullanılma aşamasında düzenlenmiş sarf tutanağının bir suretini Savunma Sanayii Millî Güvenlik Makamına gönderir. Ayrıca, kuruluş tarafından gerçekleştirilecek ithalata ilişkin bilgilerin son durumlarının üç ayda bir Savunma Sanayii Millî Güvenlik Makamına iletilmesi zorunludur.

e. Kontrole Tâbi Liste kapsamındaki herhangi bir malzemenin kuruluş tarafından 6136 sayılı Kanun kapsamında ithalata yetkili kurum ve kuruluşlar dışındaki şahıs, kurum ve kuruluşlar için yapılacak test, demonstrasyon, brifing, inceleme, sergileme veya benzeri bir nedenle yurt içine sokulmasında, ithalatçı kuruluşun talebi üzerine, Savunma Sanayii Millî Güvenlik Makamı tarafından EK-R'de yer alan Geçici İthal Belgesi tanzimedilebilir.

f. Geçici ithalat yapacak kuruluş, müracaat yazısında konu hakkında açıklayıcı bilgi vererek, geçici ithalat formunu doldurur ve Savunma Sanayii Millî Güvenlik Makamına gönderir. Yapılan incelemenin olumlu olması durumunda, Savunma Sanayii Millî Güvenlik Makamı tarafından geçici ithalat belgesi onaylanır. Kuruluş tarafından talep edilmesi hâlinde, Savunma Sanayii Millî Güvenlik Makamınca geçici ithalat izni verilen malzemenin yurt içinde kalışı ihtiyaç durumuna bağlı olarak b. fıkrasında belirtilen esaslar dâhilinde kesin ithalata çevrilebilir.

g. Kati ve geçici ithalat izinleri, izin süresi dolmadan önce başvuru yapılması kaydıyla uzatılabilir.

5. SON KULLANICI BELGESİ İŞLEMLERİ:

a. Son Kullanıcı Belgesi ihraç/ithal edilecek malzemenin beyan edilen alıcı tarafından bildirilen amaca uygun şekilde kullanılacağının ve satıcı ülke yetkili makamlarının izni alınmaksızın üçüncü bir ülkeye her ne şekilde olursa olsun verilmeyeceğinin taahhüt edildiği, ithalat işlemlerinde Savunma Sanayii Millî Güvenlik Makamınca ihracat işlemlerinde ise Savunma Sanayii Millî Güvenlik Makamına karşılık gelen karşı ülkenin Millî Güvenlik Makamı tarafından imzalanmış ve mühürlenmiş uluslararasıgeçerliliği bulunan belgedir.

b. Kontrole Tâbi Liste kapsamındaki malzemelerin üretilebilmesi maksadıyla Savunma Sanayii Millî Güvenlik Makamından Üretim İzin Belgesi alan kuruluşların Son Kullanıcı Belgesi talep etmesi durumunda; ithalatçı kuruluş tarafından, ithalatı gerektiren sözleşme ve açıklayıcı bilgi ile birlikte, EK-S'de yer alan ve talimatına uygun olarak bir suret doldurulan Son Kullanıcı Belgesi Proje Makamı vasıtasıyla veya Proje Makamının konuyla ilgili görüşleri de alınarak, Savunma Sanayii Millî Güvenlik Makamına gönderilir.

c. Savunma Sanayii Millî Güvenlik Makamı tarafından,

(1) Son Kullanıcı Belgesi onay talep yazısı ile Son Kullanıcı Belgesi üzerinde yazılı bilgiler arasında uyumsuzluk olup olmadığı,

(2) Tedarikçi (Consignee) ve Son Kullanıcı (End User) onay bölümlerinin eksiksiz olarak doldurularak onaylanıp onaylanmadığı,

(3) Son Kullanıcı Belgesinde yer alan malzemenin miktar, kullanım amacı, parça ve stok numarası ile isminin yanlış veya eksik yazılıp yazılmadığı,

(4) Proje Makamı veya İhtiyaç Makamı onay yazısı incelenir.

ç. Yapılan incelemeyi müteakip uygun bulunması durumunda, Son Kullanıcı Belgesi onaylanır.

d. Türk Silahlı Kuvvetleri ihtiyacı olarak Millî Savunma Bakanlığınca yurt dışından tedariki yapılan her türlü malzeme için satışı yapacak ülke resmî makamlarınca Son Kullanıcı Belgesi talep edilmesi halinde anılan bir nüsha Son Kullanıcı Belgesi, tedarik makamlarınca ihtiyaç makamları ile koordineli olarak, Tedarikçi (Consignee) ve Son Kullanıcı (End User) bölümleri imzalı şekilde, Hükümet onayı için Savunma Sanayii Millî Güvenlik Makamına gönderilir.

e. Kuvvet Komutanlıklarının ihtiyacına binaen dış tedarikten sorumlu makam tarafından gerçekleştirilen alımlar için, İhtiyaç Makamı tarafından hazırlanan ve asgarî bu makam tarafından imzalanan Son Kullanıcı Belgesi, onay için Savunma Sanayii Millî Güvenlik Makamına gönderilir. Onaylanan Son Kullanıcı Belgesi, muhatabına ulaştırılmak üzere, tedarik faaliyetini yürüten İhtiyaç Makamına gönderilir.

f. Malzemenin kabul muayenesinde reddedilmesi sonucu malzemenin yükleniciye iadesi gerektiğinde veya herhangi bir sebeple tedarik sürecine son verilmesi durumunda, Son Kullanıcı Belgesi yükleniciden geri istenir. Yüklenicinin bu belgeyi geri vermemesi durumunda malzemenin sevkine izin verilmez veya karşı ülke resmî makamları nezdinde girişim başlatılır. Son Kullanıcı Belgesinin geri alınmasını müteakip yüklenicinin ülkesinin resmî talebi doğrultusunda, malzemenin herhangi bir ülkeye sevkine izin verilir.

g. Savunma Sanayii Millî Güvenlik Makamı tarafından, ithalatın yapılacağı ülke makamlarınca talep edilebilecek olan ve EK-S'de yer alan Son Kullanıcı Belgesinden farklı formdaki Son Kullanıcı Belgelerinden uygun bulunan ve usulünce doldurulduğu belirlenen orijinal form ve şekillerdeki Son Kullanıcı Belgeleri de Son Kullanıcı makamın onayının olması kaydı ile onaylanabilir.

ğ. Son Kullanıcı Belgesinde yer alan Son Kullanıcı (End User) bölümü son kullanıcı tarafından onaylanır. İthal edilen malzeme başka bir malın imalinde kullanılacak komple veya yarı komple malzeme, ara mamul veya parça ise son kullanıcı, nihaî ürünü üreten ana yüklenici olduğundan bu kısım anılan kuruluş tarafından doldurularak onaylanır. İthal edilen mal doğrudan TSK'ya teslim edilecekse bu kısım, ihtiyaç makamının yetkili birimi tarafından doldurulur ve onaylanır. Savunma Sanayii Millî Güvenlik Makamı tarafından nihai onay anlamına gelen Hükümet Onayı (Certification of Government) bölümü onaylanır.

h. Yurt dışından tedarik edilecek malzemeler için sadece bir nüsha Son Kullanıcı Belgesi onaylanır.

6. KONTROLLÜ MALZEMELERİN YURT İÇİ İZİNİŞLEMLERİ:

a. Kontrole Tâbi Liste kapsamındaki malzemelerin güvenlik maksadıyla teminine yönelik olarak, Genelkurmay Başkanlığı ve/veya İçişleri Bakanlığı ile varsa ilgili diğer birimlerin de olumlu görüşleri alındıktan sonra Savunma Sanayii Millî Güvenlik Makamınca izin verilir.

b. Tesis Güvenlik Belgeli kuruluşlar tarafından ara girdi olarak ihtiyaç duyulan patlayıcılar, mühimmat ve silahların yurt içinden temini hususunda, ilgili makamlarla yapılacak koordinasyonu müteakip Savunma Sanayii Millî Güvenlik Makamınca izin verilebilir.

c. Eğitim maksatlı olarak ihtiyaç duyulan ve Kontrole Tâbi Liste kapsamında yer alan malzemelerin tedarikine, ilgili makamlar ile yapılacak koordinasyon sonrasında Savunma Sanayii Millî Güvenlik Makamınca izin verilebilir.

DOKUZUNCU BÖLÜM
ZİYARETLER

1. GENEL:

a. Girişin sınırlandırıldığı veya gizlilik dereceli proje yürütülen bölgelere, Proje Makamını temsil eden yetkililer, ana yüklenici veya alt yüklenici tarafından görevlendirilmiş uygun gizlilik dereceli Kişi Güvenlik Belgesi bulunan şahıslar dışında hiç kimsenin girmesine izin verilmez. Bu tür ziyaretler, gerekçeleri ile birlikte kuruluş tarafından kayıt altına alınır. Bunun dışındaki kişilerin ziyaretleri, Savunma Sanayii Millî Güvenlik Makamının izni alındıktan sonra gerçekleştirilir.

b. Tesis Güvenlik Belgesi ile belgelendirilmiş kuruluşlara ait tesislerde gizlilik dereceli proje yürütülen Kontrollü Bölgeler için ziyaret talebinde bulunulduğunda 21 iş günü öncesinden Savunma Sanayii Millî Güvenlik Makamından izin alınır. Bunun dışında kalan ve gizlilik içermeyen bölümler ile gizlilik içermeyen ticari maksatlı diğer ziyaretler için ziyaret talebi olması durumunda, Savunma Sanayii Millî Güvenlik Makamına sadece bilgi verilir.

c. Yabancı şahısların, gizlilik dereceli savunma sanayii projelerinin yürütülmekte olduğu bölge ve tesisleri ziyaret taleplerine verilecek cevaplar, Savunma Sanayii Millî Güvenlik Makamınca; gerektiğinde ilgili kurum ve kuruluşlarla koordine edilerek hazırlanır. Ziyaret izin başvurusu, ziyaretin gerçekleştirileceği tarihten en az 21 iş günü öncesinde yapılır ve ziyaret, Savunma Sanayii Millî Güvenlik Makamınca uygun bulunan tarihler arasında gerçekleştirilir.

ç. Devam etmekte olan bir proje için gerekli ziyaret izni bir defalık verilebileceği gibi, gerektiğinde proje bitimine kadar veya belirli zaman dilimlerini kapsayacak şekilde tekrarlanan ziyaretler şeklinde de verilebilir.

d. Bir resmî hükümet projesi, programı veya sözleşmesinin aciliyetinden dolayı, kısa süre içerisinde yapılması zorunlu olan ve standart ziyaret talebi usullerinin kullanılamadığı acil ziyaret (Emergency Visit) durumunda, ziyaret talebinde bulunan firma, ziyaret etmek istediği firma veya kuruluştaki ilgili personel ile doğrudan telefon, faks veya e-posta ile ön koordinasyonda bulunur. Bu koordinasyonun 5 (beş) iş günü öncesinden tamamlanması gerekir. Koordinasyon sağlandıktan sonra firma veya kuruluşun Savunma Sanayii Millî Güvenlik Makamı ziyaret edilecek ülkenin Savunma Sanayii Millî Güvenlik Makamına Ziyaret Talebi formatında bir mesaj gönderir. Bu tür ziyaretler Savunma Sanayii Millî Güvenlik Makamının izni alındıktan sonra gerçekleştirilir.

2. SAVUNMA SANAYİİ TESİSLERİNİ ZİYARET:

a. Savunma Sanayii Millî Güvenlik Makamından yazılı onay alınmadan gizlilik dereceli proje yürütülen tesislerin ilgili bölümlerine ziyaretçi kabul edilemez. Bu tesislerin diğer bölümleri için planlanacak ziyaretler de önceden Savunma Sanayii Millî Güvenlik Makamı ile koordine edilir.

b. Ziyaretler, aşağıda belirtilen hususları içerecek şekilde kayıt altına alınır ve kayıt yetkilisi tarafından onaylanır:

(1) Ziyaretçinin adı ve soyadı.
(2) Doğum yeri ve tarihi.
(3) Kişi Güvenlik Belgesi ve gizlilik derecesi (Savunma Sanayii Millî Güvenlik Makamından onaylı).
(4) TC. Kimlik numarası.
(5) Yabancı ise pasaport numarası.
(6) Milliyeti.
(7) Temsil ettiği Kurum/Kuruluş bilgileri.
(8) Ziyaret tarihleri.
(9) Ziyaret nedeni.

c. Tesis Güvenlik Belgesine sahip gizlilik dereceli bilgi, belge ve malzeme bulunan veya gizlilik dereceli proje yürütülmekte olan kuruluşlara; aşağıda açıklanan şartların tamamı karşılandıktan sonra, ziyaretçi kabul edilebilir:

(1) Ziyaretin önceden planlanması.

(2) Ziyaretçilerin Kişi Güvenlik Belgelerinin, istenilen gizlilik derecesine uygun veya daha üst seviyede olması.

(3) Şüpheli veya olağan dışı bir durumun olmaması.

(4) Savunma Sanayii Millî Güvenlik Makamı ile koordinasyonun yapılmış olması.

ç. Türkiye Cumhuriyeti vatandaşlarının, Tesis Güvenlik Belgesi sahibi savunma sanayii kuruluşlarının gizlilik dereceli bilgi ihtiva eden bölge ve alanlarına yapacakları ziyaretlere ilişkin talepler, ziyareti yapacak kişi, kurum veya kuruluş tarafından; ziyaret talep yazısı ile koordinasyonlar için gerekli süre dikkate alınarak Savunma Sanayii Millî Güvenlik Makamına yapılır. Söz konusu talep, ilgili birimler ile koordineli olarak Savunma Sanayii Millî Güvenlik Makamı tarafından karara bağlanır. Ziyaret sırasında izin verilmeyen alanlara ziyaretçilerin girmemesi için gerekli güvenlik önlemleri, ziyaret edilen kurum/kuruluş tarafından alınır.

d. Uluslararası andlaşma hükümleri saklı kalmak kaydıyla, yabancı ülke vatandaşlarının, Tesis Güvenlik Belgesi sahibi savunma sanayii kuruluşlarına yapacağı ziyaretlere ilişkin talepler, ziyareti yapacak kişi, kurum veya kuruluş tarafından; EK-Ş'de yer alan Ziyaret Talep (Request For Visit) Formu ve yazısı ile diplomatik temsilcilikler veya askerî ataşelikler vasıtasıyla koordinasyonlar için gerekli süre dikkate alınarak Savunma Sanayii Millî Güvenlik Makamına yapılır. Söz konusu talep, ilgili birimler ile koordineli olarak Savunma Sanayii Millî Güvenlik Makamı tarafından karara bağlanır. Ziyaret sırasında izin verilmeyen alanlara ziyaretçilerin girmemesi için gerekli güvenlik önlemleri ziyaret edilen kurum/kuruluş tarafından alınır.

e. Satışı destekleme ve ülkemizde yerleşik savunma sanayii kuruluşlarının tanıtım ve pazarlamasının yapılabilmesi amacıyla, Tesis Güvenlik Belgesine sahip kuruluşlar tarafından davet edilen yabancı personel için, daveti yapan kuruluş tarafından EK-Ş'de yer alan Ziyaret Talep (Request For Visit) Formu ve yazısı ile koordinasyonlar için gerekli süre dikkate alınarak Savunma Sanayii Millî Güvenlik Makamına başvuru yapılabilir.

f. Türkiye Cumhuriyeti vatandaşlarının Tesis Güvenlik Belgesi sahibi savunma sanayi kuruluşlarına gizlilik dereceli bilgi, belge, malzeme ve projeye nüfuz etmeyecek şekilde, pazarlama, iş geliştirme, eğitim vb. maksatlı yapacağı ziyaretler için Savunma Sanayii Millî Güvenlik Makamından izin alınması zorunlu değildir. Bu ziyaretler Kuruluşun ziyaretçi takip sistemi içerisinde kayda alınmak sureti ile icra edilir. Gerekli güvenlik önlemleri, kuruluş tarafından alınır.

g. Türkiye Cumhuriyeti vatandaşları ile yabancı ülke vatandaşlarının, NATO gizlilik dereceli Tesis Güvenlik Belgesine sahip olan kuruluşlara ait tesislerin gizlilik dereceli bilgi, belge ve malzeme bulundurulan ya da gizlilik dereceli projelerin yürütüldüğü kısımlarına yapılacak ziyaretler ile ilgili işlemler, NATO'yu ilgilendiren iş ve projelere ait güvenlik işlemlerinden sorumlu makam olan Kuzey Atlantik Andlaşması Teşkilatı Merkez Kurulu Başkanlığı tarafından devredilen yetki çerçevesinde, Millî gizlilik dereceli Tesis Güvenlik Belgesine sahip kuruluşların Tâbi olduğu esaslar dâhilinde Savunma Sanayii Millî Güvenlik Makamı tarafından yürütülür.

ğ. Ziyaretçi sayısının asgarî seviyede tutulması amaçlanır ve bu kişilerin uygun gizlilik dereceli Kişi Güvenlik Belgesi bulunan şahıslar olmasına dikkat edilir.

h. Savunma sanayii kuruluşlarınca ziyaret edilecek tesislerde istihbarata karşı koyma tedbirleri alınır ve ziyaretçi kişilerin, ziyaretin amacı dışındaki bilgilere nüfuzu engellenir. Ziyaretçilerin, ziyaret için beyan ettikleri ve ilgili makamlarca kabul edilen gerekçelere uygun konular ve bölgeler dışına çıkmalarına müsaade edilmez. Buna rağmen, ziyaret süresince bu bölgeler dışında kalan yerlerde de istihbarata karşı koyma tedbirleri alınır.

ı. Ziyaret edilen savunma sanayii kuruluşlarınca; ziyaret eden kişilerin adı ve soyadı, bağlı olduğu kuruluş ve devlet, ziyaret tarihi ve amacı gibi kimlik bilgilerini içeren kayıtları yerli ve yabancı ziyaretçiler için ayrı ayrı olmak üzere en az beş yıllık periyotlarda tutulur. Bu kayıtlar proje makamının izni olmadan elden çıkarılmaz.

i. Yabancı ülke vatandaşlarının Tesis Güvenlik Belgesi sahibi savunma sanayi kuruluşlarına gizlilik dereceli bilgi, belge, malzeme ve projeye nüfuz etmeyecek şekilde, pazarlama, iş geliştirme, eğitim vb. maksatlı yapacağı ziyaretler için Savunma Sanayii Millî Güvenlik Makamından izin alınmasına gerek yoktur. (Yabancı askerî ataşeler, yabancı misyon personeli ile yabancı ülke mensubu askerî personel hariç) Bu tür ziyaretler Kuruluşun yabancı ziyaretçi takip sistemi içerisinde kayda alınmak suretiyle icra edilir. Güvenlik önlemleri, ziyaret edilen kuruluş tarafından alınır. Firma tarafından yabancı personel ziyaretleri için üç aylık periyotlarda Savunma Sanayi Millî Güvenlik Makamına bilgi verilir.

3. ASKERÎ KARARGÂH VEYA TESİSLERİ ZİYARET:

a. Askeri karargah veya tesislere ziyaret talebi, Millî Savunma Bakanlığı kanalıyla yapılır. Genelkurmay Başkanlığı ve Kuvvet Komutanlıklarına, firmalar ve/veya temsilcileri tarafından yapılacak müracaatlar kabul edilmeyerek, başvuruların Millî Savunma Bakanlığına yapılması sağlanır.

(1) (iptal edilmiştir)

(2) (iptal edilmiştir)

b. Askerî tesisler için planlanan ziyaretlere, Savunma Sanayii Millî Güvenlik Makamınca Genelkurmay Başkanlığı ve ilgili Kuvvet Komutanlıkları ile gerekli koordinasyon yapılarak ve oluru alınarak, giriş izni verilir. Uygun bulunanlar, ilgili Proje Makamının kontrolünde gerçekleştirilir ve Genelkurmay İstihbarat Başkanlığına bilgi verilir. Bu ziyaretlerde, yürürlükteki "MY.: 114-1 Silahlı Kuvvetler İstihbarata Karşı Koyma, Koruyucu Güvenlik ve İş Birliği Yönergesi" esaslarına uygun önlemler alınır.

c. Tesis Güvenlik Belgeli savunma sanayii kuruluşlarında görevli Türkiye Cumhuriyeti vatandaşlarının, savunma sanayii konularıyla ilgili olarak, askerî birlik, karargah ve kurumlara yapacağı ziyaretlere ilişkin talepler, ziyareti yapacak kişi, kurum veya kuruluş tarafından; ziyaret talep yazısı ile koordinasyonlar için gerekli süre dikkate alınarak Savunma Sanayii Millî Güvenlik Makamına bilgi verilerek ilgili Kuvvet Komutanlıklarına yapılır. Kuvvet Komutanlığı tarafından yapılacak değerlendirme karar verilmek üzere Savunma Sanayii Millî Güvenlik Makamına bildirilir. Ziyaret sırasında izin verilmeyen alanlara ziyaretçilerin girmemesi için Millî Savunma Bakanlığınca belirlenen güvenlik önlemleri, ziyaret edilen birlik, karargâh ve kurum tarafından alınır.

ç. Uluslararası andlaşma hükümleri saklı kalmak kaydıyla, yabancı ülke vatandaşlarının, Savunma sanayii konularıyla ilgili olarak, askerî birlik, karargâh ve kurumlara yapacağı ziyaretlere ilişkin talepler, ziyareti yapacak, kişi, kurum veya kuruluş tarafından; Ziyaret Talep (Request For Visit) Formu ve yazısı ile diplomatik temsilcilikler veya askerî ataşelikler vasıtasıyla koordinasyonlar için gerekli süre dikkate alınarak Savunma Sanayii Millî Güvenlik Makamına bilgi verilerek ilgili Kuvvet Komutanlıklarına yapılır. Kuvvet Komutanlığı tarafından yapılacak değerlendirme karar verilmek üzere Savunma Sanayii Millî Güvenlik Makamına bildirilir. Ziyaret sırasında izin verilmeyen alanlara ziyaretçilerin girmemesi için Millî Savunma Bakanlığınca belirlenen güvenlik önlemleri, ziyaret edilen birlik, karargâh ve kurum tarafından alınır.

4. YABANCI ÜLKE TESİSLERİNİ ZİYARET:

a. Savunma projeleri ile ilgili olarak Türk yüklenici veya temsilcilerinin yabancı ülke resmî daire ve tesislerini ziyaretleri, Savunma Sanayii Millî Güvenlik Makamı ve Proje Makamı ile koordine edilerek planlanır ve ziyaretler uluslararası anlaşmalar çerçevesinde gerçekleştirilir.

b. Tesis Güvenlik Belgesi sahibi savunma sanayii kuruluşlarında çalışan Türkiye Cumhuriyeti vatandaşlarının, yabancı ülkede bulunan savunma sanayii ile ilgili kurum, kuruluş ve tesisler ile askerî birlik, karargâh ve kurumlara, savunma sanayii alanında icra edilen projeler ile ilgili olarak yapacağı ziyaretlere ilişkin talepler; Ziyaret Talep (Request For Visit) Formu ve yazısı ile ziyaret tarihinden en geç 30 iş günü öncesinden, Savunma Sanayii Millî Güvenlik Makamına bildirilir. Savunma Sanayii Millî Güvenlik Makamı tarafından başvurunun uygun bulunması durumunda, onaylı Ziyaret Talep (Request For Visit) Formu, diplomatik temsilcilikler veya askerî ataşelikler vasıtasıyla koordinasyonlar için gerekli süre dikkate alınarak ilgili ülkenin yetkili makamlarına gönderilir.

c. NATO gizlilik dereceli Tesis Güvenlik Belgesine sahip kuruluşlarda çalışan Türkiye Cumhuriyeti vatandaşlarının, NATO Gizlilik Dereceli Tesis Güvenlik Belgesine sahip savunma sanayii kuruluşları ile askerî birlik, karargâh ve kurumlara yapılacak ziyaret talepleri ile ilgili işlemler, NATO'yu ilgilendiren iş ve projelere ait güvenlik işlemlerinden sorumlu makam olan Kuzey Atlantik Andlaşması Teşkilatı Merkez Kurulu Başkanlığı tarafından devredilen yetki çerçevesinde, Millî gizlilik dereceli Tesis Güvenlik Belgesine sahip kuruluşların Tâbi olduğu esaslar dâhilinde Savunma Sanayii Millî Güvenlik Makamı tarafından yürütülür.

5. ZİYARET SONUCUNUN RAPOR EDİLMESİ:

Ziyaret sonrasında, ziyaret edilen kuruluş tarafından, ziyareti takip eden en geç 15 iş günü içerisinde aşağıdaki hususları içeren ziyaret sonuç raporu Savunma Sanayii Millî Güvenlik Makamına gönderilir.

a. Ziyaretin konusu, yeri, tarihi ve eşlik eden Kişi Güvenlik Belgesi sahibi personel bilgileri,

b. Ziyarete katılan personelin kimlik bilgileri ile varsa Kişi Güvenlik Belgesi bilgileri,

c. Ziyaret esnasında alınan güvenlik tedbirleri ve planlamaya uygun gerçekleşme bilgileri ile gündeme getirilen konulara ilişkin özet bilgi,

ç. Varsa olağan dışı bir olayın vuku bulup bulmadığı ile gündeme gelen konular ile teklif ve değerlendirmeler.

6. RÖPORTAJ, PROGRAM VE ÇEKİM YAPMA TALEPLERİ:

a. Yerli ve yabancı basın organlarının, Tesis Güvenlik Belgesine sahip savunma sanayii kuruluşlarına ait tesislerde veya askerî maksatlı olarak üretilen ürünlere yönelik, yayım, program ve çekim yapma talepleri; yayım program ve çekim talebinin amacı ve tarihi, katılımcı personel kimlik bilgileri (TC. Kimlik numaraları ile birlikte), temsil ettiği kurum/kuruluş bilgileri, paylaşılacak bilgi ve açıklamaların gizlilik derecesi ve iletişim bilgilerini içeren talep yazısı ile en geç röportaj, program ve çekim talebi tarihinden 30 iş günü öncesinden Savunma Sanayii Millî Güvenlik Makamına yapılır.

b. TASNİF DIŞI ve HİZMETE ÖZEL gizlilik dereceli yayım, program ve çekim talepleri Savunma Sanayii Millî Güvenlik Makamınca değerlendirilerek sonuçlandırılır. ÖZEL ve üzeri gizlilik dereceli yayım, program ve çekim talepleri ise Savunma Sanayii Millî Güvenlik Makamı tarafından başta Genelkurmay Başkanlığı olmak üzere ilgili kurum ve kuruluşlarla koordine edilerek değerlendirilir ve sonuçlandırılır. Sonuç talepte bulunan kuruluşa gönderilir.

c. Röportaj talepleri ile ilgili olarak, röportaj talebinde bulunan kuruluş tarafından, röportaj senaryosu (röportaj soruları cevaplandırılmak suretiyle), 30 iş günü öncesinden Savunma Sanayii Millî Güvenlik Makamına gönderilir, röportaja verilen soru ve cevaplar, Savunma Sanayii Millî Güvenlik Makamı tarafından ilgili kurum ve kuruluşlarla koordine edilerek değerlendirilir ve sonuçlandırılır. Sonuç, talepte bulunan kuruluşa gönderilir.

ç. Tesis Güvenlik Belgesine sahip, röportaj, program ve çekim talebinde bulunan Savunma sanayii kuruluşu, röportaj, program ve çekim sonucunu bir yazı ile birlikte Savunma Sanayii Millî Güvenlik Makamına bildirmek zorundadır.

7. BRİFİNG, DEMONSTRASYON TALEPLERİ:

a. Kuruluşların TSK birimlerine MSB ve TSK'ya hiçbir malî ve hukukî yükümlülük getirmemesi ve firma tarafından, TSK ve MSB'nin şimdi ve/veya geleceğe yönelik bir niyet beyanı olarak değerlendirilmemesi kaydıyla, ürün, hizmet tanıtımı konusunda MSB Teknik Hizmetler Genel Müdürlüğüne MSB'nin internet sayfasında yer alan başvuru belgeleri ile brifing, demonstrasyon veya brifing-demonstrasyon verme talebinde bulunabilirler. Taleple ilgili olarak;

(1) Teknik Hizmetler Genel Müdürlüğünce ilgili birimlere talep iletilerek söz konusu talebe ihtiyaç olup olmadığı belirlenir ve ihtiyaç olması durumunda tahmini katılımcı miktarı ile kuruluşa bilgilendirme yapılır.

(2) Kuruluşun katılım durumunun bildirilmesinden sonra uygun görmesi halinde MSB tarafından belirlenen ve MSB sayfasında yer alan başvuru ücreti MSB Merkez Saymanlık Müdürlüğünün T.C.Merkez Bankası Ankara Şubesi nezdindeki hesabına yatırır ve makbuzunu MSB Teknik Hizmetler Genel Müdürlüğüne gönderir.

(3) Brifing sonrasında demonstrasyon yapılması kuruluş talebinde yer alıyorsa demonstrasyon için ayrıca ödeme yapılmaz.

b. MSB ve TSK tarafından ilgili kuruluşlardan brifing, demonstrasyon alınması ihtiyacının MSB'ye bildirilmesi durumunda brifing, demonstrasyon için kuruluştan başvuru ücreti alınmaz.

c. Brifing ve demonstrasyon için kuruluş tarafından ihtiyaç duyulan tahsis, kiralama, satış ve görevlendirme bedelleri, talebin içeriğine göre hesaplanarak tahsil edilir.

TANIMLAR

EK-A

1. ALICI

Bir araya getirmek, kullanmak veya işlemek için ya da başka amaçlar için gönderenden gelen bilgi, belge veya malzemeyi alan kişi, Kuruluş veya diğer bir organizasyondur. Bu tanıma malzeme taşıyıcıları girmez.

2. ALT SÖZLEŞME:

Ana sözleşme yapılarak uygulamaya konulan bir projeyi ilgilendiren mal ve hizmetlerin bir kısmını karşılamak amacıyla; ana yüklenici ile alt yüklenici arasında yapılan ve Proje Makamı ile koordineyi müteakip imzalanan sözleşmedir.

3. ALT YÜKLENİCİ:

Ana savunma sistemlerinin bazı bölümlerini veya hizmetin bir kısmını ana yüklenici için üretmek üzere, ana yüklenici ile sözleşme yapmış kişi veya Kuruluştur.

4. ANA PLATFORMLAR:

Türk Silahlı Kuvvetleri Birlik ve Kurumlarının muharebe yeteneğini oluşturan, Zırhlı, Tırtıllı ve Tekerlekli Araçlar, Su Üstü ve Sualtı Deniz Platformları ile Hava Araçları (Uçak ve Helikopterler ile İnsansız Hava Araçları).

5. ANA SÖZLEŞME:

Bir ana savunma sistemi veya bir ana malzemenin veya bir hizmetin tedariki amacıyla Proje Makamı ile Ana Yüklenici arasında imzalanan sözleşmedir.

6. ARŞİV ARAŞTIRMASI:

Kişinin kolluk kuvvetleri tarafından hâlen aranıp aranmadığının, kolluk kuvvetleri ve istihbarat ünitelerinde ilişiği ile adli sicil kaydının ve hakkında herhangi bir sınırlama olup olmadığının mevcut kayıtlardan saptanmasıdır.

7. (İptal edilmiştir).

8. ATEŞLİ SİLAHLAR:

1899 yılından önce üretilmiş olmak kaydıyla antika ateşli silahlar veya taklitleri hariç, bir patlayıcı madde etkisiyle, fişek, kurşun veya mermi atan, atacak şekilde tasarlanan veya kolayca atacak hâle getirilebilen namlulu taşınabilir silahlardır.

9. BELGE (DOKÜMAN):

Askerî, stratejik, politik, idari, bilimsel, teknolojik, ekonomik ve endüstriyel planlar, kararlar, veriler, bulgular, uygulama sonuçları ve değerlendirmeler ile ilgili yazı, resim, fotoğraf, ses veya görüntü olarak herhangi bir malzeme üzerine kaydedilmiş, elektronik veya ileri teknolojili benzer ortamlarda bulunan veya bu ortamlara kaydedilebilecek veya kopyalanabilecek bilgiler içeren evrak veya dokümandır.

10. BİLGİ GÜVENLİĞİ:

Bilgi ve bilginin işlem gördüğü bilgi sistemlerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz şahısların bilgiye ulaşmaları hâlinde tespit edilmelerine yönelik alınan tedbirlerin tümüdür.

11. BİLMESİ GEREKEN KİŞİ:

Gizlilik dereceli bilgi, belge ve malzemeyi veya gizlilik dereceli projeyi, ancak görevi gereği öğrenme ve kullanma sorumluluğu olan ve bilmesi gereken prensibi çerçevesinde gerekli ve uygun seviyede Kişi Güvenlik Belgesi bulunan kişidir.

12. BİLMESİ GEREKEN PRENSİBİ:

Herhangi bir konu veya işi, ancak görev ve sorumlulukları gereği öğrenmekle, incelemekle, gereğini yerine getirmekle ve korumakla sorumlu bulunanların yetkisi düzeyinde bilgi sahibi olması ve nüfuz etmesidir.

13. ÇOKULUSLU SANAYİİ GÜVENLİĞİ ÇALIŞMA GRUBU:

NATO ve NATO dışı ülkelerle çok uluslu savunma programları çerçevesinde gizlilik dereceli bilgi, belge ve malzemenin değişimine yönelik işlemler ile savunma sanayii güvenliği uygulamalarının evrenselliğini sağlamak amacıyla, üye ülkeler arasında oluşturulmuş bir çalışma grubudur.

14. DAĞITICI:

Kontrole Tâbi Liste kapsamındaki malzemelerin üretici veya ithalatçıdan son kullanıcıya kadar ulaşmasını teminen alım ve satım işlemlerini yürüten kamu kurum ve kuruluşları, gerçek kişiler veya özel hukuk tüzel kişileridir.

15. DENETİM HEYETİ:

Kuruluşlara ait tesislerin denetimlerini gerçekleştirmek üzere; Savunma Sanayii Millî Güvenlik Makamının koordinatörlüğünde, Savunma Sanayii Millî Güvenlik Makamı tarafından görevlendirilen personel ile Sanayi ve Ticaret Bakanlığını temsilen katılacak personelden oluşturulan heyettir.

16. EK SÖZLEŞME:

Proje çalışmalarının ve/veya Ana Sözleşmenin geçerliliğinin devam ettiği süreç içinde ihtiyaç duyulabilecek konfigürasyon değişikliklerini, ihtiyaç miktarındaki artış veya azalışları ve gerekli görülebilecek diğer hususları karşılamak amacıyla, Ana Sözleşmeye ek olarak yapılan sözleşmedir.

17. FÜZE TEKNOLOJİSİ KONTROL REJİMİ EK LİSTESİ:

Türkiye'nin taraf olduğu uluslararası ihracat kontrol rejimlerinden biri olan, Füze Teknolojisi Kontrol Rejimi çerçevesinde yayımlanan teçhizat, yazılım ve teknoloji listesidir.

18. GEÇİCİ İTHAL BELGESİ:

Kontrole Tâbi Liste kapsamındaki herhangi bir silah, araç, gereç veya malzemeyi, test, demonstrasyon, brifing, inceleme, sergileme veya benzeri bir nedenle geçici bir süre için ithal etmek üzere yapılan başvurulardan uygun bulunanlar için tanzim edilen ve Savunma Sanayii Millî Güvenlik Makamınca onaylanan bir belgedir.

19. GİZLİLİK DERECELİ BİLGİ, BELGE VE MALZEME:

Kriptografik ve NATO çerçevesinde karşılıklı gönderilen sınırlı bilgiler anlamına gelen atomal bilgi, belge ve malzeme de dâhil olmak üzere; gizlilik dereceli içeriğe sahip her türlü kayıt, yazılı ve sözlü haberleşme ortamı, mesajlar, belgeler ve silah, mühimmat, araç ve gereç gibi her çeşit malzeme ile bunların parça ve kısımları, yazılım ve donanımlarıdır.

20. GİZLİLİK DERECELİ PROJE:

İhtiyaç makamınca savunma ihtiyacı olarak belirlenen ve gizlilik dereceli bilgi, belge ve malzeme ihtiva eden her türlü harp silah, araç ve gereçleri ile bunların önemli ve kritik alt sistemlerinin ve parçalarının alımını ve satımını, her tip üretim faaliyeti ile araştırmasını ve geliştirmesini, bunlarla ilgili hizmet ve alt yapı tesis ve faaliyetlerini kapsayan çalışmaların bütünüdür.

21. GİZLİLİK DERECELİ YER:

Gizlilik dereceli bilgi, belge ve malzeme bulundurulan, uygun iletişim ortamında bilgi aktarılan veya gizlilik dereceli proje yürütüldüğü için koruyucu güvenlik önlemleri alınmış olan tesis veya bölgedir.

22. GİZLİLİK DERECESİ:

Bilmesi gereken kişiler dışındakilere açıklanması veya verilmesi, millî güvenlik ve ülke menfaatleri bakımından sakıncalı görülen bilgi, belge ve malzemenin, haiz olduğu önem derecelerine göre "ÇOK GİZLİ", "GİZLİ", "ÖZEL" veya "HİZMETE ÖZEL" şeklinde sınıflandırılması ve adlandırılmasıdır.

A. MİLLÎ GİZLİLİK DERECESİ:

Bilmesi gereken kişiler dışındakilere açıklanması veya verilmesi, millî güvenlik ve ülke çıkarları bakımından sakıncalı görülen ve millî olan bilgi, belge ve malzemenin aşağıda ayrıntılı olarak dört grupta belirtilen gizlilik dereceleridir.

(1) ÇOK GİZLİ:

İzinsiz açıklanması durumunda devletimizin güvenliğine, milletimize, ulusal varlık ve bütünlüğümüze, iç ve dış menfaatlerimiz ile müttefiklerimize hayati bakımdan son derece büyük zarar verebilecek, yabancı bir devlete fayda sağlayabilecek ve güvenlik bakımından olağanüstü sonuçlar doğurabilecek evrak, araç, gereç, bilgi, belge, proje, malzeme, tesis ve yerler için kullanılan gizlilik derecesidir.

(2) GİZLİ:

İzinsiz açıklanması durumunda devletimizin güvenliğine, milletimize, ulusal varlık ve bütünlüğümüze, iç ve dış menfaatlerimize ciddi şekilde zarar verebilecek, saygınlık ve çıkarlarımızı sarsacak, yabancı bir devlete fayda sağlayabilecek nitelikte olan evrak, araç, gereç, bilgi, belge, proje, malzeme, tesis ve yerler için kullanılan gizlilik derecesidir.

(3) ÖZEL:

İzinsiz açıklanması durumunda, devletimizin çıkar ve itibarını sarsacak, bir şahsın zarar görmesine neden olacak veya yabancı bir devlete fayda sağlayabilecek nitelikte olan evrak, araç, gereç, bilgi, belge, malzeme, tesis ve yerler için kullanılan gizlilik derecesidir.

(4) HİZMETE ÖZEL:

Kapsadığı bilgiler bakımından "ÇOK GİZLİ", "GİZLİ" veya "ÖZEL" gizlilik dereceleriyle korunması gerekmeyen ancak, bilmesi gereken kişiler dışındaki şahıslar tarafından bilinmesi istenmeyen evrak, araç, gereç, bilgi, belge, proje, malzeme, tesis ve yerler için kullanılan gizlilik derecesidir.

B. NATO GİZLİLİK DERECESİ:

NATO ile ilgili uygulamalarda "COSMIC TOP SECRET", "NATO SECRET", "NATO CONFIDENTIAL", "NATO RESTRICTED" şeklinde; Türk makamları veya kuruluşları arasında NATO ile ilgili yapılacak yazışmalarda ise sırasıyla "KOZMİK ÇOK GİZLİ", "NATO GİZLİ", "NATO ÖZEL", "NATO HİZMETE ÖZEL" şeklinde Türkçe karşılıkları kullanılan gizlilik dereceleridir.

23. GÖNDEREN:

Gizlilik dereceli bilgi, belge ve malzemeyi alıcıya sevk etmekten sorumlu kişi veya Kuruluştur.

24. GÜVENLİK SORUŞTURMASI:

Kişinin kolluk kuvvetleri tarafından hâlen aranıp aranmadığının, kolluk kuvvetleri ve istihbarat ünitelerinde ilişiği ile adli sicil kaydının ve hakkında herhangi bir sınırlama olup olmadığının, yıkıcı ve bölücü faaliyetlerde bulunup bulunmadığının, ahlaki durumunun, yabancılar ile ilgisinin ve sır saklama yeteneğinin mevcut kayıtlardan ve yerinden araştırılmak suretiyle saptanması ve değerlendirilmesidir.

25. HAFİF SİLAHLAR:

Silahlı ve güvenlik kuvvetleri mensupları tarafından kullanılmak üzere tasarlandıkları için geniş bir şekilde kategorize edilen; ağır makinalı tüfekler, elle tutulan namlu altı ve monte edilmiş bomba atarlar, elle taşınır uçaksavar topları, elle taşınır tanksavar topları, geri tepmesiz tüfekler, tanksavar füzeleri ve roket sistemlerinin taşınabilir lançerleri, uçaksavar füze sistemlerinin taşınabilir lançerleri ve yüz milimetreden küçük kalibreli havanlardır.

26. İHTİYAÇ MAKAMI:

Türk Silahlı Kuvvetlerinin harekât ve lojistik destek ihtiyaçlarını karşılamak amacıyla tedarik edilecek mal ve hizmetleri, ilgili mevzuatta açıklanan usul ve esaslar çerçevesinde belirleyerek proje makamına bildiren ve proje makamı koordinasyonunda tedarik edilen mal ve hizmetlerin amacına uygun kullanılmasını planlayan ve yöneten makamdır.

27. İLETİŞİM ORTAMI:

Bilgilerin ve belgelerin iletilmesinde ve/veya aktarılmasında kullanılan veya kullanılabilecek olan sözlü, yazılı, elektrik, elektronik, elektromanyetik, kızılötesi veya ileri teknolojili olabilecek bir imkân veya bunlardan bazılarının müşterek kullanımı ile ortaya çıkan bir sistemdir.

28. İŞARET:

İmalâtın yapıldığı ülkenin, ilk bakışta tanınmasını mümkün kılacak şekilde üreticinin adını, üretim yerini veya ülkesinin ve silahın seri numarasını belirten sayısal veya sayı ve rakamların bileşiminden oluşan şifre ile bir araya getirilmiş basit geometrik sembollerden oluşan, kolay anlaşılabilir herhangi bir özel semboldür.

29. (İptal edilmiştir)

30. KİŞİ GÜVENLİK BELGESİ:

Personelin, gizlilik dereceli bilgi, belge, malzeme veya projeye, bilmesi gereken prensibi çerçevesinde nüfuz edebilmesini veya bunların muhafaza edildiği gizlilik dereceli yerlere giriş iznini sağlayan belgedir.

31. KONTROLE TÂBİ LİSTE:

Millî Savunma Bakanlığınca ilgili kamu kurum ve kuruluşlarının görüşleri alındıktan sonra tespit edilen ve 5201 sayılı Kanun gereğince her yıl Ocak ayında veya gerektiğinde yıl içerisinde Resmî Gazetede ilân olunan Kontrole Tâbi Harp Araç ve Gereçleri ile Silah, Mühimmat ve Bunlara Ait Yedek Parçalar, Patlayıcı Maddeler ve Bunlara Ait Teknolojilere İlişkin Listedir.

32. KONTROLLÜ BÖLGE:

Tesis içerisinde, gizlilik dereceli bilgi, belge ve malzemenin muhafaza edildiği veya gizlilik dereceli proje çalışmalarının yürütüldüğü ve yetkisiz kişilerin nüfuz etmesini engelleyecek şekilde fiziki önlemlerle giriş-çıkışı kontrol altına alınan bölgedir.

33. KONTROLLÜ ODA:

Tesis Güvenlik Belgesi ile belgelendirilmiş olan bir tesiste, gizlilik dereceli bilgi, belge ve malzemenin konulduğu dolap, dosya, kaset, teyp, disket, CD ve benzerlerinin korunması için; tavan, taban, kapı ve duvarları takviye edilmiş, giriş-çıkışı kontrol altına alınmış, içerideki bilgi, belge ve malzemeye dışarıdan nüfuz edilmesini engelleyecek şekilde önlem alınmış, bilmesi gereken kişilerden başkasının girişine izin verilmeyen, biri şifreli olmak üzere en az iki kilitli kapısı olan ve uygun alarm/ikaz sistemleri ile donatılmış odadır.

34. KURULUŞ:

5201 ve/veya 5202 sayılı Kanunlar kapsamında faaliyet gösteren veya göstermek isteyen kamu kurum ve kuruluşları ile gerçek kişilere ve özel hukuk tüzel kişilerine ait kuruluştur.

35. KURULUŞ GÜVENLİK KOORDİNATÖRÜ:

Savunma sanayii güvenliği ile ilgili faaliyetleri takip ve koordine etmek üzere Kuruluş tarafından görevlendirilen ve Savunma sanayii güvenliği ile ilgili mevzuat ve tesise özgü hazırlanan Tesis Özel Güvenlik El Kitabında yer alan hususların, Kuruluş bünyesinde uygulanmasından sorumlu olan kişidir.

36. KURULUŞ İZNİ:

Kuruluş tarafından, Kontrole Tâbi Liste kapsamında bulunan bilgi, belge, proje, malzeme veya hizmetlerin üretiminin gerçekleştirilmesi maksadıyla kurulacak tesislerin, 18 Aralık 1981 tarihli ve 2565 sayılı Askerî Yasak Bölgeler ve Güvenlik Bölgeleri Kanunu kapsamında bulunmayan arazilerde kurulabilmesi için öncelikle Savunma Sanayii Millî Güvenlik Makamından alınması gereken izindir.

37. KURYE:

Herhangi bir belgeyi veya bir gereci getirip götürme ve teslim etme sorumluluğunu alan fakat belgeye veya gerece ait bilgileri bilmesi gerekmeyen, uygun gizlilik dereceli Kişi Güvenlik Belgesine sahip kişidir.

38. KUZEY ATLANTİK ANDLAŞMASI TEŞKİLÂTI MERKEZ KURULU BAŞKANLIĞI:

Dışişleri Bakanlığı Uluslararası Güvenlik İşleri Genel Müdürlüğü bünyesinde kurulmuş olan ve NATO'yu ilgilendiren iş ve projeler konusunda çalışan Kuruluşlara NATO Tesis Güvenlik Belgesi tanzim etmekten sorumlu olan makamdır.

39. KÜÇÜK SİLAHLAR:

Silahlı ve güvenlik kuvvetleri mensupları tarafından kullanılmak üzere tasarlandıkları için geniş bir şekilde kategorize edilen; tabancalar ve kendisinden dolma tabancalar, namlusu yivli tüfekler ve karabinalar, hafif makinalı tüfekler ve saldırı tüfekleridir.

40. MALZEME:

Bilgi, belge, proje, ürün ve kalemlerdir.

41. MESAJ (HABER):

Açık ve kapalı olarak, herhangi bir haberleşme sistemi ile gönderilmek üzere hazırlanmış kısaca ifade edilen bir teklif, görüş, rapor veya yapılan bir işlemin arzıdır.

42. MÜHİMMAT:

Ateşli silahlarda kullanılan fişek kovanı, falya, barut tozu, kurşun veya mermiler dâhil, cephanenin kendisi veya bunu meydana getiren unsurlardır.

43. PARÇALAR VE AKSAMLAR:

Ateşli silahlar için özel olarak tasarlanmış ve kullanımı için gerekli namlu, gövde veya mermi haznesi, mermi sürücüsü veya silindir, pim veya atım yatağı ile silahın ateşlenmesi sonucu çıkan sesi azaltmak için tasarlanmış veya kullanılan cihaz dâhil, herhangi bir unsur veya ikame edilebilir unsurlardır.

44. PROJE:

Herhangi bir bilgi, belge, malzeme, sistem, araç, gereç veya hizmet ile ilgili araştırma, geliştirme, eğitim, alt yapı oluşturma, üretim, iletişim, alım, satım, depolama, bakım, onarım veya envanter dışına çıkarma çalışmalarının bütünüdür. Proje; anılan hususların tamamını veya birkaçını birlikte içeren kapsamlı bir çalışma olabileceği gibi, bir belgenin ilgiliye iletimi ile sınırlı bir görev de olabilir.

45. PROJE GÜVENLİK TALİMATI:

Kontrole Tâbi Listede yer alan ve en az "ÖZEL" veya üzeri gizlilik derecesini haiz projelerde, proje makamı koordinatörlüğünde hazırlanan ve Savunma Sanayii Millî Güvenlik Makamı tarafından onaylanan, projenin yürütülmesi sırasında savunma sanayii güvenliği ile ilgili mevzuata göre alınması gerekli tüm güvenlik tedbirlerini içeren dokümandır.

46. PROJE MAKAMI:

İhtiyaç makamı tarafından talep edilen mal ve/veya hizmetlerin tedariki için gerekli olan tüm faaliyetleri yürüten makamdır.

47. SATIŞ İZNİ:

Kontrole Tâbi Listede belirlenen silah, mühimmat ve bunlara ait yedek parçaların, Üretim İzin Belgesi bulunan tesis içerisinde veya 5202 sayılı Kanun kapsamında düzenlenen satış yerlerinde üretici veya dağıtıcı firmalarca satışının yapılabilmesi için Savunma Sanayii Millî Güvenlik Makamı tarafından verilen izindir.

48. SATIŞ İZNİ BELGESİ:

Satış izni alınmasını müteakip Savunma Sanayii Millî Güvenlik Makamı tarafından tanzim edilen belgedir.

49. SAVUNMA SANAYİİ:

Askerî amaçlarla kullanılabilecek nitelikteki bilgi, belge ve malzemeleri üreten, bu kapsamda araştırma geliştirme yapan veya hizmet veren sanayi tesislerinin bütünüdür.

50. SAVUNMA SANAYİİ GÜVENLİĞİ:

Kontrole Tâbi Listede yer alan malzemeleri üreten, araştırma ve geliştirme yapan, hizmet veren Kuruluşlarda, gizlilik dereceli bilgi, belge, proje, malzeme veya hizmetlerin korunması, tesislerin ve personelin güvenliklerinin sağlanmasıdır.

51. SAVUNMA SANAYİİ MİLLÎ GÜVENLİK MAKAMI:

5202 sayılı Kanun ile yetkilendirilen Millî Savunma Bakanlığı adına Teknik Hizmetler Genel Müdürlüğüdür.

52. SİLAH:

Savunmak veya saldırmak amacıyla kullanıldığında uzaktan veya yakından canlıları öldürebilen, yaralayan, etkisiz hâle getiren, yıkım gücü sağlayan, ölümcül olaylara sebep olan, herhangi bir patlayıcı madde vasıtasıyla mekanik veya basınçlı hava yardımıyla atılabilen veya fırlatılabilen ateşli veya ateşsiz, farklı menzillere sahip, uzun veya kısa namlulu, tek veya toplu olarak ateşlenebilen, ağır, hafif ve otomatiksilahlardır.

53. SON KULLANICI BELGESİ:

Harp Araç ve Gereçleri ile Silah, Mühimmat ve Patlayıcı Madde Üreten Sanayi Kuruluşlarının Denetimi Hakkında Yönetmelik hükümlerine göre denetime Tâbi mal ve fikrî ürünlerin ihracatında satıcının onayı alınmadan üçüncü kişilere veya ülkelere verilmeyeceğinin alıcı tarafından taahhüt edildiğini gösteren, ilgili ülkenin yetkili resmî makamı tarafından onaylanan ve örneği bu Yönergenin ekinde yer alan belgedir.

54. TAŞIYICI FİRMA:

Uygun gizlilik dereceli MİLLÎ/NATO Tesis Güvenlik Belgesini haiz şirket/Kuruluştur.

55. TEMPEST:

Gizlilik dereceli bilgi işleyen elektriksel ve elektronik teçhizatın yaydığı istenmeyen elektromanyetik sızıntılardır.

56. TESİS:

Kuruluş tarafından 5201 ve/veya 5202 sayılı Kanunlar kapsamında faaliyet gösterilen veya gösterilecek olan her türlü atölye, fabrika, ofis, bina ve benzeri yerlerdir.

57. TESİS GÜVENLİK BELGESİ:

Bir tesiste bulunan veya bulunabilecek gizlilik dereceli bilgi, belge, proje ve malzemenin fiziki güvenliklerinin sağlanması için, tesisin bulunduğu yer ve çevre şartları ile maruz kalabileceği dış ve iç tehditler göz önüne alınarak projelendirilmiş olan koruma önlemlerinin uygun bulunduğunu belirten belgedir.

58. TESİS ÖZEL GÜVENLİK EL KİTÂBİ:

Kuruluşlara ait tesislerde, gizlilik dereceli bilgi, belge, proje, malzeme veya hizmetlerin korunması, tesislerin ve personelin güvenliklerinin sağlanması için alınması gereken tüm tedbirleri içerecek şekilde Kuruluş tarafından hazırlanan, her sayfası güncellenebilecek şekilde değiştirilebilen, değişiklik tarih ve numarası içeren ve güvenlik koordinatörü tarafından imzalanan, Millî Güvenlik Makamı tarafından onaylanan dokümandır.

59. ÜRETİCİ:

Kontrole Tâbi Liste kapsamındaki malzemeleri üreten, hazırlayan, bunlara ticarî adını veya markasını veren Kuruluştur.

60. ÜRETİM İZİN BELGESİ:

Kuruluşlara, 5201 sayılı Kanun kapsamında üretim yapabilmeleri için, Denetim Heyeti vasıtasıyla yapılacak denetim sonucunda Millî Savunma Bakanının onayı ile verilen izni müteakip, Savunma Sanayii Millî Güvenlik Makamı tarafından tanzim edilen belgedir.

61. ÜRETİM İZNİ:

Kuruluşlara, 5201 sayılı Kanun kapsamında üretim yapabilmeleri için, denetim heyeti vasıtasıyla yapılacak denetim sonucunda, Millî Savunma Bakanının onayı ile verilen izindir.

62. YABANCI ŞİRKET/KURULUŞ:

Türkiye Cumhuriyeti sınırları dışında konuşlandırılmış veya Türkiye Cumhuriyeti şirketler hukuku mevzuatına tâbi olmayan şirketler/kuruluşlardır.

63. YASADIŞI ÜRETİM:

Ateşli silahların, parçalarının ve aksamlarının veya mühimmatının kaçak yollarla elde edilmiş parça ve aksamın kullanılması suretiyle, yetkili makamlardan ruhsat veya izin alınmaksızın veya üretilmesi aşamasında ateşli silahların Sınır Aşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesine Ek Ateşli Silahlar, Parçaları ve Aksamları ile Mühimmatının Yasa Dışı Üretimine ve Kaçakçılığına Karşı Protokol uyarınca işaretlenmesi yapılmaksızın imal ve montajıdır.

64. YERLİ ŞİRKET/KURULUŞ:

Türkiye Cumhuriyeti sınırları dâhilinde mal ve hizmet üretmek üzere ve Türkiye Cumhuriyeti şirketler hukuku mevzuatına uygun olarak kurulmuş, Sanayi ve Ticaret Bakanlığı Sanayi Siciline kayıtlı şirketlerdir. Millî şirketler/kuruluşlar ve yabancı ortaklı şirketler/kuruluşlar olmak üzere iki ana gruba ayrılırlar.

a. MİLLÎ ŞİRKET/KURULUŞ:

Sanayi ve Ticaret Bakanlığı Sanayi Siciline kayıtlı şirketlerden, şirketi idare ve temsil etmeye yetkili olanların tamamı Türk vatandaşı olan, anonim ve sermayesi paylara bölünmüş komandit şirketlerde ayrıca hisse senetleri nama yazılı ve ahara devri şirket idare meclisinin ve Millî Savunma Bakanlığının iznine bağlı bulunan Kuruluşlardır.

b. YABANCI ORTAKLI ŞİRKET/KURULUŞ:

Yabancı kurum veya kuruluşlarla ortak olarak Türkiye Cumhuriyeti sınırları dâhilinde mal ve hizmet üzere kurulmuş, Türkiye Cumhuriyeti şirketler hukuku mevzuatına tâbi ve Sanayi ve Ticaret Bakanlığı Sanayi Siciline kayıtlı şirketlerdir. Yabancı Ortaklı Şirketler/Kuruluşlar kendi aralarında; Şirketi/Kuruluşu idare ve temsil etmeye yetkili olanların çoğunluğu Türk vatandaşı olan ve şirket mukavelesine göre oy çoğunluğu Türk ortaklarda bulunanlar, Şirketi/Kuruluşu idare ve temsil etmeye yetkili olanların çoğunluğu yabancı uyruklu olan ve şirket mukavelesine göre oy çoğunluğu yabancı ortaklarda bulunanlar, olmak üzere iki gruba ayrılırlar.

65. YÜKLENİCİ:

Bir sistem, araç, gereç, yedek parça, bilgi, belge veya malzemeyi tedarik etmek veya bir hizmeti gerçekleştirmek üzere sözleşmeyle, bedel karşılığında sınaî, ticarî, eğitimsel veya diğer mahiyette bir iş yapmayı yüklenen kişi veya Kuruluştur.

66. WASSENAAR DÜZENLEMESİ MÜHİMMAT LİSTESİ:

Türkiye'nin taraf olduğu uluslararası ihracat kontrol rejimlerinden biri olan Wassenaar Düzenlemesi çerçevesinde yayımlanan mühimmat listesidir.

KISALTMALAR

EK-B

FSC	FACILITY SECURITY CLEARANCE (TESİS GÜVENLİK BELGESİ)
FTKR	FÜZE TEKNOLOJİSİ KONTROL REJİMİ
KGB	KİŞİ GÜVENLİK BELGESİ
KTL	KONTROLE TÂBİ LİSTE
MISWG	MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP-ÇOKULUSLU SANAYİ GÜVENLİĞİ ÇALIŞMA GRUBU
NATO	NORTH ATLANTIC TREATY ORGANISATION-KUZEY ATLANTİK ANDLAŞMASI TEŞKİLÂTI
PGT	PROJE GÜVENLİK TALİMATI (PROJECT SECURITY INSTRUCTION)
PSC	PERSONNEL SECURITY CLEARANCE (KİŞİ GÜVENLİK BELGESİ)
PSI	PROJECT SECURITY INSTRUCTION (PROJE GÜVENLİK TALİMATI)
SKB	SON KULLANICI BELGESİ
TGB	TESİS GÜVENLİK BELGESİ (FACILITY SECURITY CLEARANCE)
TÖGEK	TESİS ÖZEL GÜVENLİK EL KİTABI
ÜİB	ÜRETİM İZİN BELGESİ
WD	WASSENAAR DÜZENLEMESİ

KURYE YETKİLENDİRME FORMU

EK-C

THE REPUBLIC OF TÜRKİYE
THE MINISTRY OF NATIONAL DEFENCE **TEL: 90-312-410-6260**
TECHNICAL SERVICES DEPARTMENT **FAX: 90-312-410-5488**
BAKANLIKLAR/ANKARA

COURIER AUTHORISATION FORM

1. CERTIFICATION STATEMENT:

This is to certify that the bearer, …… born on …… in …… a national of the Republic of Türkiye, holder of passport/identity card no …… issued by …… on …… and employed with …… is authorised to carry on the journey detailed below the following consignment from …… to …… .

2. CONSIGNMENTS:

……
……

3. THE ATTENTION OF CUSTOMS, POLICE AND/OR IMMIGRATION OFFICIALS IS DRAWN TO THE FOLLOWINGS:

a. The material comprising this consignment is classified in the interests of National Security of the Republic of Türkiye.

b. It is requested that the consignment will not be inspected by other than properly authorized persons or those having special permission.

c. If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not have a need-to-know and in the presence of thecourier.

d. It is requested that the package, if opened for inspection, be marked after re-closing to show the evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

Customs, police and/or Immigration officials of the Republic of Türkiye and …… are requested to give assistance if necessary to assure successful and secure delivery of the consignment.

4. TRAVEL ITINERARY:

From : …… To : ……

Departure Port, Date/Time	Arrival Port, Date/Time	Airlines/Flight No.
……	……	……
……	……	……

5. POINT OF CONTACT AT THE GOVERNMENT ACTIVITY RECEIVING THE SHIPMENT:

……

6. POINT OF CONTACT AT THE ULTIMATE DESTINATION RECEIVING THE SHIPMENT:

From : …… To : ……

…… ……

COURIER AUTHORISATION FORM (CONTINUATION)
7. TO BE SIGNED ON COMPLETION OF JOURNEY BY COURIER: I declare in good faith that, during the journey covered by this Courier Authorization, I am not aware of any occurrence or action, by myself or by others, could have resulted in the compromise of the consignment. Courier: …… Signature
8. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY: NAME : TELEPHONE NUMBER : ADDRESS : SIGNATURE :
9. AUTHORIZATION APPROVAL BY THE PROJECT MANAGEMENT AUTHORITY: NAME : TITLE : ADDRESS : **STAMP** TELEPHONE : SIGNATURE : FAX:
10. CERTIFICATION OF SECURITY CLEARANCE: NAME : ADDRESS : **STAMP** TELEPHONE : SIGNATURE : FAX:
11. REQUESTING NATIONAL SECURITY AUTHORITY: NAME : ADDRESS : **STAMP** TELEPHONE : SIGNATURE : FAX:

KURYE YETKİLENDİRME FORMU

EK-C

TÜRKİYE CUMHURİYETİ
MİLLÎ SAVUNMA BAKANLIĞI **TEL : 90-312-4106260**
TEKNİK HİZMETLER GENEL MÜDÜRLÜĞÜ FAX: 90-312-417-5488
BAKANLIKLAR/ANKARA

KURYE YETKİLENDİRME FORMU

1. BELGE BEYANI:

…….. çalışan,……tarihinde …….. tarafından verilen pasaport/kimlik no.lu, …… tarihinde …… doğumlu ……..…… Türkiye Cumhuriyeti vatandaşı, taşıyıcı, ……..,
……. , ……, ……'ye aşağıda ayrıntılı olarak verilen seyahat programı süresince aşağıdaki sevkiyatı taşımakla yetkilendirildiği teyit edilir.

2. MALZEMELER:

……
……
……
……
……

3. GÜMRÜK, POLİS VE/VEYA GÖÇMENLİK YETKİLİLERİNİN AŞAĞIDAKİ HUSUSLARDA DİKKATİ ÇEKİLİR:

a. Bu sevkiyattan oluşan malzeme, Türkiye Cumhuriyetinin ulusal güvenlik çıkarları doğrultusunda sınıflandırılmıştır.

b. Bu sevkiyat, tam olarak yetkilendirilmiş kişiler veya özel izin verilmiş kişiler haricindeki personel tarafından incelenmeyecektir.

c. Eğer bir incelemeye lüzum duyulması hâlinde; incelemenin, bilmesi gerekene sahip olmayan kişilerin görüş alanı dışında ve kuryenin huzurunda yerine getirilmesi talep edilir.

d. Paket inceleme için açıldığında, malzemenin açıldığını (eğer varsa) belirten sevkiyat dokümanına not düşmek, mühürlemek ve imzalamak suretiyle açılma kanıtını göstermek için tekrar kapatıldıktan sonra paketin işaretlenmesi talep edilir.

Türkiye Cumhuriyeti ve …….....'nin Gümrük, Polis ve/veya Göçmenlik Yetkililerinden, gerekli olduğunda sevkiyatın başarılı ve güvenli bir şekilde teslim edilmesini sağlamak için yardımda bulunmaları talep edilir.

4. SEYAHAT PLANI:

Nereden : …… Nereye : ……

Kalkış Havaalanı, Tarih/Saat	Varış Havaalanı, Tarih/Saat	Havayolu/Uçuş No.
..…….	…….	……
..…….	……	……

5. SEVKİYATI ALAN HÜKÜMET KURULUŞUNDAKİ TEMAS NOKTASI:

……

6. SEVKİYATI ALAN NİHAİ VARİŞ YERİNDEKİ TEMAS NOKTASI:

Nereden : …… Nereye : ……

KURYE YETKİLENDİRME FORMU (DEVAMI)

7. KURYE TARAFINDAN SEYAHATİN TAMAMLANMASINDA İMZALANACAKTIR:

Kurye Yetkilendirme Belgesinde yer alan seyahatim süresince, tarafımca veya diğer kişiler tarafından sevkiyatın zaafa uğradığına ilişkin hiçbir olay ve durumla karşılaşmadığımı iyi niyetimle bildiririm.

Kurye : …… İmza

8. TALEPTE BULUNAN HÜKÜMET MAKAMI VEYA SANAYİ TESİSİNİN GÜVENLİK AMİRİ:

İSİM : TELEFON NUMARASI :
ADRES :
İMZA :

9. PROJE YÖNETİM MAKAMININ YETKİ ONAYI:

İSİM :

UNVAN :

ADRES :

MÜHÜR

TELEFON :

İMZA :

FAKS:

10. GÜVENLİK KLERANSI ONAYI:

İSİM :

ADRES :

MÜHÜR

TELEFON :

İMZA :

FAKS:

11. TALEPTE BULUNAN MİLLÎ GÜVENLİK MAKAMI:

İSİM :

ADRES :

MÜHÜR

TELEFON :

İMZA :

FAKS:

PROJE GÜVENLİK TALİMATI **EK-Ç**

1. GİRİŞ
- 1.1. AMAÇ
- 1.2. KAPSAM
- 1.3. YÜRÜRLÜK/GEÇERLİK SÜRESİ
- 1.4. FİRMA GÜVENLİK YAKLAŞIMI
- 1.5. FİRMA GÜVENLİK SİSTEMİ

2. KAYNAKLAR

3. TANIMLAR

4. FİZİKSEL GÜVENLİK/TESİS GÜVENLİĞİ

5. EVRAK, DOKÜMAN VE MALZEME GÜVENLİĞİ
- 5.1 EVRAK/MALZEME GÜVENLİĞİ
  - 5.1.1 PROJELERİN GİZLİLİK DERECELERİNİN BELİRLENMESİ
  - 5.1.2 GİZLİLİK DERECELİ BİLGİNİN AKTARILMASI
  - 5.1.3 GİZLİLİK DERECESİNİN İŞARETLENMESİ
  - 5.1.4 GİZLİLİK DERECELİ BİLGİ, EVRAK VE MALZEMENİN SAKLANMASI
  - 5.1.5 GİZLİLİK DERECELİ EVRAKIN ÇOĞALTILMASI VE TERCÜMESİ
  - 5.1.6 GİZLİLİK DERECELİ BİLGİ, EVRAK VE MALZEMENİN TAŞINMASI
  - 5.1.7 GİZLİLİK DERECELİ BİLGİ, EVRAK VE MALZEMENİN İMHASI
- 5.2 MALZEME GİRİŞ ÇIKIŞ USULLERİ

6. BİLGİ GÜVENLİĞİ
- 6.1. ELEKTRONİK BİLGİ GÜVENLİĞİ
  - 6.1.1 KULLANICI SORUMLULUKLARI
  - 6.1.2 ERİŞİM KONTROLÜ
  - 6.1.3 VERİ DEPOLAMA, YEDEKLEME, ÇOĞALTMA, TRANSFER, ERİŞİM İŞLEMLERİ
  - 6.1.4 KAYNAKLARIN ETKİN KULLANIMI
  - 6.1.5 VİRÜS VE ZARARLI YAZILIMLARDAN KORUMA
- 6.2 GİZLİLİK DERECELİ TOPLANTILARIN YAPILACAĞI TOPLANTI ODALARI İÇİN ALINACAK ÖNLEMLER

7. PERSONEL GÜVENLİĞİ
- 7.1 GÜVENLİK SORUŞTURMASI
- 7.2. KİŞİ GÜVENLİK BELGESİ
- 7.3. FİRMADA GÖREV YAPAN YABANCI UYRUKLU PERSONEL

8. ZİYARETÇİLER
- 8.1 ULUSAL ZİYARETÇİLER
- 8.2 ULUSLARARASI ZİYARETÇİLER
- 8.3 REFAKAT FAALİYETLERİ

9. ALT SÖZLEŞME YAPILMASI
- 9.1. ULUSAL ALT SÖZLEŞMELER
- 9.2 ULUSLARARASI ALT SÖZLEŞMELER

10. BİLGİ PAYLAŞILMASINA İLİŞKİN ESASLAR

11. PROGRAM GÜVENLİK GEREKLERİ
- 10.1. TANIMLAR
- 10.2 FİRMA TESİSLERİNE GİRİŞ
- 10.3 GİRİŞ YETKİLERİNİN DÜZENLENMESİ

12. SORUMLULUKLAR

13. MALZEMELER/CİHAZLAR

14. EĞİTİMLER VE BRİFİNGLER

15. KURAL İHLALLERİ VE SONUÇLARI

16. ENDÜSTRİYEL HİJYEN VE İŞ GÜVENLİĞİ

17. ACİL DURUM GÜVENLİK USULLERİ

EK LİSTELERİ (İHTİYAÇ DUYULAN EK'LER LİSTELENİR)

TOPLANTI KATILIM FORMU

EK-D

(AMBLEM)	**TOPLANTININ KONUSU** Subject of the Meeting	
	TOPLANTININ YERİ Place of the Meeting	
	TOPLANTININ TARİHİ Date of the Meeting	
	TOPLANTININ GİZLİLİK DERECESİ Classification of the Meeting	

KATILIMCILAR-PARTICIPANTS

	ADI SOYADI Full Name	**KURULUŞ** Organisation	**GÖREVİ** Position	**UNVANI** Title/Rank	**TEL.NO.** Phone	**İMZA** Signature
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						

KURULUŞ İZNİ BAŞVURU YAZISI

EK-E

(Yazıya, hazırlayan tarafından uygun gizlilik derecesi verilecektir.)

Kuruluşun Adı ve Adresi

SAYI : …… *Tarih:* … / … / ….

KONU: Kuruluş İzni Başvurusu.

MİLLÎ SAVUNMA BAKANLIĞI
TEKNİK HİZMETLER GENEL MÜDÜRLÜĞÜ

1. 5201 sayılı "Harp Araç ve Gereçleri ile Silah, Mühimmat ve Patlayıcı Madde Üreten Sanayi Kuruluşlarının Denetimi Hakkında Kanun" gereği ……..… tarihli ve …… sayılı Resmî Gazetede yayımlanan Kontrole Tâbi Listenin …….. maddesi kapsamındaki……ürünlerinin (izin istenen malzeme ve teçhizat detaylı olarak tanımlanmalıdır.) üretimini yapabilmek için Kuruluş İzni almak istiyoruz.

2. İstenen bilgi ve belgeler EK'te sunulmuş olup, gereğinin yapılmasını arz ederiz.

Genel Müdür
(Adı Soyadı, İmza)

Yönetim Kurulu Başkanı
(Adı Soyadı, İmza)

EKİ :
(İstenen Bilgi ve Belgeler)

EK-F

(İptal edilmiştir)

EK-G

(İptal edilmiştir)

KİŞİ GÜVENLİK BELGESİ BAŞVURU YAZISI

EK-Ğ

(Hazırlanan yazı "GİZLİ" Gizlilik Derecesinde Olacaktır.)

Kuruluşun Adı ve Adresi

SAYI :_____ Tarih: _/_/_

KONU : Kişi Güvenlik Belgesi Başvurusu.

MİLLÎ SAVUNMA BAKANLIĞI
TEKNİK HİZMETLER GENEL MÜDÜRLÜĞÜ

1. Kuruluşumuzda görevli bulunan ve aşağıda/EK-A listede kimlikleri belirtilen her bir personel için "Güvenlik Soruşturması ve Arşiv Araştırması Formu", "Nüfus Cüzdanı Sureti" ve "Adli Sicil Belgesi" üçer adet hazırlanarak EK-(B:D)'de sunulmuştur.

2. Gerekli incelemenin yapılarak adı/adları geçen personel için "MİLLÎ GİZLİ"/"NATO GİZLİ" gizlilik dereceli Kişi Güvenlik Belgesi tanzim edilmesini arz ederiz.

Genel Müdür
(Adı Soyadı, İmza)

Yönetim Kurulu Başkanı
(Adı Soyadı, İmza)

EKLER :
EK-A (İsim Listesi-TC Kimlik No. ve Görev Ünvanları ile birlikte)
EK-B (…..adet TC No.lu Nüfus Cüzdanının Arkalı Önlü Fotokopisi)
EK-C (…..adet Güvenlik Soruşturması ve Arşiv Araştırması Formu ile Nüfus Cüzdanı Sureti)
EK-Ç (…..adet Adlî Sicil Belgesi)
EK-D (….. İptal edilmiştir)

BEYANNAME

EK-H

Aşağıda imzası bulunan……..……..oğlu/kızı,…….. doğumlu, …….....'de ikamet etmekte olan ben ……..... yürürlükteki Millî Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi ve buna ilişkin bütün mevzuattan HABERDAR EDİLDİĞİMİ, bunları tamamen anladığımı, nüfuz ettiğim veya edeceğim gizlilik dereceli konuların, planların, yazıların, istihbarat bilgilerinin, malzemenin, araç ve gerecin, cihazın, atölye, tesis ve mahallerin sır vasfını korumak için ÜSTÜME DÜŞEN SORUMLULUĞU BİLDİĞİMİ, kasten veya bilerek bu gibi sırların yetkisiz ellere geçmesine veya yetkisiz kişilerin bunlara nüfuz etmesine NEDEN OLDUĞUM TAKDİRDE; yürürlükteki kanun, tüzük, yönetmelik veya idarî ve hukukî mevzuat hükümlerine göre SORUMLU TUTULACAĞIMI BİLİYORUM.

Bana verilen ve içeriğinin üçüncü kişilere açıklanması istenmeyen gizlilik dereceli bir görev ile ilgili bilgi, belge, malzeme, araç ve gereci sadece veriliş AMACINA UYGUN OLARAK KULLANACAĞIM ve bunların korunmasını sağlamak için mümkün olabilecek her önlemi alacağım.

Gizlilik dereceli yerlerde ve projelerde çalıştığım süre içerisinde öğrenmiş olduğum her tür bilgiyi, görevin gerektirdiği hâller dışında üçüncü kişilere aktarmayacağımı, bu gibi gizlilik dereceli proje yürütülen bölümden veya kuruluştan ayrılmış olsam dahi GİZLİLİK KURALLARINA UYACAĞIMI ve bu bilgileri başka amaçlar için kullanmayacağımı, aksi takdirde hakkımda idarî ve hukuki işlem yapılmasını şimdiden kabul ettiğimi BEYANEDERİM…../…../201

(Tarih, Kişi Güvenlik Belgesi Verilen Şahsın İmzası)

Yukarıda açık kimliği ve imzası bulunan ……..... kuruluşumuzun ……..bölümünde ……statüsünde istihdam edilmektedir.

Kuruluş Yetkilisinin :
Adı S o y a d ı :
Görevi :
İmzası :

KİŞİ GÜVENLİK BELGESİ

EK-I

(İptal edilmiştir.)

TESİS GÜVENLİK BELGESİ BAŞVURU YAZISI

EK-İ

(Yazıya, hazırlayan tarafından uygun gizlilik derecesi verilecektir.)

Kuruluşun Adı ve Adresi

SAYI : …… *Tarih: … / … / ….*

KONU: Tesis Güvenlik Belgesi Başvurusu.

MİLLÎ SAVUNMA BAKANLIĞI
TEKNİK HİZMETLER GENEL MÜDÜRLÜĞÜ

1. TSK ihtiyaçlarını karşılamak maksadıyla planlanan projelerde görev üstlenmek isteyen kuruluşumuz, (Bu dilekçeye gerekirse EK yapılarak TGB almayı gerektirecek faaliyet ayrıntılı olarak açıklanmalıdır.) hâlen …… konularında faaliyet göstermektedir. Savunma sanayi ve savunma sistem ve malzemeleri tedariki konularını ilgilendiren gizlilik dereceli projeler kapsamında görüşmelerde bulunmak, istenilen mal veya hizmete ilişkin istek ve özellikleri, doküman ve belgeleri incelemek, imkân ve kabiliyetlerimiz içinde olanlar için teklif hazırlamak, uygun bulunduğunda hizmet vermek arzusundayız.

2. Kuruluşumuzu, savunma projelerinde ana yüklenici ve/veya alt yüklenici olarak çalışabilecek şekilde teşkilâtlandırmak ve gerekli düzenlemeleri yaparak …… gizlilik dereceli Tesis Güvenlik Belgesi almak istiyoruz.

3. İstenen bilgi ve ve belgeler EK'te sunulmuş olup, gereğinin yapılmasını arz ederiz.

Genel Müdür	Yönetim Kurulu Başkanı
(Adı Soyadı, İmza)	(Adı Soyadı, İmza)

EKİ :
(İstenen Bilgi ve Belgeler)

EK-J

TESİS GÜVENLİK BELGESİ PROTOKOLÜ

……..…… GİZLİLİK DERECELİ TESİS GÜVENLİK BELGESİ PROTOKOLÜ

..... FİRMASI TESİS GÜVENLİK SİSTEMİNİN İNCELENMESİ, DEĞERLENDİRİLMESİ VE BELGELENDİRİLMESİ HİZMETİNİN MİLLÎ SAVUNMA BAKANLIĞINCA 3212 SAYILI KANUNA UYGUN OLARAK ÜCRETİ MUKABİLİ YAPILMASINA İLİŞKİN PROTOKOLDÜR.

1. PROTOKOLÜN TARAFLARI:

Bu protokolde taraflar; Millî Savunma Bakanlığı Teknik Hizmetler Genel Müdürlüğü ile …….....…. olup, Savunma Sanayii Millî Güvenlik Makamı ve Firma olarak isimlendirilmişlerdir.

2. AMAÇ:

Firmanın tesis güvenlik sisteminin incelenmesi, değerlendirilmesi ve belgelendirilmesi hizmetinin ücreti mukabili yapılmasında, tarafların yerine getireceği hususları belirlemektir.

3. KAPSAM:

Bu Protokol**,** Tesis Güvenlik Sisteminin incelenmesini talep eden Savunma Sanayii Kuruluşu ile Savunma Sanayii Millî Güvenlik Makamı arasında yapılacak çalışma ile müteakip dönemde gerçekleştirilebilecek denetlemelere ilişkin esas ve usullerikapsar.

4. GENEL:

a. Bu protokol gereği yapılacak inceleme ile yerinde denetimler sonucunda tanzim edilebilecek TGB'ye istinaden, verilebilecek gizlilik dereceli bilgi, belge ve malzemenin korunması ve savunma sanayii güvenliği ile ilgili işlemler bakımından; Firma üst düzey yöneticileri ile kuruluş güvenlik koordinatörü, Savunma Sanayii Millî Güvenlik Makamına karşı sorumludur.

b. Firma, bu protokolde ve yürürlükteki MSY.: 317-2 Millî Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesinin yürürlükte olan son versiyonunda belirtilen bütün tanımları, hüküm ve şartları ve açıklamaları aynen kabul eder. Savunma Sanayii Millî Güvenlik Makamı tarafından belirlenen koruyucu güvenlik tedbirlerini almayı ve uygulamayı taahhüt eder.

c. Firma, söz konusu tanımların, hüküm, şartların ve açıklamaların değiştirilmesi veya uygulanmaması, firmaya verilen gizlilik dereceli dokümanın geri istenmesi, planlanan proje veya programlardan çıkarılması ve/veya belirsiz bu süre için güvenlik belgesinin kaldırılması durumunda herhangi bir tazminat talep etmeyeceğini kabul ve beyan eder.

ç. Güvenlik önlemlerindeki yetersizlik nedeniyle oluşabilecek mağduriyetler, Firma tarafından tazmin edilir. Belgelendirme tarihinden sonraki dönemde,güvenlik sisteminde ihtiyaç duyulabilecek değişiklikler Savunma Sanayii Millî Güvenlik Makamı onayı alındıktan sonra uygulanır.

5. FİRMANIN YERİNE GETİRECEĞİ HUSUSLAR:

a. Talep ettiği Tesis Güvenlik Belgesinin gizlilik derecesini, Savunma Sanayii Millî Güvenlik Makamına yaptığı başvuruda belirtir.

b. Firma, başvuru dosyası ile Tesis Özel Güvenlik El Kitabının ve tesislerinin incelenmesine yönelik bu yönergenin 6. Bölüm 1.j. (1) maddesinde belirtilen ücreti yatırır ve makbuzunu Savunma Sanayii Millî Güvenlik Makamına gönderir.

c. Gizliliğin korunması uygulamaları kapsamında, gizlilik dereceli bilgilere nüfuz edebilecek hissedarlar, yönetim kurulu başkanı ve üyeleri, üst düzey yöneticileri ve bu hususta yetkilendirilen veya yetkilendirilebilecek diğer personeli için Kişi Güvenlik Belgesi tanzimi amacıyla güvenlik soruşturmalarını yaptırmak ve bu personele ilişkin değişiklikleri Savunma Sanayii Millî Güvenlik Makamına bildirmek zorundadır.

ç. Yapılan inceleme ve denetlemeler sonunda, aranan istek ve özelliklerin karşılandığı belirlenerek, Tesis Güvenlik Belgesi verilmesi uygun bulunduğu takdirde; Firma, belgelendirme işlemine yönelik bu yönergenin 6. Bölüm 1.j. (2) maddesinde belirtilen ücreti yatırır ve makbuzunu Savunma Sanayii Millî Güvenlik Makamına gönderir.

d. Firmanın; Tesis Güvenlik Belgesi için aranan şartlar bakımından yetersiz bulunması durumunda ve talebi hâlinde, tespit edilen eksiklikleri gidermesi için firmaya ek süre verilebilir. Eksiklikleri giderici düzenlemelerin yapılması, Firmanın keyfiyetindedir. İkinci denetleme Firmanın, gerekli işlemleri tamamladığını belirterek Savunma Sanayii Millî Güvenlik Makamından yazılı talepte bulunması hâlinde planlanır.

e. İkinci denetlemenin yapılabilmesi için Firma, bu yönergenin 6. Bölüm 1.j. (3) maddesinde belirtilen ücreti yatırır ve makbuzunu Savunma Sanayii Millî Güvenlik Makamına gönderir. Bunun üzerine yapılacak denetlemede uygun sonuç alınması durumunda diğer işlemlere devam edilir.

6. SAVUNMA SANAYİİ MİLLÎ GÜVENLİK MAKAMI TARAFINDAN YERİNE GETİRİLECEK HUSUSLAR:

a. Firmanın ön inceleme ücretini yatırmasını müteakip işlemler başlatılır ve teknik bir heyet oluşturularak uygun görülecek bir tarihte tesisler denetlenir.

b. Yapılan tetkik ve incelemelerin sonunda Firmanın, istenilen özellikleri sağladığı belirlenir ve diğer şartlar da uygun bulunursa, Tesis Güvenlik Belgesitanzim edilir.

c. Mevcut güvenlik altyapısı ve dokümantasyonunun yeterli bulunmadığı hâllerde, tespit edilen eksiklikler yazılı olarak bildirilir. Talebi hâlinde Firmaya ek süre verilebilir.

ç. Firmanın, belirtilen eksikliklerin giderildiğini belirten bir yazı ile denetlemenin tekrarlanmasını talep etmesi hâlinde, ikinci bir denetleme planlanabilir. Bu denetleme, Firmanın gereken ücreti yatırması ve makbuzunu Savunma Sanayii Millî Güvenlik Makamına göndermesini müteakip uygun görülecek bir süre içinde gerçekleştirilir.

d. İkinci denetleme sonunda, gerekli koşulların sağlandığı belirlendiği takdirde, Tesis Güvenlik Belgesi tanzimi ile ilgili işlemlere devam edilir. Bu denetlemenin de olumsuz sonuçlanması durumunda, Tesis Güvenlik Belgesi işlemleri iptal edilir. Firma tarafından altı aydan daha önce yeniden başvuru yapılamaz.

7. UYUŞMAZLIKLARIN HALLİ:

Bu protokolün uygulanması sırasında doğacak uyuşmazlıklar karşılıklı görüşmeler yolu ile çözümlenmeye çalışılacak, bu suretle giderilemeyen uyuşmazlıkların hallinde T.C. Ankara Mahkemeleri ve İcra Daireleri yetkili olacaktır.

8. Bu protokol, bu madde dâhil sekiz maddeden ibarettir.

	……
MİLLÎ SAVUNMA BAKANLIĞI ADINA	**FİRMASI ADINA**
YETKİLİ PERSONELİN	YETKİLİ PERSONELİN
ADI SOYADI :	ADI SOYADI :
RÜTBESİ :	UNVANI :
GÖREVİ :	FİRMA KAŞESİ :
İMZA VE TARİH :	İMZA VE TARİH :

EK-K

(İptal edilmiştir)

EK-L

(Türkçe ve İngilizce Belge, tek bir belge şeklinde hazırlanabilir)

BELGE NU.: ……/……

T.C.
MİLLÎ SAVUNMA BAKANLIĞI
ANKARA

TESİS GÜVENLİK BELGESİ

TÜRKİYE CUMHURİYETİ SAVUNMA SANAYİİ MİLLÎ GÜVENLİK MAKAMI tarafından, **……...** adresinde yerleşik,

……
……..'ne

Savunma sanayii ile ilgili faaliyetleri düzenleyen yürürlükteki 5202 sayılı Kanun ve ilgili mevzuat ile NATO Güvenlik Talimatı esaslarına göre tesis güvenliği denetimi yapılmıştır. "……" gizlilik derecesine uygun olarak, gizlilik dereceli bilgi, belge, proje, malzeme ve teçhizatı korumaya yönelik olarak alınan önlemlerin ve mevcut uygulamaların yeterli olduğu, ……. bünyesinde hazırlanan Tesis Özel Güvenlik El Kitabında yer alan güvenlik sisteminin oluşturularak uygulandığı ve

"……" gizlilik dereceli bu belgenin

... / ... / ..... tarihine kadar

geçerli olduğu TASDİK OLUNUR.

MİLLÎ SAVUNMA BAKANI NAMINA

(Adı Soyadı)
(Rütbesi)
Müsteşar Yardımcısı

DOCUMENT NUMBER: ……/……

MINISTRY OF NATIONAL DEFENCE
OF THE REPUBLIC OF TÜRKİYE
FACILITY SECURITY CLEARANCE CERTIFICATE

This is to certify that the National Security Authority for Defence Industry granted

……
……..

Located at **……** **"……..."** Security Clearance according to Law No: 5202 on Defence Industrial Security, rules and regulations of the security activities for Defence Industry. The National Security Authority for Defence Industry confirms that the facility referred in paragraph above, possesses the capabilities for safeguarding of classified information, documentation, projects, materials and equipment at

"……" level. This certificate is

valid until ... / ... / .....

ON BEHALF OF MND.

(Full Name)
(Rank)
Deputy Undersecretary

EK-M

ÜRETİM İZİN BELGESİ BAŞVURU YAZISI

(Yazıya, hazırlayan tarafından uygun gizlilik derecesi

verilecektir.) Kuruluşun Adı ve Adresi

SAYI : …… *Tarih:* … / … / ….

KONU: Üretim İzin Belgesi Başvurusu.

MİLLÎ SAVUNMA BAKANLIĞI
TEKNİK HİZMETLER GENEL MÜDÜRLÜĞÜ

1. 5201 sayılı "Harp Araç ve Gereçleri ile Silah, Mühimmat ve Patlayıcı Madde Üreten Sanayi Kuruluşlarının Denetimi Hakkında Kanun" gereği yayımlanan Kontrole Tâbi Listenin …….maddesi kapsamındaki .....ürün ve malzemenin (gerekirse bu dilekçeye EK yapılarak izin istenen malzeme ve teçhizat detaylı olarak tanımlanmalıdır) üretimini yapabilmek için Üretim İzin Belgesi almak istiyoruz.

2. İstenen bilgi ve belgeler EK'te sunulmuş olup, gereğinin yapılmasını arz ederiz.

Genel Müdür (Adı Soyadı, İmza)

Yönetim Kurulu Başkanı (Adı Soyadı, İmza)

EKİ :
(İstenen Bilgi ve Belgeler)

ÜRETİM İZİN BELGESİ PROTOKOLÜ **EK-N**

..... FİRMASININ, ÜRETİM İZNİ VERİLMESİ AMACIYLA İNCELENMESİ, DEĞERLENDİRİLMESİ VE BELGELENDİRİLMESİ HİZMETİNİN MİLLÎ SAVUNMA BAKANLIĞINCA 3212 SAYILI KANUNA UYGUN OLARAK ÜCRETİ MUKABİLİ YAPILMASINA İLİŞKİN PROTOKOLDUR.

1. PROTOKOLÜN TARAFLARI:

Bu protokolde taraflar; Millî Savunma Bakanlığı Teknik Hizmetler Genel Müdürlüğü ile …….....…. olup, Savunma Sanayii Millî Güvenlik Makamı ve Firma olarak isimlendirilmişlerdir.

2. AMAÇ:

Firmanın, Üretim İzin Belgesi alma talebine esas teşkil eden faaliyetlerinin incelenmesi, değerlendirilmesi ve belgelendirilmesi hizmetinin, ücreti mukabili yapılmasında tarafların yerine getireceği hususları belirlemektir.

3. KAPSAM:

Bu Protokol, üretim izni talep eden Firma ile Savunma Sanayii Millî Güvenlik Makamı arasında yapılacak çalışma ile müteakip dönemde gerçekleştirilebilecek denetlemelere ilişkin esas ve usulleri kapsar.

4. GENEL:

a. Üretim İzin Belgesi; 5201 sayılı Kanun ve Yönetmeliği gereği üretimi Millî Savunma Bakanlığı iznine tâbi harp araç, gereç, silah, mühimmat ve malzeme kapsamında değerlendirilebilecek bir sistem veya malzemeyi üretmek isteyen kuruluşlardan istenilen şartları sağlayanlara verilen bir belgedir. Belgelendirme işlemlerinin başlatılabilmesi için kuruluşun, uygun gizlilik dereceli bir Tesis Güvenlik Belgesine sahip olması veya belge almak amacıyla müracaatta bulunmuş olması gerekir. Üretim İzni verilebilmesi için kuruluşun, Tesis Güvenlik Belgesini almış olması şartı aranır.

b. Bu protokol gereği yapılacak inceleme ve Savunma Sanayii Millî Güvenlik Makamı koordinasyonunda teşkil edilen heyetin tesisleri denetlemesini müteakip tanzim edilebilecek belgeye istinaden verilebilecek bilgi, belge ve malzemenin korunması ve personel güvenliği ile ilgili işlemler bakımından Firma, Savunma Sanayii Millî Güvenlik Makamına karşı sorumludur. Güvenlik önlemlerinin yetersizliği veya gizlilik dereceli bilgi, belge veya malzemenin istenmeyen üçüncü şahıslara verilmesi nedeniyle oluşabilecek her türlü mağduriyet, firma tarafından tazmin edilir.

c. Firma, bu protokolde ve yürürlükteki Millî Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesinde belirtilen bütün tanımları, hüküm, şartları ve açıklamaları aynen kabul eder. Söz konusu tanımların, hüküm ve şartlar ve açıklamaların Savunma Sanayii Millî Güvenlik Makamınca değiştirilmesi durumunda herhangi bir tazminat talep etmeyeceğini kabul ve beyan eder. Firmanın kabiliyetleri çerçevesinde Üretim İzin Belgesi verilmiş olması, firmanın idarenin düzenleyeceği tedarik ihalelerinde öncelik kazanması ve/veya her defasında ihaleye davet edilmesi anlamına gelmez.

5. FİRMANIN YERİNE GETİRECEĞİ HUSUSLAR:

a. Üretim İzin Belgesi için Savunma Sanayii Millî Güvenlik Makamına yaptığı başvuruda, 5201 sayılı Kanun gereği yayımlanan "Kontrole Tâbi Tutulacak Harp Araç Ve Gereçleri İle Silah, Mühimmat Ve Bunlara Ait Yedek Parçalar, Askerî Patlayıcı Maddeler, Bunlara Ait Teknolojilere İlişkin Listesi"ndeki ürünlerden hangisini ürettiğini/üreteceğini ve üretime ilişkin kapasite raporları ile üretim hattı bilgilerini açık bir şekilde belirtir.

b. Firma, tesislerinin incelenmesine yönelik bu yönergenin 7. Bölüm 1.e. (1) maddesinde belirtilen ücreti yatırır ve makbuzunu Savunma Sanayii Millî Güvenlik Makamına gönderir.

c. Üretim izni dosyasının incelenmesi ve üretim tesislerinin denetlenmesi sonucunda; mevcut imkân ve kabiliyetleri yeterli görülürse Firma; belgelendirme işlemine yönelik bu yönergenin 7. Bölüm 1.e.(2) maddesinde belirtilen ücreti yatırır ve makbuzunu Savunma Sanayii Millî Güvenlik Makamına gönderir.

ç. Yapılan inceleme ve denetlemede, tespit edilen eksikliklerin giderilmesine yönelik olarak firmanın talepte bulunması durumunda; Savunma Sanayii Millî Güvenlik Makamınca, ek süre verilebilir.
d. İkinci denetlemenin yapılabilmesi için Firma, bu yönergenin 7. Bölüm 1.e.(3) maddesinde belirtilen ücreti yatırır ve makbuzunu Savunma Sanayii Millî Güvenlik Makamına gönderir. Test ve denemelerle ilgili her türlü masraf, Firma tarafından karşılanır.

6. SAVUNMA SANAYİİ MİLLÎ GÜVENLİK MAKAMI TARAFINDAN YERİNE GETİRİLECEK HUSUSLAR:

a. İnceleme ücretinin yatırılması ve istenen belge ve bilgilerin tamamlanmasını müteakip işlemler başlatılır ve bir teknik heyet oluşturularak, uygun görülecek bir tarihte tesisler denetlenir.
b. Yapılan denetlemenin sonucunun olumlu olması ve diğer şartların da sağlandığının belirlenmesi durumunda, Firma için Üretim İzin Belgesi tanzim edilmesine yönelik rapor düzenlenir ve MSB onayı alınır.
c. Firmanın belgelendirme ücretini yatırarak makbuzunu göndermesi ve aranan diğer isteklerin de karşılandığının belirlenmesi durumunda, Üretim İzin Belgesi tanzim edilir.
ç. Mevcut imkân ve kabiliyeti yeterli bulunmayan, fakat diğer şartları sağlayan kuruluşlara talep etmeleri hâlinde ek süre verilebilir.
d. Ek süre verilen kuruluşun, eksiklerini giderdiğini yazılı olarak bildirmesi ve gereken ücreti yatırarak makbuzunu Savunma Sanayii Millî Güvenlik Makamına göndermesini müteakip, uygun görülecek bir tarihte denetim ve doğrulamalar yeniden yapılır. Bunlardan olumlu sonuç alınması ve diğer şartların da karşılanması hâlinde Üretim İzin Belgesi tanzim edilir.
e. İkinci denetleme olumsuz sonuçlandığı takdirde başvuru iptal edilir.

7. UYUŞMAZLIKLARIN HALLİ:

Bu protokolün uygulanması sırasında doğacak uyuşmazlıklar, karşılıklı görüşmeler yolu ile çözümlenmeye çalışılacak, bu suretle giderilemeyen uyuşmazlıkların hallinde T.C. Ankara Mahkemeleri ve İcra Daireleri yetkili olacaktır.

8. Bu protokol, bu madde dâhil sekiz maddeden ibarettir.

	……
MİLLÎ SAVUNMA BAKANLIĞI ADINA	**FİRMASI ADINA**
YETKİLİ PERSONELİN	YETKİLİ PERSONELİN
ADI SOYADI :	ADI SOYADI :
RÜTBESİ :	UNVANI :
GÖREVİ :	FİRMA KAŞESİ :
İMZA VE TARİH :	İMZA VE TARİH :

EK-O

BELGE NU.: ……/……

T.C.
MİLLÎ SAVUNMA BAKANLIĞI ANKARA
ÜRETİM İZİN BELGESİ

TÜRKİYE CUMHURİYETİ SAVUNMA SANAYİİ MİLLÎ GÜVENLİK MAKAMI TARAFINDAN, **……...**
adresinde konuşlandırılmış;

……
……
……
…..

HARP ARAÇ VE GEREÇLERİ İLE SİLAH, MÜHİMMAT VE PATLAYICI MADDE ÜRETEN SANAYİ KURULUŞLARININ DENETİMİ HAKKINDAKİ 5201 SAYILI KANUNA GÖRE GEREKLİ DENETİMLER YAPILMIŞ OLUP,

ANILAN KURULUŞA; ……. tarihli ve …… sayılı Resmî Gazetede yayımlanan "Kontrole Tâbi Tutulacak Harp Araç ve Gereçleri ile Silah, Mühimmat ve Bunlara Ait Yedek Parçalar, Askerî Patlayıcı Maddeler, Bunlara Ait Teknolojilere İlişkin Liste"nin,"……"başlıklı **……...……** kapsamında, "……" üretimini gerçekleştirebilmesi için,

ÜRETİM İZNİ'nin verildiği

TASDİK OLUNUR.

... / ... / .....

MİLLÎ SAVUNMA BAKANI NAMINA

(Adı Soyadı)
(Rütbesi)
Müsteşar

EK-Ö

(İptal edilmiştir)

EK-P

(İptal edilmiştir)
Kuruluşun Adı ve Adresi

SAYI : …… *Tarih:* … / … / ….

KONU: İthalat İzni Başvurusu.

MİLLÎ SAVUNMA BAKANLIĞI
TEKNİK HİZMETLER GENEL MÜDÜRLÜĞÜ

İLGİ: ……..

1. İlgi sözleşme *(veya proje)* kapsamında aşağıda cins ve miktarı belirtilen …….. G.T.İ.P. numaralı malzemeyi ……. ülkesinde yerleşik …….. 'dan ithal etmek istiyoruz.

2. İstenen bilgi ve belgeler EK'te sunulmuş olup, gereğinin yapılmasını arz ederiz.

Genel Müdür (Adı Soyadı, İmza)	Yönetim Kurulu Başkanı (Adı Soyadı, İmza)

EKİ :
(İstenen Bilgi ve Belgeler)

İTHAL EDİLECEK MALZEMENİN CİNS VE MİKTARI:
1. …….

2. …….

3. …….

4. …….

EK-R

GEÇİCİ İTHAL BELGESİ

THE REPUBLIC OF TÜRKİYE MINISTRY OF NATIONAL DEFENCE

TEMPORARY IMPORT CERTIFICATE

1. Name and Address of Applicant:

2. Name and Address of Exporter :

3. Contract or Order Reference: Date:

4. Articles/Data:

We certify that we have placed an order with the person named in item 2 for the following articles/data in the quantity and value shown below:

Quantity	Articles/data description	Value

5. To be used for the following purpose(s)

6. Validation
Time Starting Date: Expiry Date:

7. Certification of Consignee :

We certify that we are importing the articles/data listed in item 4 for the purposes stated in item 5. We undertake not to sell, lend or deliver to any third party under any conditions whatsoever, with or without compensation, temporarily or permanently, the articles listed in item 4 including equipment and spares delivered in connection with the after-sales support, documentation and operating manuals.

Signature of official of consignee :
Date signed :
Name & title of signer :

8. Certification of Temporary - User

We undertake not to authorise the re-export, resale or other disposition of the articles listed in item 4 including equipment and spares delivered in connection with the after-sales supports, documentation and operating manuals outside the country, for the time period shown in item 6, except to the exporting country.

Signature of official consignee :
Date signed :
Name & title of signer

GEÇİCİ İTHAL BELGESİ DOLDURMA TALİMATI

1. Name and Address of Applicant:
Malzemeyi geçici olarak ithal edecek kuruluşun adı ve açık adresi yazılır.

2. Name and Address of Exporter:
Malzemeyi temin eden kuruluşun (İhracatçının) adı ve açık adresi yazılır.

3. Contract or Order Reference:
Geçici olarak ithal edilecek malzemenin sipariş veya sözleşme numarası yazılır.

4. Articles/Data:
Tedarik edilecek malzemelerin cins ve miktarı belirtilerek tanımı yapılır.

5. To be used for the following purpose(s):
Geçici ithalatın hangi amaçla yapılacağı belirtilir.

6. Validation Time:
Geçici ithal belgesinin geçerlik süresi belirtilir.

Starting Date:
Malzemenin ithal edilebileceği dönemin başlangıç tarihini gösterir.

Expiry Date:
İthal edilecek malzemenin Türkiye'de bulundurulabileceği son tarihi gösterir.

7. Certification of Consignee:
Bu kısım, ithalatçı kuruluş yetkilisince doldurularak onaylanır.

8. Certification of Government:
Bu kısım, Savunma Sanayii Millî Güvenlik Makamı olan MSB.Teknik Hizmetler Genel Müdürlüğünce doldurularak onaylanır.

THE REPUBLIC OF TÜRKİYE
MINISTRY OF NATIONAL DEFENCE

EK-S

SON KULLANICI BELGESİ
END-USER CERTIFICATE

1. Name and Address of Applicant:

2. Name and Address of Exporter:

3. Name and Address of End User:

4. Contract or Order Reference: Date:

5. Articles/Data:

We certify that we have placed an order with the person named in item 2 for the following articles/data in the quantity and value shown below:

Quantity	Articles/data description	Value

6. To be used for the following purpose(s) :

7. Certification of Consignee :

We certify that we are importing the articles/data listed in item 5 for delivery to the end-user in item 3. We undertake not to sell, lend or deliver to any third party under any conditions whatsoever, with or without compensation, temporarily or permanently, the articles listed in item 5 including equipment and spares delivered in connection with the after-sales support, documentation and operating manuals, without the prior written approval of the .....

Signature of official of consignee : Date signed :

Name & title of signer :

8. Certification of End-User :

We certify that we are the end-user of the articles/data listed in item 5. We undertake not to sell, lend or deliver to any third party under any conditions whatsoever, with or without compensation, temporarily or permanently, the articles/data listed in item 5 including equipment and spares, delivered in connection with the after-sales support, documentation and operating manuals, without the prior written approval of the .....

Signature of official of consignee : Date signed :

Name & title of signer :

9. Certification of Government :

We undertake not to authorise the re-export, resale or other disposition of the articles listed in item 5 including equipment and spares delivered in connection with the after-sales supports, documentation and operating manuals outside the country in item 3 without the prior written approval of the …….....

Signature of official of consignee : Date signed :

Certification of Government :

SON KULLANICI BELGESİ DOLDURMA TALİMATI

1. Name and Address of Applicant:
Malzemeyi ithal edecek kuruluşun adı ve açık adresi yazılır.

2. Name and Address of Exporter:
Malzemeyi temin eden kuruluşun (İhracatçının) adı ve açık adresi yazılır.

3. Name and Address of End-User:
Malzemenin son kullanıcısı olan kuruluşun adı ve açık adresi yazılır.

4. Contractor Order Reference:
Malzemenin sipariş numarası yazılır.

5. Articles/Data:
Tedarik edilecek malzemenin tanımı yapılarak, miktar ve alım bedeli yazılır.

6. To be used for the following purpose:
İthal edilecek malzemenin hangi amaçla kullanılacağı yazılır.

7. Certification of Consignee:
Bu kısım, malzemeyi ithal edip son kullanıcıya ulaştıracak olan kuruluş tarafından onaylanır.

8. Certification of End-User:
Bu kısım, son kullanıcı tarafından onaylanır. İthal edilen malzeme başka bir malın imalinde kullanılacak komple veya yarı komple malzeme, ara mamul veya parça ise son kullanıcı, nihaî ürünü üreten ana yüklenici olduğundan bu kısım anılan kuruluş tarafından doldurularak onaylanır. İthal edilen mal doğrudan TSK'ya teslim edilecekse bu kısım, İhtiyaç Makamının yetkili Birimi tarafından doldurulur ve onaylanır.

9. Certification of Government:
Bu kısım, Savunma Sanayii Millî Güvenlik Makamı olan MSB Teknik Hizmetler Genel Müdürlüğünce doldurularak onaylanır.

REQUEST FOR VISIT EK-Ş

( ) One-time
( ) Recurring
( ) Emergency
( ) Amendment

Annex(es)
( ) Yes: ---
( ) No

	ADMINISTRATIVE DATA
1.	REQUESTER DATE : … / … / … TO: VISIT ID:
2.	REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY NAME : POSTAL ADDRESS : TELEX/FAX NO. : TELEPHONE NO.: POINT OF CONTACT:
3.	GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED NAME : ADDRESS : TELEX/FAX NO. : TELEPHONE NO.: POINT OF CONTACT:
4.	DATE OF VISIT : TO:
5.	TYPE OF VISIT : (SELECT ONE FROM EACH COLUMN) ( )GOVERNMENT INITIATIVE ( ) INITIATED BY REQUESTING AGENCY OR FACILITY ( )COMMERCIAL INITIATIVE ( ) BY INVITATION OF THE FACILITY TO BE VISITED
6.	SUBJECT TO BE DISCUSSED/JUSTIFICATION:
7.	ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED:
8.	IS THE VISIT PERTINENT TO: SPECIFIY: A SPECIFIC EQUIPMENT OR WEAPON SYSTEM ( ) FOREIGN MILITARY SALES OR WEAPON SYSTEMS ( ) A PROGRAMME OR AGREEMENT ( ) A DEFENCE ACQUSITION PROCESS ( ) OTHER ( )
9.	PARTICULARS OF VISITORS NAME : DATE OF BIRTH : … / … / … PLACE OF BIRTH : SECURITY CLEARANCE: ID/PP NUMBER: NATIONALITY : POSITION : COMPANY/AGENCY :

REQUEST FOR VISIT (CONTINUATION)

NAME :
DATE OF BIRTH : … / … / … PLACE OF BIRTH :
SECURITY CLEARANCE: ID/PP NUMBER: NATIONALITY :
POSITION :
COMPANY/AGENCY :

10. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY
NAME : TELEPHONE NUMBER :
ADDRESS :
SIGNATURE :

11. CERTIFICATION OF SECURITY CLEARANCE :

NAME :

ADDRESS :

STAMP

TELEPHONE : 90-312-410 6132

SIGNATURE :

FAX : 90-312-417 5488

12. REQUESTING NATIONAL SECURITY AUTHORITY :

NAME :

ADDRESS :

STAMP

TELEPHONE : 90-312-410 6102

SIGNATURE :

FAX : 90-312-417 5488

13. REMARKS:

REQUEST FOR VISIT (CONTINUATION)

() Bir Günlük
() Tekrarlanan
() Acil
() Değişiklik

Ek(ler)
( ) Evet: ---
( ) Hayır

İDARİ BİLGİ

1. TALEPTE BULUNAN TARİH : … / … / …
ZİYARET NO. :

2. TALEPTE BULUNAN HÜKÜMET MAKAMI VEYA SANAYİ TESİSİ
İSİM :
POSTA ADRESİ :
TELEKS/FAKS NO. : TELEFON NO.:
TEMAS NOKTASI :

3. ZİYARET EDİLECEK HÜKÜMET MAKAMI VEYA SANAYİ TESİSİ
İSİM :
ADRES :
TELEKS/FAKS NO. : TELEFON NO.:
TEMAS NOKTASI :

4. ZİYARET TARİHLERİ :

5. ZİYARET TİPİ : (HER BİR SÜTUNDAN BİRİNİ SEÇİNİZ)
( ) HÜKÜMET GİRİŞİMİ ( ) TALEPTE BULUNAN MAKAM VEYA TESİS TARAFINDAN BAŞLATILMIŞ

( ) TİCARİ GİRİŞİM ( ) ZİYARET EDİLECEK TESİSİN DAVETİ İLE

6. GÖRÜŞÜLECEK KONU/DOĞRULAMA:

7. YER ALACAK GİZLİLİK DERECELİ BİLGİNİN SEVİYESİ:

8. ZİYARET NE İLE İLGİLİ: BELİRTİNİZ:
BİR BELİRLİ EKİPMAN VEYA SİLAH SİSTEMİ ( )
YABANCI ASKERİ SATIŞLAR VEYA SİLAH SİSTEMLERİ ( )
BİR PROGRAM VEYA ANLAŞMA ( )
BİR SAVUNMA TEDARİK İŞLEMİ ( )
DİĞER ( )

REQUEST FOR VISIT (CONTINUATION)

9. ZİYARETÇİLERİN KİMLİK BİLGİLERİ:

İSİM :
DOĞUM TARİHİ : … / … / … DOĞUM YERİ :
GÜVENLİK KLERANSI : ID/PP NUMARASI: MİLLİYETİ :
GÖREVİ :
ŞİRKET/MAKAM :

İSİM :
DOĞUM TARİHİ : … / … / … DOĞUM YERİ :
GÜVENLİK KLERANSI : ID/PP NUMARASI: MİLLİYETİ :
GÖREVİ :
ŞİRKET/MAKAM :

10. TALEPTE BULUNAN HÜKÛMET MAKAMI VEYA SANAYİ TESİSİNİN GÜVENLİK AMİRİ:

İSİM : TELEFON NUMARASI :
ADRES :
İMZA :

11. GÜVENLİK KLERANSI ONAYI :

İSİM :

ADRES :

MÜHÜR

TELEFON :

İMZA :

FAKS: 90-312-417 5488

12. TALEPTE BULUNAN MİLLÎ GÜVENLİK MAKAMI :

İSİM :

ADRES :

MÜHÜR

TELEFON :

İMZA :

FAKS: 90-312-417 5488

13. GÖRÜŞLER :

REQUEST FOR VISIT (CONTINUATION)

1. Doldurmayınız. (Savunma Sanayii Millî Güvenlik Makamı tarafından doldurulur.)

2. Şehir, ülke, posta kodu ve faks numarası ile birlikte açık olarak yazılır. Temas Noktasının ismi ve telefon numarası belirtilir.

3. Şehir, ülke, posta kodu ve faks numarası ile birlikte açık olarak yazılır. Temas Noktasının ismi ve telefon numarası yazılır.

4. Gün-Ay-Yıl yazılarak planlanan tarih ve süre belirtilir. Eğer mümkünse parantez içerisinde alternatif tarih ve süre yazılır.

5. Belirtilen sütunlardan uygun olanı işaretlenir.

6. Ziyaret sebebi belirtilerek konu hakkında kısa bir açıklama yapılır.

7. İlgili bilginin gizlilik derecesi belirtilir.

8. Uygun kutu işaretlenir, kısaltma kullanılarak proje/program açıklanır.

9. Bu kısımda ziyaretçi kişi/kişiler hakkında bilgi verilir.

NAME : (Soyadı, (virgül) Adı (tam))

DATE OF BIRTH : (Doğum tarihi (Gün-Ay-Yıl)) PLACE OF BIRTH : (Doğum Yeri)
SECURITY CLEARANCE : (Güvenlik Kleransı Statüsü) ID/PP : (Kimlik veya Pasaport No.)
NATIONALITY : (Milliyeti) POSITION : (Görevi)
COMPANY/AGENCY : (Temsil ettiği kuruluş)

10. Bu kısım, ziyaret talebinde bulunan ülke, kuruluş veya Tesisin Güvenlik Yetkilisi tarafından, ad, adres ve telefon numarası yazılarak imzalanır.

11. Doldurmayınız. (Savunma Sanayii Millî Güvenlik Makamı tarafından doldurulur.)

12. Doldurmayınız. (Savunma Sanayii Millî Güvenlik Makamı tarafından doldurulur.)

13. Bu bölüm,

a. Belirli idarî gereksinimler (Önerilen seyahat plânı, otel ve/veya ulaşım talebi),

b. Savunma Sanayii Millî Güvenlik Makamınca gerek görülebilecek notlar (Örnek; "No security objection", vb.),

c. ID Numara değişiklikleri, gibi ihtiyaçlar için kullanılabilir.

NOT:

1. Ziyaret Talebi (Request for Visit (RFV)) formu, yanlışsız ve eksiksiz olarak doldurulmalıdır. Eksik bilgi ile gönderilmesi, talebin işlem süresini geciktirecektir.

2. RFV, bir yılı geçmeyen belirli bir zaman içinde gerçekleştirilen bir seferlik "one-time" ziyaretler ve/veya tekrarlanan ziyaretler "recurring visits" içinkullanılmalıdır.

3. RFV, büyük harflerle ya da daktilo ile yazılmalıdır. Bilgisayar üzerinde RFV'nin işlenmesine, orijinal form ve içerik aynı tutulmak koşuluyla izin verilmektedir.

TÜRKİYE CUMHURİYETİ
MİLLÎ SAVUNMA BAKANLIĞI

SAVUNMA SANAYİ FİRMALARI UZAKTAN ÇALIŞMA SİBER GÜVENLİK ESASLARI

1. GİRİŞ

KOVID-19 salgını sonrası, birçok ulusal ve uluslararası firma uzaktan çalışma yöntemini devreye almış ve bu yeni çalışma yöntemi tüm dünyada yaygınlaşmıştır.

Bu doküman; Savunma Sanayi firmalarının temsilcileri ile müştereken maliyet etkin, pratik, esnek, elastik fakat bir o kadar güvenli bir uzaktan çalışma çözümü üretmek üzere başlatılan çalışmalar neticesinde Bakanlığımızca da uygun ve risklerinin yönetilebileceği seviyede güvenli bulunan bir yöntem geliştirme çalışmaları neticesinde hazırlanmıştır.

Yapılan çalışmalarda; savunma sanayii firmalarının **en fazla Hizmete Özel** gizlilik dereceli projelerde uzaktan çalışma yapabileceği kabul edilmiştir. Daha yüksek gizlilik dereceli bilgilere erişmek için burada belirtilen uzaktan çalışma esasları kullanılmayacaktır.

Bu dokümanda; uzaktan çalışma yönteminin getirdiği riskler ifade edilmiş, her kurumun kendisine ait bir uzaktan çalışma politikası belirlemesi gerektiği vurgulanmış, çalışmalar neticesinde mutabık kalınan kurumsal mimari belirtilmiş, alınması gereken güvenlik sıkılaştırma ve kontrol tedbirler sıralanmış, mutabık kalınan mimariye yönelik yapılan risk analizi ve risk çözümlemesi sunulmuştur.

Dokümanda belirtilen hususlar statik her zaman geçerli olan kurallar olmayıp, uyulması gereken asgari siber güvenlik tedbirlerini ifade etmektedir. Kendisine uzaktan çalışma izni verilen savunma sanayii firmaları risk yönetimi anlayışı ile burada belirtilen tedbirleri sürekli olarak geliştirmeli, uygulanacak olan uzaktan bağlantıda TÜBİTAK Bilgem tarafından geliştirilen Millî VPN kullanımı öncelikli olarak tercih edilmelidir.

Bu kapsamda uzaktan çalışacak her firma; uzaktan çalışma politikasını belirlemeli, asgari bu dokümanda belirtilen güvenlik sıkılaştırma ve kontrol tedbirlerini yerine getirmeli ve düzenli olarak icra edecekleri risk analizleri ve yılda en az bir kez icra edilecek sızma testleri ile alınan tedbirlerinin yerindeliğini teyit etmelidir.

Sonuç olarak;

a.Savunma sanayii firmalarına ilgili mevzuatta gerekli değişikliğin yapılmasını müteakip en fazla Hizmete Özel gizlilik dereceli bilgilere erişmek için uzaktan çalışma izni verilebileceği,

b. Uzaktan çalışma izni verilecek firmalar tarafından asgari bu dokümanda yer alan siber güvenlik tedbirlerinin uygulanması ile risklerin azaltılabileceği, ancak **tüm tedbirler alınsa bile uzaktan çalışma nedeniyle kaynaklanabilecek risklerin tamamen ortadan kaldırılmasının mümkün olmadığı hususunun** uzaktan çalışma iznini verecek makam tarafından göz önünde bulundurulmasının uygun olacağı değerlendirilmektedir.

2. UZAKTAN ÇALIŞMANIN GÜVENLİK RİSKLERİ

Savunma Sanayi firmaları, kendi tesislerinde sistem ve ürün geliştirme faaliyetlerini icra ederken bilgi güvenliği kapsamında fiziksel, personel, bilgi sistemleri ve belge güvenliği kapsamında birçok güvenlik kontrolünü icra etmektedir.

Fiziksel güvenlik kapsamında güvenlik görevlileri, kameralar, giriş/çıkış aramaları, giriş kartları vb. gibi önlemler sadece tesisin değil aynı zamanda o tesis içinde üretilen bilginin de güvenliğini sağlamak üzere kullanılmaktadır. Bu kapsamda;

- Personel güvenliği kapsamında personelin tüm hareketleri kontrol edilmekte, izlenmekte ve olağan dışı davranış sergileyenler istihbarata karşı koyma tedbirleri altında takip edilmektedir.
- Belge güvenliği kapsamında gizlilik dereceli veya hassas bilgi ve belgeler kilitli dolaplarda korunmakta, bilmesi gereken prensibine göre sadece yetkili kişilerce görülmesi sağlanmaktadır.
- Bilgi sistemleri güvenliği kapsamında ise siber güvenlik tedbirleri ile dijital ortama taşınan her türlü bilgi ve sistem siber ortamdan gelebilecek tehditlere karşı ağ

güvenliği, sınır güvenliği, uç nokta güvenliği, veri tabanı güvenliği, uygulama güvenliği gibi çeşitli güvenlik tedbirleri ile korunmaktadır.

Çalışma ortamının güvenli tesis ortamından ev, otel, hava alanı, alışveriş merkezi, kütüphane, restoran gibi yerlere taşınması durumunda, tesis güvenliği kapsamında alınan birçok güvenlik tedbirinden mahrum kalınacağı için ilave güvenlik riskleri ortaya çıkacaktır.

Firmaların kendi çalışma ortamlarında tesis edilen güvenlik tedbirleri kapsamında kullanılan bilgi sistem malzemelerinden, iletişim ortamına kadar erişim kontrolü, kimlik kontrolü, kriptolu haberleşme, güçlü şifre politikası, zararlı yazılım, saldırı tespit ve önleme sistemleri gibi birçok güvenlik kontrolü firmanın güvenlik birimlerince alınmaktadır. Fakat evden veya uzaktan çalışma esnasında bu tür güvenlik tedbirlerinin birçoğu kullanılamayacaktır.

Uzaktan çalışılırken kullanılan ağlar firma dışında bir yapı tarafından kurulduğu için güvenlik terbilerine ilişkin bir güvence yoktur. Hatta havalimanı, hotel, alışveriş merkezi gibi bazı toplu alanlarda saldırganların özellikle sahte Wi-Fi noktaları veya sahte GSM istasyonları kurarak o bölgedeki trafiği üzerlerinden geçirip takip ettikleri bilinmektedir. İlave olarak bu tür yerlerdeki ağ altyapılarında, öncelik güvenlikten ziyade elverişlilik ve kullanılabilirlik olduğundan dolayı çoğunlukla yeterli güvenlik tedbirleri alınamamaktadır. Bu nedenle ilgili firma, bu tür alanlardan yapılabilecek bir uzaktan çalışma senaryosunda o alandaki güvenlik tedbirlerinin artırılmasına yönelik bir etkisi olmayacağından dolayı kendi güvenlik önlemini almak durumundadır.

Uzaktan çalışacak personel firmanın kendi tesislerinde kurduğu güvenlik önlemlerinden mahrum kalacağından dolayı yaptığı her işlem, ürettiği her veri, şifre gibi hassas verileri yeterli güvenlik tedbirlerinin alınamaması durumunda saldırganların kolaylıkla hedefi haline gelecektir.

İlave olarak uzaktan çalışan personelin iş ve kişisel işlemleri arasındaki keskin çizgiler bulanıklaşacak, kurumsal işleri için kendisine tahsis edilen bilgisayardan kişisel işlemlerini de yapabilir duruma gelecek veya kişisel ev ağından işine yönelik işlemlerini yapıyor duruma gelebilecektir. Bu tür bir durum özellikle gizlilik dereceli bilgileri içeren bir işlemin %100 kayıt altına alınması ve takip edilmesi gibi güvenlik politikaların uygulanması gereken durumlarda kişisel verilerin korunması kapsamında kişisel ve kurumsal verilerin ve işlemlerin ayrıştırılmasına yönelik ilave riskler ve güçlükler çıkaracaktır.

Özellikle uzaktan çalışmanın evden yapıldığı durumlarda, evlerdeki artan nesnelerin interneti cihazlarının sayısının artması ile beraber akıllı televizyon, robot süpürge, eğlence sistemleri gibi ev internet ağını kullanan ve sıklıkla güncelleme almadıkları için güvenliği çok zayıf olan nesnelerin interneti cihazlardan dolayı saldırı yüzeyi artabilecek ve evden yapılan kurumsal işlemlere ve üretilen/işlenen veriye yönelik ilave riskler ortaya çıkabilecektir.

Firmalarda, kurumsal ağlar ve bilgi sistemleri üzerinde kişisel işlemlerin yapılmasına yönelik kurum politikaları açık ve nettir. Fakat uzaktan çalışma kapsamında işlerin eve taşınması ile beraber kişisel alan ile kurumsal alan arasındaki çizgiler bulanıklaşarak birbirine girmeye başlayacaktır. Örnek olarak;

- Kişisel cep telefonu üzerinden kurumsal bir işe ait e-posta göndermek veya kurumsal laptop üzerinden kişisel bir e-posta göndermek,
- Kurumsal bilgisayar üzerinden evdeki güvenlik kamerasını izlemek,
- Hafta sonu evdeki bilgisayarda kurumsal bir toplantının sonuç raporunu yazıp kurumsal e-postaya göndermek,
- Evde çalışırken kurumsal bilgisayarda Youtube üzerinden müzik dinlemek, film izlemek,
- Çocuğunun futbol antrenmanında kurumsal bir toplantıya firmanın tahsis ettiği cep telefonu üzerinden iştirak etmek.

Uzaktan çalışma yöntemleri ile beraber bu tür faaliyetlerin sayısının artmasının sonucunda kurumsal güvenlik tedbirlerine yönelik sorumluluklar artık firmanın güvenlik birimlerinden yavaşça kişinin kendisine doğru kaymaya başlamaktadır. Uzaktan çalışan kişiler tesis içinde firmanın sağladığı güvenlik tedbirlerini artık kendileri almak zorunda kalacak ve sorumluluk almaya başlayacaktır. Ayrıca, kurum içinde sağlanan çalışma ortamının getirdiği kurum güvenlik kültüründen ve çalışma ortamının güvenlik atmosferinden uzak bir şekilde, daha rahat hissettiği, daha alışık oldukları ev gibi ortamların çevresel faktörleri ile beraber alınacak güvenlik tedbirlerinde kişiler daha rahat ve iltimaslı olabileceğinden dolayı ilave güvenlik riskleri oluşabilecektir.

Uzaktan çalışmanın ülke sınırları dışına çıkması durumunda içinde bulunulan ülkenin çalışma ile ilgili kanun ve yasal mevzuatına uyumluluk konusunda da dikkatli olunması gereklidir. Diğer bir ülkede izin verilenin üzerinde uzatılan oturumlar, geçerli bir çalışma izni olmadan bir ülkede diğer bir ülke adına çalışmak ve korunması gereken kişisel ve kamusal/kurumsal verilerin diğer ülke sınırları içine taşınması gibi hassas ve mutlaka bir hukuk danışmanlığı alınarak yapılması gereken işlerde internet sayesinde sınırların kalktığı uzaktan çalışma yöntemlerinde dikkatli olunması gereklidir.

Yukarıda bir kısmı verilen örnekler her ne kadar iyi niyetli bir davranışın sonucunda ortaya çıksa da fark etmeden güvenlik, kişisel verilerin korunması, ulusal ve uluslararası çalışma izinleri gibi bir takım yasal mevzuatın ihlaline neden olabilecek durumlardır. Bu tür durumlar ile karşılaşmamak için uzaktan çalışma yöntemlerinde tereddüde mahal bırakmayacak açıklık ve netlikle politikaların belirlenmiş olması, eğitim ve farkındalık faaliyetlerinin tüm çalışanlara verilmiş olması gereklidir.

3. UZAKTAN ÇALIŞMA POLİTİKASININ BELİRLENMESİ

Uzaktan çalışmanın etkin ve verimli bir şekilde işletilebilmesi için fiziksel, sosyal ve teknolojik faktörlerin çok iyi yönetilmesi gereklidir.

Etkili bir uzaktan çalışma yönteminin uygulanabilmesi için Savunma Sanayi Firmaları tarafından "**Uzaktan Çalışma Politika Belgesi**" oluşturulmalıdır. Bu belge içinde uzaktan çalışacak firma personelinin uyması gereken kurallar ve uygun davranış modelleri tanımlanırken **bilgi güvenliği, hukuk hizmetleri, personel güvenliği ve fiziksel güvenlikten** sorumlu ilgili birim amirliklerinin katkıları alınmalıdır.

Politika belgesi hazırlanırken en az aşağıdaki hususların belge içinde yer alması sağlanmalıdır.

- Kimler uzaktan çalışabilir? Çeşitli teknik, sosyolojik, yasal sebeplerden dolayı bazı işlerin firma dışında uzaktan çalışılması mümkün değildir. Bu tür durumlarda hangi işlerin ve hangi personelin dışarıda uzaktan çalışmasına müsaade edileceği Uzaktan Çalışma Politika Belgesi içinde açıkça belirtilmelidir.
- Uzaktan çalışmaya yönelik kısıtlar nelerdir? Uzaktan çalışmasına müsaade edilen personelin uyması gereken kısıtlar açık ve net bir şekilde tanımlanmalıdır. Personelin nerede, ne zaman, hangi tür işleri firma dışında yapabileceğine ilişkin hususlar tanımlanmalıdır. Bu maksatla uzaktan çalışma alanlarında havaalanı, kafe/restoran, açık hava park/bahçe vb. gibi kesinlikle kullanılmaması gereken alanlar tanımlanmalıdır.
- Uzaktan çalışacak personel sınırsız bir şekilde istediği yerde çalışabilir mi yoksa içinde bulunulan ülkeye göre belirli kısıtlar var mı?
- Uzaktan çalışacak personel olası bir acil durum nedeni ile firma tesislerinden belirli bir mesafe içinde bulunması gerekli mi?
- Uzaktan çalışacak kişiler tek bir yerde mi kalmalı yoksa hareket halinde çalışabilir mi?
- Uzaktan çalışacak personelin bir zaman limiti var mı? Günde en fazla kaç saat, hangi saatler arasında uzaktan çalışılabilir?

- Uzaktan çalışmaya yönelik iş türlerinde bir kısıt var mıdır? (Örnek: Uzaktan yazılım geliştirilebilir fakat uzaktan test yapılamaz vb. gibi)
- Belirli iş türlerinde uzaktan çalışırken firma tesislerine yakın bir yerde bulunma şartı var mıdır?
- Yurt dışından uzaktan çalışmaya izin var mıdır?
- Uzaktan çalışma için personel ve uzaktan çalışma yapılacak işin tanımlanmasına yönelik bir gözden geçirme ve onay mekanizması var mı? Onay mekanizmasında işi ve uzaktan çalışacak personeli kim onaylamaktadır? Onayın süresi ne kadardır? Onay uzatma süreci nedir?
- Uzaktan çalışma için gerekli donanım ve yazılımı kim sağlayacaktır? Firmanın ve personelin temin ve tedarike yönelik sorumlulukları nedir? Kendi Cihazını Kendin Getir politikası kullanılacak mıdır? Personelin evinde veya diğer alanlarda ihtiyaç duyacağı internet hizmetinin ücretini kim ödeyecektir? Bazı iller için e-imza vb. gibi ihtiyaç duyulabilecek ilave donanımları kim nasıl karşılayacaktır?
- Uzaktan çalışma için kullanılacak donanım ve yazılım altyapısının siber güvenliği için alınması gereken tedbirler ne olmalıdır?
- Uzaktan çalışma maksadıyla kullanılacak bilgisayar donanım ve yazılımın minimum gereksinimleri veya kısıtları nedir?
- Uzaktan çalışma maksadıyla kullanılacak internet bağlantısının minimum bağlantı hızı ne olmalıdır? Kullanılacak İnternet servis sağlayıcılarında bir kısıt var mıdır?
- Firmanın yardım masasının uzaktan çalışan kişilere özellikle şahsi cihazlarını kullanacaklarsa yardım etme politikası ne olacaktır? Bu tür şahsi cihazlar üzerinde yapılandırma yaptırabilecekmidir? Uzaktan çalışma esnasında firma tarafından verilen yazılım ve donanım kullanılırsa uzaktan yardım politikası ne olacaktır?
- Uzaktan çalışacak personelin alması gereken minimum eğitim nedir? Bu eğitimi hangi sıklıkta tekrarlamalıdır?

3.1. GÜVENLİ UZAKTAN ÇALIŞMA ORTAMININ HAZIRLANMASI

Uzaktan çalışmaya izin verilen personel, firma dışındaki çalışma alanının güvenliğini almaktan sorumludur. Bu tür uzak çalışma alanlarında kurumsal veri ve servislerinin sağlanmasına yönelik birçok çevresel faktör dikkat alınması gereklidir. Bu faktörler kurumsal uzaktan çalışma politika belgesi ile bağlayıcılığı sağlanmalı ve kurumsal farkındalık eğitimleri ile desteklenmelidir. Uzaktan çalışacak personel çalışma ortamlarının güvenliğinin sağlanmasının firma için ne kadar önemli olduğunu ve bu tedbirlerin alınmaması durumunda kuruma yaratabilecekleri güvenlik risklerinin ne kadar büyük ölçekli olabileceğini çok iyi anlamalıdır.

Uzaktan çalışacak personel firma tesisleri dışında halka açık, omuz üzerinden veya çevreden üzerinde çalıştıkları kurumsal bilginin görülebileceği, duyulabileceği, odaklanamayacakları kadar gürültülü ve kalabalık ortamlardan uzakta, bu iş için ayrılmış özel bir alan seçmelidir. Uzaktan çalışma esnasında dikkat dağıtabilecek faktörlerden arındırılmış özel bir ortam seçilmelidir. Bu tür özel bir alanın yaratılamayacağı, evdeki aile fertleri veya ev arkadaşı ile paylaşılan bir alanda çalışılmak zorunda kalındığında ekran görüntüsünün, çalışma belgelerinin görülemeyeceği şekilde oda düzenlemesinin yapılması önem arz etmektedir. Mümkünse, uzaktan çalışma için ayrılan bölüm çalışma yapılmadığı zamanlarda kilitlenmelidir. Uzaktan çalışma usulleri içinde iş alanı ile kişisel alanın ayrılması güvenliğin sağlanmasında önemli bir husustur.

3.2. İŞ HAYATI İLE KİŞİSEL HAYATIN AYRILMASI

Uzaktan çalışan personelin iş hayatı ile kişisel hayatı arasındaki sınırlar ortandan kalkarak bulanıklaşır ve iş ile şahsi kişisel meseleler birbirine karşımaya başlayabilir. Bu tür durumlar özellikle firmaların uzaktan çalışma için personeline kendi şahsi cihazlarını kullanmalarına izin verildiği durumlarda daha fazla karşılaşılır.

Kurumsal veri ile kişisel bilgilerin birbirine karşıması hem firma hem de kişiler üzerinde istenmeyen sonuçlar üretebilir. Uzaktan çalışma için kullanılacak yazılım ve donanımın firmalar tarafından sağlanması durumunda bu bilgi teknolojileri üzerinde sadece kurumsal işler yapılmalı, kişisel işlemlerin yapılmamasına özen gösterilmelidir. Bu tür durumlarda firmalar kendi verdikleri donanım ve yazılımlar üzerinde izleme ve kayıt alma gibi doğal hak ve sorumlulukları kapsamında kişisel verilerin de toplanmasına karşı dikkatli olunması gereklidir. Uzaktan çalışma için firmaların personele şahsi yazılım ve donanımlarını kullanmalarına müsaade ettiği durumlarda ise personele iş ve şahsi dosyalar arasındaki yarımın nasıl yapılacağına ilişkin yeterli eğitim verilmelidir. Bu tür durumlarda firmalar personelin şahsi yazılım ve donanımları üzerinde kurumsal veri ve işlemlerin yapılabileceği ayrı ve güvenli bir alanın yaratılması çözümünü tercih etmelidir.

3.3. VİDEO KONFERANS

Uzaktan çalışma esnasında video konferans yöntemi ile bir toplantıya iştirak etmek veya bir diğer personel ile etkileşime girmenin özellikle bir havaalanı, hotel lobisi, restoran vb. gibi halka açık ve kalabalık yerlerde icra edilmesi durumunda ilave bazı riskler ortaya çıkabilmektedir. Bu tür durumlarda uzaktan çalışan personelin yakındaki diğer kişilerin toplantıya ilişkin bilgi ve belgelerin dışarıdan görülmemesi, durulmaması için gerekli tedbirleri alması gereklidir. Bu tür durumlar sadece firmanın uzaktan çalışma politikalarını ihlal olmayıp, saçılan bilginin hassasiyet ve gizlilik derecesine göre daha üst seviyedeki kanun ve yasal mevzuatın da ihlali olabileceğinden daha ciddi problemlere neden olabilecektir.

3.4. HALKA AÇIK ALANLARDA UZAKTAN ÇALIŞMA

Uzaktan çalışmaya yönelik tanımlanacak politikalarda uzak yerin bir ev olması veya halka açık bir alan olması büyük değişikliklere neden olacaktır. Halka açık alanlarda yapılan uzaktan çalışma evden uzaktan çalışmaya nispeten daha fazla güvenlik riski içermektedir. Bu tür alanlarda firmanın ve firma personelinin açık alandaki ağ altyapısı ve fiziksel güvenliğe yönelik herhangi bir etkisi olamayacaktır. Bu tür durumlarda firma personeli mutlaka yeterli ve gerekli güvenlik tedbirlerinin varlığından emin olmalıdır.

Bu tür yerlerde kullanılabilecek halka açık internet bağlantıları en büyük güvenlik riskidir. Bu tür bağlantılar üzerinden yapılabilecek bağlantılarda kullanıcı adı, şifre vb. gibi birçok hassas bilginin üçüncü şahıslar tarafından ele geçirilmesi ihtimali yüksektir. Bu tür yerlerde uçtan uca kriptolu haberleşme imkânları kullanmadan hiçbir şekilde uzaktan çalışmaya yönelik bir bağlantı yapılmamalıdır.

İlave olarak bu tür yerlerde uzaktan çalışırken kullanılan donanımın fiziksel güvenliğinin alınması çok önemlidir. Bilgisayarın hiçbir zaman gözetimsiz bırakılmaması, daima el altında bulunulması, masa üzerinde bırakılarak kahve almaya gidilmesi gibi kontrolsüz bir an yaratılmaması, kullanılmadığı zamanlarda mutlaka şifreli ekran koruyucunun devreye alınması gereklidir.

3.5. GÜVENLİK FARKINDALIK EĞİTİMLERİ

Uzaktan çalışacak firma personeli, özellikle bu tür bir yöntem ile ilk defa iş yapacakları zaman bu tür çalışmanın yaratabileceği güvenlik risklerini yönetebilmek için yoğun ve sürekli bir farkındalık eğitimine alınmalıdır. Özellikle firma tesisleri içindeki ofis ortamının yarattığı güvenlik kültüründen mahrum olacakları uzaktan çalışmanın yaratabileceği gevşeme, göz ardı etme, boşluklardan yararlanma içgüdüsünün yaratacağı güvenlik risklerinin yönetilebilmesi için bu tür eğitimler bir şarttır.

Uzaktan çalışma yöntemlerinin başarılı ve sürdürülebilir bir şekilde yürütülebilmesi için etkin ve verimli bir eğitim gereklidir. Yukarıda bahsedilen politika belgesi firma çalışanlarına uzaktan çalışmaya yönelik sınırları gösterir fakat ancak iyi kurgulanmış bir farkındalık eğitimi firma çalışanlarına bu politikaları ve önemini en iyi şekilde anlamalarını ve uygulamalarını sağlayacaktır. Bu tür eğitimler uzaktan çalışacak personele çalışma izni verilmeden önce bir ön şart olarak sunulmalı ve teknoloji, tehditler değiştikçe eğitim müfredatını da güncel tutacak şekilde periyodik olarak tekrarlanmalıdır.

Eğitim, politika gereği verilmiş olmak için değil, müfredatı ve eğitim veriliş yöntemi verimliliği artıracak şekilde hazırlanmalıdır. Eğitim kapsamında en az aşağıdaki hususlar firma personeline teorik ve pratik olarak verilmelidir.

- Uzaktan çalışma esnasında kullanılacak güvenlik kontrolleri nelerdir ve neden önemlidir? Hangi tehditleri bertaraf etmek için kullanılır?
- Uzaktan çalışırken kullanılacak protokol ve teknolojiler nasıl yapılandırılmalı ve kullanılmalıdır?
- Firma yazılım ve donanımlarının kullanımına yönelik izin verilen ve verilmeyen kullanım şekilleri ve amaçları.
- Uzaktan çalışırken takip edilmesi gereken güvenlik aklı ve davranışları.
- Güvenlik ihlalleri nedir ve nasıl rapor edilmelidir?
- Uzaktan çalışırken ihtiyaç halinde teknik, operasyonel veya güvenlik yardımını talep etme yöntemleri.
- İş hayatı ile kişisel hayat arasında sınırların sağlıklı bir şekilde çizilebilmesi için kullanılacak teknikler.

4. UZAKTAN ÇALIŞMA YÖNTEMİ İÇİN GEREKLİ TEKNİK TEDBİRLER

Uzaktan çalışma esnasında savunma sanayii firmaları tarafından alınacak minimum güvenlik tedbirleri aşağıda belirtilmiştir. Bazı güvenlik kontrollerinde firmalara kendi tedbirlerini belirlemeye yönelik esneklik sağlanırken bazı tedbirlerde standartlaşmaya gidilerek tüm firmalarda benzer tedbirlerin alınması hedeflenmiştir. Uzaktan çalışmaya yönelik güvenlik tedbirleri genel olarak 4 ayrı kategoride tanımlanmıştır

- Uç nokta güvenliği
- Kurumsal veri ve bilginin güvenliği
- İletişim hatlarının güvenliği
- Firmanın bilgi sistem altyapısının güvenliği

4.1. UÇ NOKTA GÜVENLİĞİ

Uç nokta güvenliği kapsamında uzaktan çalışma için kullanılacak bilgisayar, tablet, cep telefonu gibi cihazların güvenliğinin sağlanması hedeflenmektedir. Bu cihazların şahsi veya kurumsal olmasına göre güvenlik tedbirleri değişebilecektir. Özellikle son yıllarda artan siber güvenlik tehditlerinin büyük bir çoğunluğu kişisel siber hijyen seviyesinin düşük olduğu kullanıcıların uç nokta güvenliğine yönelik tedbirleri almaması durumunu istismar etmektedir. Bu nedenle kurumsal verilerin işlendiği uç noktalardaki bilgi işlem donanım ve yazılımlarının korunması uzaktan çalışma güvenliği kapsamında ilk cephedir ve mutlaka en yüksek seviyede alınmalıdır.

Uzaktan çalışma esnasında kullanılacak tüm donanım ve yazılımların yamaları tam olmalı ve bilinen tüm açıklıklara karşı tedbirler alınmış olmalıdır. Güncel yaması tam olmayan hiçbir donanım ve yazılım uzaktan çalışma kapsamında kullanılmamalıdır. Yamalar bahse konu yazılım ve donanımlara periyodik olarak merkezi bir güncelleme sunucusu üzerinden gönderilmeli ve her bağlantı öncesinde tamlığı kontrol edilmelidir.

Uzaktan çalışma kapsamında kullanılacak donanım ve yazılımların varlık yönetimi tam yapılmalı, beyaz listesi hazırlanmalı ve bu liste haricinde donanım ve yazılım kullanılması yasaklanmalıdır.

Firma tarafından uzaktan çalışma esnasında personelin kendi donanım ve yazılım kullanılmasına müsaade edilmemelidir. Fakat bu tür bir müsaadenin verileceği durumlarda personelin kendi yazılım ve donanımlarının bağlantı öncesinde güncelliğinin tam olduğu kontrol edilmelidir.

Uzaktan çalışma esnasında kullanılacak erişim noktası, modem gibi donanımlar üzerinde güvenlik tedbirleri tam olarak alınmalıdır. Özellikle fabrika ayalarında kalan şifreler güçlü şifre politikası kapsamında mutlaka değiştirilmelidir. Bu tür donanımlar üzerinde alınması gereken tedbirler Uzaktan Çalışma Politika Belgesinde mutlaka belirtilmelidir.

Uç noktada kullanılacak bilgisayarlarda veya cihazlarda bulunan güvenlik duvarları aktif hale alınmalı ve bu tür güvenlik duvarlarının yapılandırılmasına yönelik tedbirler Uzaktan Çalışma Politika Belgesinde tanımlanmalıdır. Firma tarafından verilen ve varsayılan olarak yapılandırılan güvenlik duvarlarının ayarlarının personel tarafından değiştirilmesi engellenmelidir.

Uç noktada kullanılacak donanımlarda saldırı tespit ve önleme sitemleri aktif halde tutulmalıdır. Bu donanımlarda kullanıcı davranış modellerini takip ederek davranış analizleri neticesinde hayatın normal akışına aykırı hareketleri tespit edebilecek önlemler alınmalıdır.

Firma tarafından sağlanan donanımların veya yazılımların bozulması durumunda nasıl destek alınabileceğine ilişkin usul ve esaslar tam olarak tanımlanmalıdır. Özellikle uzaktan çalışan personelin kullandığı donanım ve yazılımların güvenlik yapılandırmasına yönelik bir ihtiyaç olduğunda bahse konu alanlarda fiziksel güvenlik tedbirlerinin olmaması ve tehditlere karşı daha fazla maruz kalınabileceği göz önünde bulundurularak destek personeli tarafından öncelikli olarak destek verilmesi sağlanmalıdır. Arızalı donanımların firmaya nasıl getirileceğine ilişkin usul ve esaslar tanımlanmalıdır. İdeal durumda arızalı donanımlar asla firma personeli tarafından üçüncü parti destek firmalarına teslim edilmemeli, firmaya teslim edilmelidir. Fakat istisnai durumlarda desteğin üçüncü taraflar tarafından sağlanması ve donanımın personel tarafından üçüncü taraf destek kurumuna teslim edilmesi gerektiğinde firma bilgisayarının disklerinin güvenliğine yönelik alınması gereken tedbirler Uzaktan Çalışma Politika Belgesinde tanımlanmalıdır.

Uzaktan çalışma kapsamında kullanılan bilgi sistem donanımlarında ekran kilit zamanı 5-10 dakika gibi kısa bir süreye ayarlanmalı ve mutlaka şifre ile tekrar açılacak şekilde önlem alınmalıdır.

4.2. KURUMSAL VERİ VE BİLGİ GÜVENLİĞİ

Uzaktan çalişma esnasında taşınan, işlenen ve üretilen kurumsal veri tüm güvenlik tedbirlerinin odak noktasıdır. Bu nedenle uzaktan çalışma kapsamında işlenen kurumsal verinin çalınma, istismar edilme veya kazara açığa çıkarak bilmemesi gereken kişilerin eline geçmesine neden olabilecek tehdit ve olaylara karşı korunması gereklidir.

Uzaktan çalışma kapsamında kullanılan donanım ve yazılımlarda uç nokta bilgisayarlarda kişisel veriler ile kurumsal veriler birbirleri ile tamamı ile ayrılmalı ve kurumsal veri işlenirken mutlaka şifrelenmiş bir alanda işlem görmeli, donanım veya ağ üzerindeki diğer yazılım ve işlemler (process) tarafından görünmesi ve erişilmesi engellenmelidir.

Uzaktan çalışma esnasında kullanılacak bilgisayar donanımlarında güvenlik maksadıyla kullanılanlar hariç (dongle) USB vb. gibi harici veri depolama cihazlarında yazma özelliğinin kullanılması engellenmelidir. Bu tür cihazlarda okuma özelliğine izin verilmesi durumunda okunan verinin virüs ve zararlı yazılım kontrolünün tam olarak yapılması sağlanmalıdır. Harici depolama donanımlarının kullanılmasının bir gereklilik olduğu durumlarda bu donanımlarda şifreleme özelliğinin kullanılması sağlanmalıdır.

Bulut depolama ortamlarının kullanılmasına yönelik detaylı bir risk analizi yapılmalıdır. Dropbox, OneDrive gibi bulut veri depolama ortamlarının kullanılmasının bir zorunluluk olduğu durumlarda alınacak güvenlik tedbirleri tanımlanmalıdır.

Kimlik doğrulama ve yetkilendirmeye yönelik çok güçlü politikalar tanımlanmalıdır. Uzaktan çalışma esnasında mutlaka çok faktörlü kimlik doğrulama kullanılmalıdır. Sıfır güven ilkeleri kapsamında daha önceden verilen bir yetkilendirme, daha sonra yapılacak benzer bir kaynak kullanım talebinde otomatik olarak yetkilendirmeye mahal vermemeli, her seferinde kimlik doğrulama ve yetkilendirme kontrolü yapılmalıdır.

Kullanılacak şifrelerde en az 12 karakterli, en az 1 adet rakam, büyük/küçük harf ve özel karakter içeren güçlü şifre politikası kullanılmalıdır. Personelin kişisel veya güvenlik seviyesinin düşük olduğu başka servisler için kullandığı şifreleri uzaktan çalışma kapsamında kullanmamasına yönelik tedbirler alınmalıdır.

Uzaktan çalışma kapsamında firma personeline verilen bilgisayar ve tabletlerin güvenliğini sağlamak ve takip etmek maksadıyla mobile cihaz yönetimi (Mobile Device Management) ve mobil uygulama güvenliği (Mobile Application Management) gibi kabiliyetler kullanılmalıdır.

4.3. İLETİŞİM HATLARI GÜVENLİĞİ

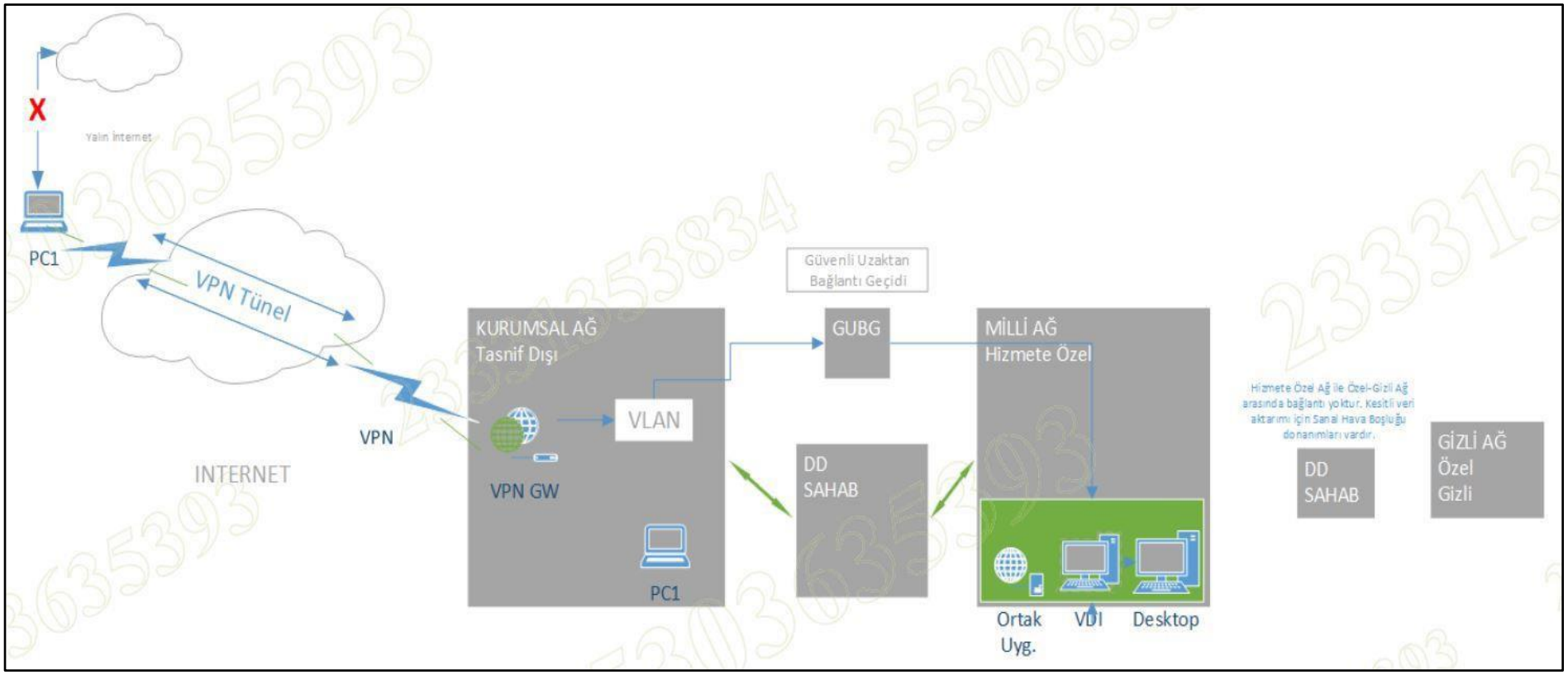
İletişim hatları güvenliği, uzaktan çalışma kapsamında bulunulan yer ile firma tesisleri arasındaki iletişim katmanının güvenliğine yönelik tedbirleri içermektedir. Bu kategori uzun yıllardır tehditlere karşı tecrübe kazanılan alan olması nedeni ile kriptolu haberleşme teknikleri kullanılarak alınan güvenlik tedbirleri büyük bir oranda riskleri ortadan kaldırabilmektedir. Bu maksatla TÜBİTAK tarafından geliştirilen Millî VPN kullanılacaktır.

4.4. KURUM BİLGİ SİSTEM ALTYAPISI GÜVENLİĞİ

Uzaktan çalışan personelin kurum bilgisini alması veya oluşturduğu kurumsal veriyi kurumsal veri tabanına tekrar yükleyebilmesi için kurumsal bilgi sistem altyapısının ve veri tabanlarının uzaktan çalışacak personele bağlanması, firmanın bilgi sistem altyapısına dışarıdan ulaşılabilmesi için bir vektör yaratmaktadır. Bu nedenle firma veri tabanlarının uzaktan çalışma kapsamında oluşabilecek tehditlere karşı korunması gereklidir.

Yukarıda verilen her bir kategoride güvenlik tedbirleri tanımlanmalı ve istisnasız uygulanmalıdır.

5. Uzaktan Çalışma için Kavramsal Mimari



Şekil-1 Uzaktan Çalışma için Kavramsal Mimari

Açıklamalar :

DD : Diyot
SAHAB : Sanal Hava Boşluğu
GUBG : Güvenli Uzaktan Bağlantı Geçidi
VPN GW : Sanal Özel Ağ Geçidi (Virtual Private Network Gateway)
Uzaktan bağlantı yapılırken TÜBİTAK BİLGEM tarafından geliştirilmiş Millî VPN kullanılmalıdır.

6. Uzaktan Çalışma Mimarisi Güvenlik Sıkılaştırma ve Kontrol Listesi

Uzaktan erişim kapsamında Şekil-1'de yer alan Uzaktan Bağlantı Yapan İstemci (PC1), Uzaktan Erişim Altyapısı, Uzaktan Erişim Altyapı Sunucuları ve Güvenli Uzaktan Bağlantı Geçitlerini kapsayacak şekilde uygulanacak güvenlik sıkılaştırma ve kontrol listesi aşağıda yer almaktadır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
1	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.1 - Uzaktan Çalışma Politikasının Hazırlanması ve Uygulanması	Kurum tarafından uzaktan çalışma faaliyetlerinde uygulanması gereken şartları ve kısıtlamaları tanımlayan bir politika hazırlanmalı ve uygulanmalıdır. Hazırlanan politika asgari olarak aşağıdaki hususları içermelidir. • Önerilen uzaktan çalışma ortamı • Zararlı yazılımlardan korunma ve güvenlik duvarı gereksinimleri • Yetkisiz erişimin engellenmesi • Kablosuz ağ hizmetlerinin kullanımı • Yedekleme gereksinimleri • Fiziksel güvenlik • Kişilere ait teçhizatlar üzerinde geliştirilen işlere ait fikri mülkiyet hakları ile ilgili anlaşmazlıklar • Uzaktan çalışmanın sona ermesi durumunda; yetki ve erişim haklarının iptali ve kullanılan teçhizatın iadesi
2	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.2 - Ekipman Güvenliğinin Sağlanması	Kurum personeli, uzaktan çalışma faaliyetlerinde yalnızca kurum tarafından sağlanan ve/veya yapılandırma ayarları kurumun bilgi güvenliği gereksinimlerine uygun olan cihazları kullanmalıdır.
3	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.3 - Dosya Paylaşımı	Uzaktan çalışma faaliyetlerinde, çalışma dosyalarını paylaşmak için kurumsal kaynaklar kullanılmalıdır.
4	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.4 - Farkındalık Eğitimlerinin Verilmesi	• Uzaktan çalışan kurum personeline özellikle güçlü parola kullanımı, sosyal mühendislik ve kimlik avı/oltalama saldırıları gibi konularda farkındalık eğitimleri verilmelidir. • Farkındalık ve Eğitim: Kuruluşlardaki tüm çalışanlar ve ilgili olan yerlerdeki yükleniciler ve üçüncü taraf kullanıcıların, kendi işlevleri kapsamındaki kurumsal politikalar ve süreçlerle ilgili uygun farkındalık eğitimlerini almaları sağlanmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
				• Güvenlik Eğitimi ve Farkındalığı: İşletiminde, kullanımında ve yönetiminde yetkili olan bütün personeli kapsayacak şekilde güvenlik eğitim ve farkındalık programları düzenlenmelidir. • Söz konusu eğitimlerde ana hedef söz konusu bağlantı kapsamında bilgi sistemleri güvenliği politikaları, yöntemleri ve kuralları konusunda personelin bilinçlendirilesi olmalıdır. Gerekirse personelin sorumluklarını tam ve doğru olarak anladığını gösterir bir belge (güvenlik brifingi tebellüğ belgesi) imzalatılmalıdır.
5	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.5 - Zararlı Yazılımdan Korunma Uygulamaları	Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazlarda zararlı yazılımdan korunma uygulaması kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır. Bk. Tedbir No: 1.5.1 Bk. Tedbir No: 1.5.4
6	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.6 - Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazların işletim sistemlerinin ve kullanılan uygulamaların güncel olması sağlanmalı, güvenlik yamaları yüklü olmalıdır. Bk. Bölüm 4
7	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.7 - Kurum Kaynaklarına Uzaktan Erişim	Uzaktan çalışma kapsamında kurum kaynaklarına erişim VPN teknolojileri ve çok faktörlü kimlik doğrulama ile sağlanmalıdır. Erişimler kurum politikalarına göre en az yetki prensibine göre sınırlandırılmalıdır. Bk. Tedbir No: 1.6.8
8	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.8 - Video Konferans Uygulamalarının Kullanımı	Video konferans uygulamaları kurum içerisinde barındırılmalıdır.
9	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.9 - Güçlü Parola Kullanımı	Uzaktan çalışma kapsamında kurumun politikalarına uygun güçlü parolaların kullanılması sağlanmalıdır.
10	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.10 - Video Konferans Toplantı Veri Tasnifi	Video Konferans ortamları gizlilik sınıfına uygun olarak ilgili ortamda bulundurulacaktır, kullanılan video konferans ortamı bağlanılan ağın tasnif sınıfında olmalıdır. Tasnif sınıfına bağlı olarak yalnız tek video konferans ortamı uzaktan erişilebilmelidir.
11	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.11 - Kullanıcı Bilgisayarında Güvenlik Duvarının Aktif Olması	Uzaktan çalışan kullanıcı bilgisayarlarında güvenlik duvarı yazılımları aktif durumda olmalıdır. Bk. Tedbir No: 1.6.11

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
12	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.12 - Uç Nokta Seviyesinde Veri Sızıntısının Önlenmesi	Uzaktan çalışan kullanıcı bilgisayarlarında olası veri sızıntısını engellemek amaçlı uç nokta seviyesinde veri sızıntısını önlemeye yönelik güvenlik önlemleri alınmalıdır. Bk. Tedbir Başlık No: 1.7
13	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.13 - Erişimin Kurum Bilgisayarları ile Sınırlandırılması	Uzaktan çalışma kapsamında sadece kurum cihazları üzerinden erişim sağlanmalıdır.
14	**1-Ağ ve Sistem Güvenliği**	1.1-Uzaktan Çalışma	1.1.14 - Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Bk. Tedbir No: 1.6.17
15	**1-Ağ ve Sistem Güvenliği**	1.2-Siber Güvenlik Olay Yönetimi	1.2.1 - Siber Olaylara Müdahale Planlarının Hazırlanması	Siber olaylara müdahale planları; uygulanması gereken akış, rol ve sorumlulukları içerecek şekilde yazılı hale getirilmelidir.Kurumsal SOME Kurulum ve Yönetim Rehberi'ne uygun olarak çalışmalar yürütülmelidir.
16	**1-Ağ ve Sistem Güvenliği**	1.2-Siber Güvenlik Olay Yönetimi	1.2.2 - Siber Olay Yönetimi Kapsamında Görev Alacak Personelin Belirlenmesi	Siber olayların yönetimi aşamalarında görev alacak personelin rol ve sorumlulukları tanımlanmalı, olay müdahale için gerekli teknik alt yapı personele sağlanmalı ve belirlenen personel ilgili taraflara bildirilmelidir. Siber olay yönetimi kapsamında görev alacak personel Kurumsal SOME Kurulum ve Yönetim Rehberi kriterlerine uygun olmalıdır.
17	**1-Ağ ve Sistem Güvenliği**	1.2-Siber Güvenlik Olay Yönetimi	1.2.3 - İletişim Bilgileri Dokümanının Hazırlanması	Siber olay bildirimi yapılacak resmi kurumlara ilişkin iletişim bilgileri dokümanı oluşturulmalı ve periyodik olarak gözden geçirilmelidir. İletişim bilgileri dokümanı, iletişim kurulacak konu kapsamında iletişim kurulacak kişileri tanımlamalıdır.
18	**1-Ağ ve Sistem Güvenliği**	1.2-Siber Güvenlik Olay Yönetimi	1.2.4 - Siber Tehdit Bildirimlerinin Yönetilmesi	Kurumlar siber olayların tespiti için gerekli altyapıları kurmalı, USOM ve olası diğer siber tehdit istihbarat kaynaklarından alınan bildirimler doğrultusunda gerekli önlemleri almalıdır.
19	**1-Ağ ve Sistem Güvenliği**	1.2-Siber Güvenlik Olay Yönetimi	1.2.5 - Siber Olayların Raporlarının Standardize Edilmesi ve Yayınlanması	Siber olaylar ile ilgili bildirim süresi ve rapora yansıtılacak bilgiler USOM tarafından belirlenen kriterler göz önünde bulundurularak belirlenmeli ve standart hale getirilmelidir. Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu, kurum standartlarına göre hazırlanmalı, üst yönetim, USOM ve varsa bağlı olduğu Sektörel SOME'ye iletilmelidir.
20	**1-Ağ ve Sistem Güvenliği**	1.2-Siber Güvenlik Olay Yönetimi	1.2.6 - Üçüncü Taraflardan Alınan Siber Olay Yönetim Hizmetleri	Kurumların siber olay yönetimi kapsamındaki hizmetleri üçüncü taraflardan alması durumunda hizmetin güvenliği garanti altına alınmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
21	**1-Ağ ve Sistem Güvenliği**	1.3-Tehdit ve Zafiyet Yönetimi	1.3.1 - Yazılım Güncelleme Araçlarının Kullanımı	Tüm sistemlerdeki yazılımların, mevcut iş gereksinimlerini karşılayacak ve yazılım üreticisi tarafından sağlanan en kararlı ve güncel güvenlik sürümleri ile çalıştırılmakta olduğu otomatik yazılım güncelleme araçları kullanılarak kontrol edilmelidir. Otomatik yazılım güncelleme araçlarının kullanılamadığı durumlarda uzman personel tarafından manuel olarak gerekli kontroller periyodik olarak yapılmalıdır.
22	**1-Ağ ve Sistem Güvenliği**	1.3-Tehdit ve Zafiyet Yönetimi	1.3.2 - Zararlı Yazılımların Engellenmesi	Zararlı yazılımların kuruma ait ve/veya kurum tarafından yönetilen kullanıcı uç nokta cihazları ve altyapı bileşenleri üzerinde çalışmasını, kaydedilmesini ve aktarılmasını engellemek için politikalar/prosedürler tanımlanmalı ve işletilmelidir. Personelin beyaz listede bulunan uygulamalar haricinde uygulama kurmasının engellenmesine yönelik politika/prosedür oluşturulmalıdır. Politika/prosedürün uygulanmasını temin etmek üzere gerekli teknolojik altyapılar ve uyarı mekanizmaları aktif edilmelidir.
23	**1-Ağ ve Sistem Güvenliği**	1.3-Tehdit ve Zafiyet Yönetimi	1.3.3 - Zafiyet/Yama Yönetimi	Kurumsal uygulamaların, kurum ağının ve sistem bileşenlerinin güvenlik açıklarının zamanında tespit edilmesi için uygulanacak politikalar ve süreçler tanımlanmalıdır. Zafiyet ve yama yönetimine ilişkin değişiklikler, tanımlanmış değişiklik yönetimi süreci üzerinden kontrollü olarak gerçekleştirilmelidir.
24	**1-Ağ ve Sistem Güvenliği**	1.3-Tehdit ve Zafiyet Yönetimi	1.3.4 - Yüksek ve Üzeri Seviyede Zafiyet İçeren Sunucu/Uygulamaların Yalıtılması	Yüksek ve üzeri seviyede zafiyet barındıran sunucu ve uygulamalar, diğer sistemlerden fiziksel ya da mantıksal olarak izole edilmelidir. İzolasyon yapılamadığı durumlarda söz konusu sunucu ve uygulamalarda katmanlı güvenlik prensibine uygun şekilde güvenliğin artırılması sağlanmalıdır.
25	**1-Ağ ve Sistem Güvenliği**	1.3-Tehdit ve Zafiyet Yönetimi	1.3.5 - Son Kullanıcıların Yetkisiz Program Ekleme/Kaldırma İşlemlerinin Engellenmesi	Son kullanıcıların, güvenlik sıkılaştırmaları kapsamında kurum tarafından uygulanması gerekli görülen konfigürasyonlara müdahale etmemesi ve beyaz listede bulunan programlar haricinde program kurmalarının engellenmesi için son kullanıcı hesaplarının yerel yönetici yetkileri kaldırılmalıdır. Bk. Tedbir No: 4.2.4
26	**1-Ağ ve Sistem Güvenliği**	1.3-Tehdit ve Zafiyet Yönetimi	1.3.6 - Güvenlik Açıkları için Risk Analizi Tabanlı Önceliklendirme	Tespit edilen güvenlik açıklarının giderilmesi için hazırlanan aksiyon planına yönelik önceliklendirme risk analizi tabanlı yapılmalıdır.
27	**1-Ağ ve Sistem Güvenliği**	1.3-Tehdit ve Zafiyet Yönetimi	1.3.7 - Güvenlik Sıkılaştırmalarının Yapılması	Kurumsal uygulamalar (web, DNS, e-posta, FTP vb. ile diğer uygulamalar) ve kurum ağındaki bileşenler, işletim sisteminin ve paket yazılımların kurulumuyla gelen varsayılan güvenlik ayarlarıyla kullanılmamalıdır. Kullanıma alınmadan

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
				önce bilgi güvenliği gereksinimleri dikkate alınarak gerekli güvenlik sıkılaştırmaları yapılmalıdır. Bk. Bölüm 5
28	**1-Ağ ve Sistem Güvenliği**	1.3-Tehdit ve Zafiyet Yönetimi	1.3.8 - İşletim Sistemi Yama Yönetimi Araçlarının Kullanımı	Güvenlik güncellemeleri başta olmak üzere işletim sistemlerine yönelik güncellemelerin ve yamaların üreticisi tarafından bildirilen en kararlı, güncel ve güvenilir sürüm dikkate alınarak yapıldığı, otomatik yazılım güncelleme araçları ile kontrol edilmelidir
29	**1-Ağ ve Sistem Güvenliği**	1.3-Tehdit ve Zafiyet Yönetimi	1.3.9 - Zafiyet Tarama Araçlarının Kullanımı	Kurum ağında yer alan tüm sistemler (test sistemleri de dâhil olmak üzere) güvenlik içeriği otomasyon protokolü (SCAP) uyumlu güvenlik zafiyeti tarama aracı kullanılarak periyodik olarak taranmalıdır. Güvenlik taramaları için oluşturulan hesaplar farklı bir amaç için kullanılmamalı, en az yetki ve bilmesi gereken prensibi doğrultusunda yetkilendirme yapılarak ilgili erişim kayıtları tutulmalıdır. Güvenlik taramaları için oluşturulan hesaplar düzenli olarak kontrol edilmeli ve izlenmelidir. Zafiyet tarama araçları, güvenlik açıklarına yönelik yapılan doğrulama faaliyetleri öncesi ve sonrası durumu içerecek şekilde raporlama yapmalıdır. Üretilen raporların güvenliği sağlanmalı ve raporlara sadece yetkili personel erişim sağlamalıdır.
30	**1-Ağ ve Sistem Güvenliği**	1.4-Sızma Testleri ve Güvenlik Denetimleri	1.4.1 - Sızma Testleri ve Güvenlik Denetimlerinin Gerçekleştirilmesi	Kurum sistemlerinin güvenlik açıklarını ve saldırı yüzeyini belirlemek için düzenli aralıklarla harici ve dâhili sızma testleri ve güvenlik denetimleri gerçekleştirilmelidir. Sızma testleri ve güvenlik denetimleri gerçekleştirilmeden önce testi gerçekleştirecek taraftan, test süresince elde edilen hiçbir verinin yetkisiz kişilere verilmemesi, aktarılmaması ve ifşa edilmemesine yönelik taahhüt alınmalıdır. Sızma testi ve güvenlik denetimi kapsamı tanımlanmalı ve yazılı hale getirilmelidir. Sosyal mühendislik testleri de sızma testi kapsamına dâhil edilmelidir.
31	**1-Ağ ve Sistem Güvenliği**	1.4-Sızma Testleri ve Güvenlik Denetimleri	1.4.2 - Sızma Testlerinin Kullanıcı Profillerine Göre Gerçekleştirilmesi	Sağlıklı ve gerçek hayata uygun bir sızma testi için testler sırasında anonim kullanıcılar, misafir kullanıcılar, çalışanlar, kurumdan hizmet alan kullanıcılar ve kuruma destek veren kullanıcılar gibi farklı yetki seviyesindeki kullanıcı profilleri kullanılmalıdır.
32	**1-Ağ ve Sistem Güvenliği**	1.4-Sızma Testleri ve Güvenlik Denetimleri	1.4.3 - Sızma Testi Gerçekleştirilemeyen Bileşenlerin Yönetimi	Operasyonel ortamda olup sızma testi yapılması mümkün olmayan veya yüksek risk içeren sistemler için güvenlik denetimleri ve güvenlik sıkılaştırmaları düzenli olarak yapılmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
33	**1-Ağ ve Sistem Güvenliği**	1.4-Sızma Testleri ve Güvenlik Denetimleri	1.4.4 - Sızma Testi için Oluşturulan Hesapların Yönetimi	Sızma testini gerçekleştirmek için kullanılan herhangi bir kullanıcı veya sistem hesabı, yalnızca meşru amaçlar için kullanıldığından emin olmak için kontrol edilmeli, izlenmeli, kayıt altına alınmalı ve test bittikten sonra pasif hale getirilmelidir.
34	**1-Ağ ve Sistem Güvenliği**	1.4-Sızma Testleri ve Güvenlik Denetimleri	1.4.5 - Doğrulama Testlerinin Yaptırılması	Kapatılan güvenlik açıklarına yönelik doğrulama testleri görevlerin ayrılığı ilkesi doğrultusunda yapılmalıdır.
35	**1-Ağ ve Sistem Güvenliği**	1.4-Sızma Testleri ve Güvenlik Denetimleri	1.4.6 - Sızma Testi ve Güvenlik Denetimi Bulgularının Seviyelendirilmesi	Sızma testi ve güvenlik denetimi bulguları karşılaştırılabilir bir puanlama yöntemi dikkate alınarak raporlanmalıdır.
36	**1-Ağ ve Sistem Güvenliği**	1.4-Sızma Testleri ve Güvenlik Denetimleri	1.4.7 - Test Ortamlarının Hazırlanması	Canlı ortamda olup sızma testi yapılması mümkün olmayan ve/veya yüksek risk içeren sistemler için gerçeğine benzer test ortamları oluşturulmalıdır. Test ortamının oluşturulması mümkün olmayan her bir bileşen için 1.4.3 numaralı tedbir maddesi uygulanmalıdır.
37	**1-Ağ ve Sistem Güvenliği**	1.4-Sızma Testleri ve Güvenlik Denetimleri	1.4.8 - Sızma Testleri ve Güvenlik Denetimlerinin Periyodu	Sızma testleri ve güvenlik denetimleri yılda en az 1 defa yapılmalıdır.
38	**1-Ağ ve Sistem Güvenliği**	1.4-Sızma Testleri ve Güvenlik Denetimleri	1.4.9 - Düzenli Kırmızı Takım Tatbikatlarının Yapılması	Siber saldırılara karşı kurumsal hazırlığı test etmek adına düzenli kırmızı takım tatbikatları yapılmalı veya yaptırılmalıdır. Tatbikat sonuçları kurum içi yazılı hale getirilerek raporlanmalıdır. Rapor sonuçlarına göre kurumda gerekli iyileştirmeler sağlanmalıdır.
39	**1-Ağ ve Sistem Güvenliği**	1.5-Zararlı Yazılımlardan Korunma	1.5.1 - Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması ve Merkezi Olarak Yönetilmesi	• İstemci ve sunucu sistemlerinin tamamında zararlı yazılımdan korunma uygulamaları kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır. Zararlı yazılımdan korunma uygulamalarına ait politikalar merkezi olarak yönetilmelidir. • Antivirüs programlarının gerçek zamanlı tarama özelliği aktif edilerek, dosyalara ulaşım esnasında virüs taramasının yapılması sağlanmalıdır. • Kayıt dışı taşınabilir veri depolama ortamları ilk kullanımdan önce mevcut kullanılandan farklı bir antivirüs programı ile taramadan geçirilmelidir.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
				• Kullanıcıların antivirüs programının ayarlarına müdahale etmeleri ve programı kapatmaları teknik olarak engellenmelidir. • Antivirüs programı alınırken sıkıştırılmış dosyaların içeriğini de (.zip, .rar vb.) kontrol edebilecek yetenektekiler tercih edilmelidir.
40	**1-Ağ ve Sistem Güvenliği**	1.5-Zararlı Yazılımlardan Korunma	1.5.2 - Taşınabilir Disklerin Zararlı Yazılım Taramalarından Geçirilmesi	Kurumdaki tüm bilgisayarlar, taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılmalıdır.
41	**1-Ağ ve Sistem Güvenliği**	1.5-Zararlı Yazılımlardan Korunma	1.5.3 - Cihazların Otomatik Kod Çalıştırmasına İzin Vermemesi	Kurumdaki tüm bilgisayarlar, taşınabilir ortamlarda otomatik kod çalıştırılmasına izin vermeyecek şekilde yapılandırılmalıdır.
42	**1-Ağ ve Sistem Güvenliği**	1.5-Zararlı Yazılımlardan Korunma	1.5.4 - Zararlı Yazılımdan Korunma Uygulamalarının Yapılandırılması ve Güncel Tutulması	Zararlı yazılımlardan korunma uygulaması üretici veya ilgili kurum tarafından önerilen şekilde yapılandırılmalı ve güncel tutulmalıdır.
43	**1-Ağ ve Sistem Güvenliği**	1.5-Zararlı Yazılımlardan Korunma	1.5.5 - Zararlı Yazılımdan Korunma Uygulamalarına Ait Kayıtların Merkezi Olarak Tutulması	Tüm zararlı yazılım tespitleri, merkezi yönetim ve kayıt sunucularına iletilmelidir.
44	**1-Ağ ve Sistem Güvenliği**	1.5-Zararlı Yazılımlardan Korunma	1.5.6 - Komut Satırı Kayıtlarının Tutulması	Uzaktan erişim için kullanılan cihazlarda Kurumda, kullanıcı tarafından PowerShell ve Bash gibi komut satırı kullanılarak yapılan işlemler denetlenmelidir.
45	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.1 - Ağ Topolojisi	Uzaktan çalışma kapsamında yer alan Kurum ağlarına ait topolojiler güvenli bir şekilde tutulmalı ve güncelliği kontrol edilmelidir.
46	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.2 - Ağ Cihazlarının Güvenli Konfigürasyonu	Ağ cihazları endüstri standartları, en iyi uygulamalar ve üretici tavsiyelerine uygun olarak yapılandırılmalıdır. Varsayılan parola ve kullanıcı adları değiştirilmelidir. Ağ altyapısındaki cihazlar ağ üzerinden yönetilebilir olmalıdır. Yönetimsel erişimlerde komut satırına, konsol erişimine parola ile giriş sağlanmalıdır. Güvenli protokoller ile yönetimsel işlemler gerçekleştirilmelidir.
47	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.3 - Ağ Cihazlarında Güvenlik Güncellemelerinin Yapılması	Tüm ağ cihazlarında güvenlikle ilgili güncellemelerin üretici tarafından yayımlanan kararlı ve güncel sürümü kullanılmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
48	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.4 - Tasnif sınıfı farklı ağlar arasında çalışma yöntemi	Tasnif sınıfı farklı ağlar kullanıcıların çalışması esnasında arasında sadece görüntü, klavye ve fare aktarımına izin veren cihazlar kullanılmalıdır.
49	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.5 - İzin Verilmeyen Trafiğin Engellenmesi	Kurum ağ sınırlarından sadece izin verilen kaynaklardan izin verilen hedeflere, izin verilen port ve protokoller ile trafiğin akışı sağlanmalıdır.
50	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.6 - Ağların İzole Edilmesi	Kablolu ve kablosuz ağlar, bilgi güvenliği gereksinimleri doğrultusunda katmanlara ayrılmalıdır. Yalnızca yetkili sistemlerin, belirli sorumluluklarını yerine getirmek amacıyla gerekli diğer sistemlerle iletişim kurabilmelerini sağlamak için oluşturulan LAN/VLAN'lar arasında erişim denetimi yapılmalıdır. İstemcilerin yer aldığı ağlar ile sunucu/uygulamaların yer aldığı ağlar ayrılmalıdır. Sunucu ağında istemci yer almamalıdır. Yönetimsel işlemler için ayrı yönetim ağları kullanılmalıdır.
51	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.7 - Uygulama Seviyesi Saldırıların Engellenmesi	Kurum ağının uygulama seviyesi saldırılara karşı korunması için gerekli yapılar (WAF, IPS, DDoS vb.) uygun şekilde konumlandırılmalı, test edilmeli ve sürekli iyileştirilmelidir. Bu amaçla bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki şartlara göre hizmet verildiğine dair taahhüt alınmalı, tedarik şartname ve sözleşmelerinde bu hususlar belirtilmelidir.
52	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.8 - İnternet Ortamından Kurum İçi Kaynaklara Erişim	İnternet ortamından kurum içi kaynaklara kontrol dışı erişim engellenmelidir. İnternet ortamından kurum içi kaynaklara erişim için VPN teknolojileri kullanılmalıdır. Uzaktan erişimlerin kurum politika ve prosedürlerine uygun olarak, kısıtlı süre ve yetkilerle yapılması sağlanmalıdır.
53	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.9 - Ağ Cihazlarının Yapılandırma Yönetimi	Ağ cihazı mevcut yapılandırmaları, onaylanmış ve olması gereken güvenlik yapılandırma içerikleri ile karşılaştırılmalı ve herhangi bir uyumsuzluk tespit edildiğinde alarm üreten mekanizmalar devreye alınmalıdır.
54	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.10 - Ağ Cihazlarının Yönetimi	Ağ cihazlarının yönetimi, çok faktörlü kimlik doğrulama mekanizmaları kullanılarak şifreli ağ trafiği üzerinden yapılmalıdır. Ağ yönetimi için gerekli işlemler, bu amaç için tahsis edilen ve internet erişimi olmayan makineler üzerinden yapılmalıdır.
55	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.11 - Yerel Güvenlik Duvarı Ayarlarının Yapılması	Tüm uzaktan erişim istemcilerde yerel güvenlik duvarı yapılandırılmalıdır. Bu yapılandırma en az yetki prensibi göz önüne alınarak yapılmalıdır. Yapılandırma varsayılan reddetme (default deny) kuralını içermelidir. Tüm açık portlara ilişkin güvenlik duvarı kuralları yazılmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
56	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.12 - Ağ Tabanlı URL Filtreleri Kullanımı	Kurumdaki sistemlerin, kurum tarafından onaylanmayan ve mevzuat gereği erişimi yasak olan web sitelerine bağlanmasını engelleyen ağ tabanlı URL filtreleri uygulanmalıdır.
57	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.13 - URL Kategori Hizmeti Kullanımı	URL sınıflandırma servisleri kullanılmalıdır. Bu servislerin kullandığı listeler güncel tutulmalıdır. Kategorilendirilmemiş siteler varsayılan olarak engellenmelidir.
58	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.14 - URL'lerin Kayıt Altına Alınması	Potansiyel olarak zararlı etkinlikleri tanımlamak ve saldırıya uğramış sistemlerin belirlenmesine yardımcı olmak için sistemlerden gelen tüm isteklere ait URL'ler kaydedilmelidir.
59	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.15 - Ağ Erişim Denetimleri	Bk. Tedbir No: 1.1.7
60	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.16 - Ağ Cihazlarına Ait Yapılandırmaların Yazılı Hale Getirilmesi	Kurum ağ cihazlarına ait güvenlik yapılandırmaları; ağ trafiğini düzenleyen kurallara ait tanımlar, kullanılma amacı ve kuralı tanımlayan kişi bilgisi yer alacak şekilde dokümante edilmeli ve güncelliği sağlanmalıdır.
61	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.17 - Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Kuruma uzaktan bağlanacak cihazların; zararlı yazılımdan korunma, işletim sistemi ve uygulama güncelliği vb. hususlar kapsamında kurum politikalarına uygunluğu güvenli uzaktan bağlantı sağlayan sistemler üzerinden (VPN vb.) kontrol edilmelidir. Kurum politikasına uymayan cihazlara bağlantı izni verilmemelidir.
62	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.18 - Ağ Sınır Cihazlarında Kayıt Tutulması	Ağ sınır cihazlarındaki bağlantı trafiği, kullanıcı işlemleri gibi bilgiler kayıt altına alınmalıdır.
63	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.19 - Ağ Tabanlı Saldırı Tespit/Engelleme Sistemi Kullanımı	Saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit ve engelleme sistemleri kullanılmalıdır.
64	**1-Ağ ve Sistem Güvenliği**	1.6-Ağ Güvenliği	1.6.20 - Uygulama Katmanında Filtreleme Yapılması	İnternetten gelen veya internete giden tüm ağ trafiği, yetkisiz bağlantıları engellemek için uygulama katmanında filtreleme ve kimlik doğrulaması yapılarak iletilmelidir.
65	**1-Ağ ve Sistem Güvenliği**	1.7-Veri Sızıntısı Önleme	1.7.1 - Veri Sınıflandırma Politikasının Oluşturulması	Kurum verilerinin sistematik olarak kategorilere ayrılması ve sınıflandırılması için politikalar oluşturulmalıdır.
66	**1-Ağ ve Sistem Güvenliği**	1.7-Veri Sızıntısı Önleme	1.7.2 - Ağda Kritik Veri Taşınması	Ağda kritik verinin taşınmasında güvenli protokoller kullanılmalı (VPN teknolojileri, SSL/TLS vb.) ve kritik veri şifreli olarak taşınmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
67	**1-Ağ ve Sistem Güvenliği**	1.7-Veri Sızıntısı Önleme	1.7.3 - Ağ İçerisinde Veri Sızıntısı Önleme	Ağ içerisinde veri akışını kontrol etmek, izlemek ve izinsiz ağ trafiğini takip etmek amacıyla ağ tabanlı veri sızıntısı önleme sistemi kullanılmalıdır.
68	**1-Ağ ve Sistem Güvenliği**	1.7-Veri Sızıntısı Önleme	1.7.4 - Taşınabilir Ortam Engelleme	Kritik sistemler taşınabilir depolama birimlerini desteklemeyecek şekilde yapılandırılmalıdır. Taşınabilir depolama birimleri takıldığında uyarı üretecek mekanizmalar aktif edilmelidir. Bu uyarılar izlenmelidir.
69	**1-Ağ ve Sistem Güvenliği**	1.8-İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	1.8.1 - İz ve Denetim Kayıtlarının Tutulması	• Tüm sistemlerde ve ağ cihazlarında kayıt mekanizması etkin olmalıdır. Kayıtlar, bilgi güvenliği gereksinimleri ve ilgili mevzuat gereği kabul edilebilir süre boyunca cihaz üzerinde veya harici sistemlerde tutulmalı, yetkisiz erişime ve değişime karşı korunmalıdır. Kayıtlar, muhafazaları için tanımlanan kabul edilebilir sürenin sona ermesi ile birlikte güvenli bir şekilde yok edilmelidir. • Kullanıcı ve uygulamaların bağlantı kapsamındaki faaliyetlerinin kayıt altına alınacağı mekanizmalar kurulmalı veya yapılandırılmalıdır. Kaydedilen faaliyetler asgari; olay türü, tarihi ve zamanı, kullanıcı tanımları, terminal bilgileri, erişim denemelerinin başarılı mı başarısız mı olduğu, sistem yöneticisi veya güvenlik sorumluları tarafından yapılan işlem bilgisini içermelidir. İzleme kayıtları (audit logs) sadece okuma erişimine açık olmalı ve bu kayıtlara yalnızca yetkilendirilmiş personel tarafından erişilebilmelidir. Söz konusu kayıtlar çalınma ve silinme riskine karşı güvenli bölgelerde muhafaza edilmeli, asgari bir yıl süre ile saklanmalı ve taraflarca önceden belirlenen sıklıklarla çalışırlığı kontrol edilmelidir. • İşletim sistemleri ve verileri saklayan veri tabanı yönetim sistemlerine ilişkin aşağıda yer alan kayıtlar tutulmalı ve en az 6 ay muhafaza edilmelidir: .Sisteme yerel giriş (Kullanıcıların bilgisayarlarına bilgisayar üzerinde var olan hesaplarla ne zaman giriş yaptığı bilgisi). .Etki alanına giriş (Kullanıcıların bilgisayarlarına etki alanı hesabıyla ne zaman giriş yaptığı bilgisi. .Kullanıcı/Grup hesap yönetimi (Kullanıcı/grup ekleme/silme/ değiştirme) bilgileri. • Kullanıcı bilgisayarlarında ise güvenlik olay günlükleri (“Security Event Log”) açık tutulmalıdır. Bu kayıtların ne kadar süre ile tutulacağı veya belli bir kotaya ulaştığında üstüne yazılabilirliği, disk kapasitesine bağlı olarak, ilgili kuruma bırakılmış olup, mümkün olan azami miktarda kayıt tutulması sağlanmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
70	**1-Ağ ve Sistem Güvenliği**	1.8-İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	1.8.2 - Denetim Kayıtlarının Yönetimi	Sistem yöneticisi, operatörler ve kullanıcıların faaliyetleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir.
71	**1-Ağ ve Sistem Güvenliği**	1.8-İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	1.8.3 - Zaman Sunucusu Kullanımı	Kayıtlarda zaman damgalarının tutarlı olması için ağa bağlı tüm sistemlerin (sunucular, iş istasyonları, güvenlik ürünleri, ağ aygıtları vb.) düzenli olarak zaman bilgisinin alındığı; yedekli yapıda ve senkronize zaman sunucusu kullanılmalıdır. Bk. Tedbir No: 4.1.11
72	**1-Ağ ve Sistem Güvenliği**	1.8-İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	1.8.4 - Detaylı Kayıt Tutulması	Sistem iz kayıtları; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulmalı ve bütünlüğü zaman damgası ile korunmalıdır.
73	**1-Ağ ve Sistem Güvenliği**	1.8-İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	1.8.5 - Kayıtlar için Yeterli Depolama Alanı Tahsisi	Kayıt tutan sistemlerde yeterli depolama alanı tahsis edilmelidir. Depolama alanı doluluk oranı düzenli olarak kontrol edilmelidir.
74	**1-Ağ ve Sistem Güvenliği**	1.8-İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	1.8.6 - Merkezi Kayıt Yönetimi	Analiz ve inceleme amacıyla kayıtlar merkezi bir kayıt yönetim sisteminde toplanmalı ve düzenli olarak yetkili personel tarafından gözden geçirilmelidir. Kayıt tutma veya gönderme işlemi sırasında hata oluştuğunda uyarı mekanizmaları aktif edilmeli ve izlenmelidir.
75	**1-Ağ ve Sistem Güvenliği**	1.8-İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	1.8.7 - Kayıt Analizi Araçları Kullanımı	Siber olayların korelasyon kuralları doğrultusunda tespiti ve detaylı analizi için siber tehdit ve olay yönetim sistemleri veya kayıt analizi araçları kullanılmalıdır.
76	**1-Ağ ve Sistem Güvenliği**	1.8-İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	1.8.8 - Siber Tehdit ve Olay Yönetim Sistemlerinin Düzenli Yapılandırılması	Aksiyon alınabilecek olayların daha iyi tanımlanabilmesi ve gereksiz olayların elenebilmesi amacıyla siber tehdit ve olay yönetim sistemlerinin yapılandırması düzenli olarak gözden geçirilmelidir. Kayıtlar düzenli olarak izlenmelidir. Bk. Tedbir Başlık No: 1.2

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
77	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.1 - Güncel Sürümlerin Kullanılması	Sanallaştırma ürünlerinin üretici tarafından desteği devam eden ve kararlı sürümleri kullanılmalıdır. Bu ürünlerin güvenliği ile ilgili duyurular takip edilmelidir.
78	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.2 - Kapasite Planlaması	Gelecekteki ihtiyaçlar, yasal yükümlülükler ve olası güvenlik riskleri göz önünde bulundurularak sistem kaynaklarının planlaması yapılmalı ve kaynaklar sürekli izlenmelidir. Kapasite artırımı için kurumsal eşik değerleri tanımlanmalıdır.
79	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.3 - Sanal Makinelerin Yönetilmesi	Sanallaştırma ortamında kullanılmayan sanal makineler kapatılmalı, ağdan izole edilmeli ve sanal makine görev ömrünü tamamlayınca üzerinde yer alan veriler güvenli silme yöntemleri ile imha edilmelidir.
80	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.4 - İşletim Sistemi Sıkılaştırmalarının ve Güvenlik Kontrollerinin Yapılması	Kullanılmakta olan işletim sistemleri, iş gereksinimlerini karşılamak için ihtiyaç duyulan bağlantı noktaları, protokoller ve servisleri sağlayacak şekilde sıkılaştırılmalıdır. Zararlı yazılımdan korunma uygulamaları kullanılmalı, dosya bütünlüğünü izleyecek ve kayıt tutacak mekanizmalar devreye alınmalıdır. Bk. Bölüm 4
81	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.5 - Tedarik Edilen Sanallaştırma Hizmeti Ortam Güvenliğinin Sağlanması	Sanallaştırma hizmetinin üçüncü taraflar aracılığıyla sunulması durumunda, sanallaştırma ortamının güvenliği garanti altına alınmalıdır.
82	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.6 - Depolama Ortamları ile İletişim Güvenliğinin Sağlanması	Sanallaştırma ortamları ile birlikte kullanılacak veya kurum bünyesinde müstakil olarak kullanılacak depolama ortamları ile iletişimin güvenliğinin sağlanmasında aşağıdaki hususlar dikkate alınmalıdır. • Ağ dosya paylaşım servisleri, ayrılmış depolama ağlarında veya yönlendirilemeyen ağlarda hizmet vermelidir. • Ağ dosya paylaşım servislerinde, eğer destekleniyorsa trafik şifreli olmalı, uygun kimlik doğrulama protokolleri kullanılarak erişim denetimi yapılmalı ve kayıtlar tutulmalıdır.
83	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.7 - Sanal Ağ Güvenliği	Ağ ortamları ve sanal makineler, kurum tarafından belirlenen kriterlere göre güvenilir ve güvenilmeyen bağlantılar arasındaki trafik kısıtlanacak şekilde yapılandırılmalıdır. Bu yapılandırmalar düzenli olarak gözden geçirilmeli; izin verilen tüm servisler, protokoller, portlar dokümante edilmeli ve kullanım gerekçesi gösterilmelidir. Bk. Tedbir No: 1.6.6
84	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.8 - Operasyon ve Test Ortamlarının İzolasyonu	Operasyon ve test ortamları güvenlik duvarları, alan/bölge bazlı kimlik doğrulama vb. yöntemler kullanılarak birbirinden ayrılmalı ve bu ortamların yöneticileri için görevler ayrılığı prensibi uygulanmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
85	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.9 - Sanallaştırma Yönetim Ortamına Erişim	Sanallaştırma sistemleri yönetim ara yüzlerine erişim, iş ihtiyaçları doğrultusunda tanımlanan yetki ile güvenli bir şekilde yapılmalıdır.
86	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.10 - Sanallaştırma Ortamı Sertifika Yönetimi	Sanallaştırma ortamında kendinden imzalı sertifikalar yerine kuruma ait ve yetkili otoriteden alınmış sertifikalar kullanılmalıdır.
87	**1-Ağ ve Sistem Güvenliği**	1.9-Sanallaştırma Güvenliği	1.9.11 - Fiziksel Kaynakların İzole Edilmesi	Farklı güvenlik seviyesinde yer alan ağlarda kullanılan sanal sistemlere ait kaynaklar fiziksel olarak izole edilmelidir.
88	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.1 - Erişim Kontrol Politikasının Oluşturulması ve Uygulanması	Erişim kontrol politikaları oluşturulmalı, uygulamaya alınmalı ve güncelliği periyodik olarak kontrol edilmelidir. Kullanıcı (sistem yöneticisi ve sisteme işlem amacıyla erişen kullanıcılar) hesap işlemleri (açma, kapama, değişiklik) ve erişim talepleri tanımlı bir süreç ile takip edilmeli ve kayıt altına alınmalıdır.
89	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.2 - Kullanıcı Hesaplarının Yönetimi	Her kullanıcı için kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabı tanımlanmalı, tüm kullanıcı hesaplarına ait bir parola ataması yapılmalıdır. Kullanıcı hesaplarına ait parolalar belirlenirken dikkat edilmesi gereken kurallar tanımlanmalı ve uygulanmalıdır.
90	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.3 - Başarısız Oturum Açma Denemelerinin Yönetimi	Oturum açma mekanizmasına yapılacak saldırıları engellemek amacıyla uygun güvenlik önlemleri (istek sınırlandırma, IP bloklama, CAPTCHA vb.) alınmalıdır. Başarısız oturum açma denemeleri kayıt altına alınmalıdır.
91	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.4 - Varsayılan Kullanıcıların ve Parolaların Değiştirilmesi	Kurum bilgi sistemindeki herhangi bir varlıkta varsayılan kullanıcı adı ve parolalar kullanılmamalıdır. Test ortamlarında kullanımda olan tüm varsayılan kullanıcılar ve parolalar, canlıya alınmadan önce silinmeli veya değiştirilmelidir.
92	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.5 - Yönetici Hesaplarının Kullanımı	Sistem yöneticilerinin yüksek haklar gerektiren işlemleri yapmak için ayrı bir hesapları olmalıdır. Yönetici hesaplarıyla yapılan işlemler için denetim kayıtları oluşturulmalıdır.
93	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.6 - İşlem Yapılmayan Oturumların Sonlandırılması	İşlem yapılmayan oturumlar belirli bir süre sonra sonlandırılmalıdır.
94	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.7 - Kimlik Doğrulama	Kurum kaynaklarına erişimlerde çok faktörlü kimlik doğrulama mekanizmaları kullanılmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
95	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.8 - Kullanıcı Yetkilerinin Güncellenmesi	Sistem yöneticilerinin ve kullanıcılarının yetkileri düzenli olarak gözden geçirilmeli, görev değişikliklerinde erişim yetkileri güncellenmelidir. Bir personelin veya yüklenicinin sorumluluklarının değişmesinden hemen sonra hesapları devre dışı bırakmak ve sistem erişimini iptal etmek için süreç oluşturulmalı ve uygulanmalıdır. Bu hesaplar devre dışı bırakılmalıdır.
96	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.9 - Servis Hesaplarının Yönetimi	Servis hesapları en az yetki prensibi göz önünde bulundurularak oluşturulmalıdır. Kullanıcı veya yetkili hesaplar servis hesabı olarak kullanılmamalıdır. Servis hesaplarının kurum içerisinde bir sahibi olmalı ve periyodik olarak gözden geçirilmelidir.
97	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.10 - Kullanılmayan Hesapların Devre Dışı Bırakılması	Belirli bir süre kullanılmayan, bir iş süreci veya kurum personeli ile ilişkilendirilemeyen tüm hesaplar otomatik olarak devre dışı bırakılmalıdır.
98	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.11 - Yönetici Hesaplarının İşletimi	Etki alanı ve yerel hesaplar dâhil tüm yönetim hesaplarını yönetmek için otomatik araçlar kullanılmalıdır. Kurumdaki sistemler bir yönetici hesabı oluşturulduğunda veya silindiğinde kayıt tutacak ve alarm oluşturacak şekilde yapılandırılmalıdır. Tüm yönetici hesap erişimleri için çok faktörlü kimlik doğrulama ve şifreli kanallar kullanılmalıdır. Kurumdaki sistemler bir yönetici hesabından giriş denemesi yapıldığında kayıt tutmalı ve giriş denemesi yapılması durumunda alarm oluşturacak şekilde yapılandırılmalıdır.
99	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.12 - Betik Dillerinin Kullanımına Yönelik Erişimin Sınırlandırılması	Uzaktan erişim cihazlarında Betik dosyası oluşturma araçlarına (PowerShell ve Python gibi) erişim, yalnızca iş amaçları doğrultusunda bu özelliklere erişmesi gereken hesaplar ile sınırlandırılmalıdır.
100	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.13 - Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması	Yerel veya uzak servis sağlayıcılarında bulunanlar da dâhil olmak üzere, kurumun tüm kimlik doğrulama sistemlerinin ve bu sistemlerle entegre uygulamaların envanteri tutulmalıdır.
101	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.14 - Merkezi Kimlik Doğrulama	Kimlik doğrulama merkezi olarak yapılmalıdır. Merkezi kimlik yönetim ve doğrulama sisteminin kullanılamadığı durumlarda, risk analizi çalışması doğrultusunda telafi edici önlemler alınmalıdır.
102	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.15 - Çok Faktörlü Kimlik Doğrulama Yapılması	Kurum ağına dışarıdan yapılan erişimler çok faktörlü kimlik doğrulaması ile sağlanmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
103	**1-Ağ ve Sistem Güvenliği**	1.10-Kimlik Doğrulama ve Erişim Yönetimi	1.10.16 - Kimlik Doğrulama Bilgilerinin Güvenli Olarak Saklanması	Tüm kimlik doğrulama bilgileri güçlü kriptografik algoritmalar kullanılarak saklanmalı ve şifreli kanallar kullanılarak iletilmelidir.
104	**2-Taşınabilir Cihaz ve Ortam Güvenliği**	2.1-Taşınabilir Bilgisayar Güvenliği	2.1.1 - Taşınabilir Bilgisayarların Kabul Edilebilir Kullanımı	Taşınabilir bilgisayarların kurum bünyesinde kullanılabilmesi için taşınabilir bilgisayarların kullanımı, uygunluğu ve uzaktan yönetimi ile ilgili aşağıdaki hususları içeren kullanım politikası hazırlanmalı ve uygulanmalıdır. • Fiziksel koruma ile ilgili gereksinimler • Parola tanımlama • Yazılım kurulum kısıtları • İşletim sistemi ve uygulama güncelleme politikası • Yedekleme • Bulut servislerinin kullanımı • Kablosuz ağların kullanımı • El değiştirme ve imha Kurum, taşınabilir bilgisayarın temini öncesinde politikayı çalışana tebliğ etmelidir. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda bulundurulmamalıdır.
105	**2-Taşınabilir Cihaz ve Ortam Güvenliği**	2.1-Taşınabilir Bilgisayar Güvenliği	2.1.2 - Güvenlik Yazılımlarının Yüklenmesi	Zararlı yazılımları tespit eden ve önleyen güvenlik yazılımları kullanılmalıdır. Bk. Tedbir No: 1.5.1 Bk. Tedbir No: 1.5.4
106	**2-Taşınabilir Cihaz ve Ortam Güvenliği**	2.1-Taşınabilir Bilgisayar Güvenliği	2.1.3 - Tamire Verilen Taşınabilir Bilgisayarlarda Bulunan Verinin Silinmesi	Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek taşınabilir bilgisayarlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler güvenli yöntemler kullanılarak silinmelidir.
107	**2-Taşınabilir Cihaz ve Ortam Güvenliği**	2.1-Taşınabilir Bilgisayar Güvenliği	2.1.4 - Disk Şifreleme	Taşınabilir bilgisayarlara, çalınma ve kaybolma riskine karşı disk şifreleme uygulanmalıdır. Kullanıcıların disk şifreleme özelliğini devre dışı bırakmaları engellenmelidir.
108	**2-Taşınabilir Cihaz ve**	2.1-Taşınabilir Bilgisayar Güvenliği	2.1.5 - Harici Depolama Ortamlarına Erişimin Yönetimi	Taşınabilir bilgisayarlarda, harici depolama ortamlarına okuma ve yazma izinleri varsayılan olarak devre dışı bırakılmalıdır. İş gereksinimleri doğrultusunda

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
	Ortam Güvenliği			gerekli onayların alınması durumunda okuma ve yazma izinleri devreye alınmalı, yapılan işlemler izlenmelidir.
109	**2-Taşınabilir Cihaz ve Ortam Güvenliği**	2.1-Taşınabilir Bilgisayar Güvenliği	2.1.6 - Taşınabilir Bilgisayar Yönetimi	Taşınabilir bilgisayarlar uzaktan yönetilebilmeli, cihazlara güvenlik politikaları uygulanabilmeli ve gerek duyulduğunda politikalar uzaktan güncellenebilmelidir.
110	**2-Taşınabilir Cihaz ve Ortam Güvenliği**	2.1-Taşınabilir Bilgisayar Güvenliği	2.1.7 - Güncel Olmayan Bilgisayarların Sistemlere Erişiminin Engellenmesi	Güncel olmayan işletim sistemi ve/veya güvenlik yazılımları barındıran bilgisayarların kurum sistemlerine erişimi engellenmelidir.
111	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.1 - VPN Güvenliği	Ajanlar, istemci üzerinde uyumluluk kontrolü yapabilmelidir.
112	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.2 - VPN Güvenliği	Her kullanıcı aynı anda tek oturum açabilmelidir
113	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.3 - VPN Güvenliği	Bağlantının gerekli durumda bireysel veya toplu şekilde sonlandırılabilmesi sağlanmalıdır.
114	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.4 - VPN Güvenliği	Uzaktan bağlantı yapılan istemcinin bağlantı esnasında Kurum etki alanına dâhil olduğu teyit edilmelidir.
115	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.5 - VPN Güvenliği	Uzaktan bağlantı yapılan istemcide bağlantı esnasında oturumun etki alanındaki kullanıcı ile açılmış olmasının teyit edilmesi? (yerel kullanıcılar ile VPN bağlantısı yapılamaması koşulu sağlanmalıdır)
116	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.6 - VPN Güvenliği	Uzaktan bağlantı yapılan istemcide Antivirüs uygulamasının yüklü ve çalışır durumda olduğu teyit edilmelidir.
117	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.7 - VPN Güvenliği	Uzaktan bağlantı yapılan istemcide Antivirüs uygulamasının imza veri tabanı güncelliğinin en az 14 günden yeni olduğu teyit edilmelidir.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
118	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.8 - VPN Güvenliği	Uzaktan bağlantı yapılan istemcilerinde diskinin şifrelenmiş olduğu teyit edilmelidir.
119	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.9 - VPN Güvenliği	Uzaktan bağlantı yapılan istemci İşletim sistemi güncellemelerinin en az 30 günden yeni olduğu teyit edilmelidir.
120	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.10 - VPN Güvenliği	Uzaktan bağlantı yapılan istemcide Registry kaydı kontrolü yapılabilmelidir.
121	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.11 - VPN Güvenliği	VPN bağlantısı "idle time" kontrolü yapılarak belli sürede oturum sonlandırılabilmelidir.
122	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.12 - VPN Güvenliği	VPN erişim kayıtları merkezi kayıt ve log sistemine gönderilebilmelidir.
123	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.13 - VPN Güvenliği	VPN Kullanım raporları alınabilmelidir.
124	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.14 - VPN Güvenliği	VPN kullanımı yetkileri onaylanmış kullanıcılara tanımlanacaktır. Her bağlantıda onay makamına VPN kullanımı bilgilendirme gönderilebilmelidir.
125	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.15 - VPN Güvenliği	VPN üzerinden detaylı log kayıtları alınabilmeli, merkezi log sistemine kayıtlar gönderilebilmelidir.
126	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.16 - VPN Güvenliği	Uzaktan bağlantı istemcisi sadece ilgili kurumun uzaktan bağlantı ara yüzüne bağlanabilmelidir, internet erişimi VPN üzerinden kurum interneti ile olacaktır.
127	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.17 - VPN Güvenliği	Uzaktan bağlantı için çok faktörlü kimlik doğrulama kullanılmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
128	**3-Uzaktan Erişim (VPN) Güvenliği**	3.1-Genel Güvenlik Tedbirleri	3.1.18 - VPN Güvenliği	VPN teknolojisi ajan temelli çalışmaya uygun olmalıdır.
129	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.1 - Bilgisayar Tabanlı Saldırı Tespit ve Engelleme Sistemlerinin Kullanılması	Uzaktan bağlantı istemcilerinde özelinde saldırı tespit ve engelleme sistemi (HIDS/HIPS) kullanılmalıdır. Office makroları ve browser eklentileri devre dışı bırakılmış olmalıdır.
130	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.2 - Servis Güvenliği	Uzaktan bağlantı sunucularında normal işleyişi için gerekli olmayan tüm servisler kapatılmalıdır. Sistemlerde çalışan servisler ihtiyaçları olan en az yetki ile çalışmalıdır. Servis kullanıcılarının yetkileri ayrıca kısıtlanmalıdır. Servislerin döndüğü başlık bilgileri (banner) bilgi ifşasına yol açmayacak şekilde değiştirilmelidir.
131	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.3 - Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Güncel ve güvenlik desteği devam eden işletim sistemleri kullanılmalıdır. Uygulama sürümleri periyodik olarak kontrol edilmelidir.
132	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.4 - Şifreli Haberleşen Servislerin Kullanılması	Şifresiz kimlik doğrulama ve haberleşme kullanan servisler (Telnet, FTP, rlogin, HTTP, SMTP vb.), eğer varsa şifreli haberleşme imkânı sağlayan muadilleri (SSH, SFTP, HTTPS, SMTPS vb.) ile değiştirilmelidir.
133	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.5 - Parola Politikasının Belirlenmesi	Tüm makinelerde kullanıcı parolaları için güçlü bir parola politikası belirlenmelidir. Kullanıcılar ilk girişten sonra parolalarını değiştirmeye zorlanmalı ve parolaların belirli bir süreden sonra geçerliliğini yitirip yenilenmesi sağlanmalıdır. Ayrıca belirli bir sayıda hatalı giriş denemesinden sonra kullanıcı hesapları kilitlenmelidir.
134	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.6 - Son Kullanıcı Bilgisayarlarında Ağ Erişiminin Kısıtlanması	Kullanıcı bilgisayarlarında, bilgisayara ağ üzerinden erişim yetkisi, sadece yönetici hesapları ve uzak masaüstü kullanıcıları veya grupları ile sınırlandırılmalıdır.
135	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.7 - Hata ve Sorun Bilgilerinin Üretici ile Paylaşılmaması	İşletim sistemi kurulumu ile gelen hata ve sorun bilgilerinin üretici ile paylaşılması özelliği pasif hale getirilmelidir.
136	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.8 - Kablosuz Ağ Ara Yüzlerinin Kapatılması	Tüm sunucularda kullanılmayan kablosuz ağ ara yüzleri pasif hale getirilmelidir.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
137	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.9 - Sistem Üzerinde Düzenli Olarak Zafiyet ve Zararlı Yazılım Taraması Yapılması	Sistemde düzenli olarak zafiyet taraması yapılmalı ve bu zafiyetlerin yönetimi gerçekleştirilmelidir. Sistem zararlı yazılımlara karşı düzenli olarak taranmalıdır. Bk. Tedbir No: 1.5.1
138	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.10 - Yerel Güvenlik Duvarı Ayarlarının Yapılması	Bk. Tedbir No: 1.6.11
139	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.11 - Sunucularda Zaman Senkronizasyonunun Sağlanması	Sunucularda ilgili NTP ayarlamaları yapılarak tüm sunucularda zaman senkronizasyonu sağlanmalıdır.
140	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.12 - Merkezi Güncelleme Sunucusu	İşletim sistemi güncellemeleri için merkezi bir güncelleme sunucusu oluşturulmalıdır.
141	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.13 - Sistem İz Kayıtlarının Aktif Edilmesi	Tüm sunucu ve makinelerde iz kayıtları aktif edilmelidir. Sistem zaman ve tarih ayarları, kullanıcı hesapları, ağ yapılandırması, erişim kontrolleri üzerinde yapılan değişiklikler kayıt altına alınmalıdır. Ayrıca giriş ve çıkış bilgileri, yetkisiz dosya okuma denemeleri, dosya silme işlemleri ve sistem yöneticisi hareketleri de kayıt altına alınmalıdır. Bk. Tedbir No: 1.8.1
142	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.14 - Sistem İz Kayıtlarının Merkezi Bir Sunucuda Toplanması	Sistemlerden syslog vb. araçlarla toplanan sistem iz kayıtları merkezi bir kayıt yönetim sistemine gönderilmelidir. Burada toplanan iz kayıtları kurum kritiklik seviyesi ve dinamiklerine uygun olarak işlenmelidir. Bk. Tedbir No: 1.8.6
143	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.15 - Merkezi Kimlik Yönetimi Servisinin Kullanılması	Tüm makinelerde kullanıcı kimlik doğrulama için merkezi kimlik yönetimi servisi kullanılmalıdır.
144	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.16 - Sunucularda Çalışan Servislerin Takibi	Uzaktan bağlantı sunucularında normal işleyişi için gerekli olan servisler dışında başka bir servisin sunucuda açılması halinde alarm üretilmeli ve ilgili servis kapatılmalıdır.
145	**4-Sıkılaştırma Tedbirleri**	4.1-Genel Sıkılaştırma Tedbirleri	4.1.17 - Disk Seviyesinde Şifreleme Yapılması	Uzaktan bağlantı yapılan istemcilerinde disk seviyesinde şifreleme yapılmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
146	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.1 - Kullanıcı Haklarının Kısıtlanması	Kullanıcı hakları en az yetki prensibi göz önünde bulundurularak sadece ihtiyaç duyulan kullanıcı ve gruplara verilmelidir.
147	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.2 - Otomatik Güncellemenin Aktif Olması	Tüm kullanıcı makinelerinde otomatik güncelleme özelliği aktif hale getirilmelidir.
148	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.3 - SMB Protokolü Güvenliği	Uzaktan erişim için kullanılan Windows işletim sistemlerinde SMB versiyon 1 protokolü yerine daha güvenli ve güncel SMB protokol versiyonları kullanılmalıdır.
149	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.4 - Yerel Yönetici Hesapları Yönetimi	Gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesapları devre dışı bırakılmalıdır. Gerekli kullanıcılar için varsayılan olarak aynı tanımlanan yerel yönetici hesaplarının parolaları değiştirilmelidir.
150	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.5 - Ayrıcalıklı Hesap Sayılarının Sınırlandırılması	Etki alanı yöneticisi (Domain Admin) ve diğer yetkili hesapların (Enterprise Admin, Backup Admin ve Schema Admin) sayısı sınırlandırılmalıdır.
151	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.6 - Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi	Yetkili hesapların parola özetlerinin çalınmasının engellenmesi için: • Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında gerekli olmadıkça işlem yapılmamalı, işlem yapıldığı durumlarda kullanıcı bilgisayarlarının yeniden başlatılması sağlanmalıdır. • Yerel bilgisayarlarda parola özetleri tutulma sayısı 0 yapılmalıdır. • Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) grubuna alınmalıdır.
152	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.7 - Kullanılmayan Hesapların Devre Dışı Bırakılması	Aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarını tespit etmek için bir yordam tanımlanmalıdır. Bk. Tedbir No: 1.10.10
153	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.8 - Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması	Sistemlerde yer alan varsayılan yönetici ve misafir hesapları pasif hale getirilmelidir.
154	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.9 - Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması	Standart kullanıcıların betik çalıştırma motorlarına (Windows Script Host, Powershell, Command Prompt ve Microsoft HTML Application Host vb.) erişimi engellenmeli veya kısıtlanmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
155	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.10 - Yönetici Hesaplarının İzlenmesi	Ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ve oturum açma kapama işlemleri izlenmelidir. Bk. Tedbir No: 1.10.11
156	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.11 - Güvenli Yönetici İş İstasyonu Kullanımı	Yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu konumlandırılmalı, ek yazılım veya rol yüklenmemeli, eposta, internet vb. erişimleri için kullanılmamalıdır.
157	**4-Sıkılaştırma Tedbirleri**	4.2-Windows İşletim Sistemi Sıkılaştırma Tedbirleri	4.2.12 - Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi	Aktif dizinde devre dışı bırakılan kullanıcı hesabı için activesync mail erişimi hemen kesilmelidir.
158	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.1 - Güncel Web Sunucu Yazılımlarının Kullanılması	Web sunucu yazılımlarının güncel, zafiyet içermeyen ve üreticisi tarafından desteği devam eden kararlı sürümleri kullanılmalıdır. Ayrıca, sunucuda kullanımda olan tüm araçların/paket programların güvenlik yamaları için düzenli aralıklarla kontrol yapılmalıdır.
159	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.2 - WebDAV Desteğinin Kaldırılması	Web sunucusunun WebDAV (Web Distributed Authoring and Versioning) desteği kaldırılmalıdır. WebDAV ile ilgili modüller pasif hale getirilmelidir.
160	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.3 - Web Sunucusu Kullanıcı Yönetimi	Web sunucu yazılımı yönetici hesabıyla değil, bu amaç için özel olarak oluşturulmuş bir hesap ile çalıştırılmalıdır. Web sunucusunda bulunan varsayılan hesaplar/parolalar kullanım dışı bırakılmalıdır.
161	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.4 - Web Sunucusunun Bilgi İfşalarını Önleyecek Şekilde Yapılandırılması	Web sunucusu bilgi ifşalarını önleyecek şekilde yapılandırılmalıdır. Varsayılan hata ve kurulum sayfaları kaldırılmalıdır. Web sunucu teknolojisi hakkında bilgi ifşasına neden olan HTTP başlıkları kaldırılmalıdır. Hatalı HTTP isteklerine dönen cevaplarda bilgi ifşasına izin verilmemelidir.
162	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.5 - Desteklenen HTTP Metotlarının Kısıtlanması	POST, GET, OPTIONS ve HEAD metotları dışında diğer HTTP metotları desteklenmemelidir. PUT, DELETE, PROPFIND gibi metotlar web servisi için kullanılıyorsa, kullanımlarının sadece web servis ihtiyaçları ile sınırlı olup olmadığı kontrol edilmelidir. Bu metotların dosya yükleme veya silme gibi farklı amaçlarla kullanımı engellenmelidir.
163	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.6 - Dizin Listelemenin Pasif Hale Getirilmesi	Dizin listelemesi pasif hale getirilmelidir.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
164	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.7 - Debug Modunun Kapalı Olması	Web sunucu yazılımı debug (hata ayıklama) modunda çalıştırılmamalıdır.
165	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.8 - İstek Limitlerinin Tanımlanması	Web sunucu yazılımının desteklediği ölçüde, istekler için limitler belirlenmelidir.
166	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.9 - İz Kayıtlarının Alınması	Web sunucu yazılımına ilişkin iz kayıtları alınmalıdır. Bk. Tedbir No: 1.8.1
167	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.10 - Yazma İzni Olan Dizinlerin Kısıtlanması	Yazma izni olan dizinler belirlenmeli, yazma yetkileri sadece dosya yükleme ihtiyacı olan dizinlere verilmelidir. Uygulama üzerinden yüklenen dosyalar için oluşturulmuş dizinlerde çalıştırma izni kaldırılmalıdır.
168	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.11 - SSL/TLS Kullanımı	Sunucu SSL/TLS kullanımına elverişli yapılandırılmalıdır. Bu kapsamda, sunucuda sadece, bilinen zafiyet içermeyen güvenilir sürüme sahip SSL/TLS versiyonları kullanılmalıdır.
169	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.12 - İsteklerin HTTP'den HTTPS'e Yönlendirilmesi	Web sunucusundaki herhangi bir HTTP bağlantı noktası, şifreleme kullanan bir sunucu bağlantı noktasına yönlendirmelidir.
170	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.13 - Kullanılmayan Modüllerin Kaldırılması	Sunucuda sadece kullanılan modüllerin aktif olmalıdır.
171	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.14 - Açık Portların Kısıtlanması	Web sunucusu yalnızca yetkili bağlantı noktalarındaki ağ bağlantılarını dinlemelidir. Kullanımda olmayan portlar kapatılmalıdır. Bk. Tedbir No: 4.1.2
172	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.15 - Kaynak Kullanım Optimizasyonu	Uygulama seviyesinde yapılabilecek servis dışı bırakma saldırılarına karşı aşağıdaki sunucu üzerinde aşağıdaki sıkılaştırmalar yapılmalıdır: • Sunucunun kabul edebileceği maksimum kullanıcı sayısı artırılmalıdır. • Tek bir IP adresinden yapılabilecek bağlantı sayısı sınırlandırılmalıdır. • Her bir bağlantının kullanabileceği maksimum ve minimum transfer hızı belirlenmelidir. • Bağlantılar için zaman aşım değeri belirlenmeli, belirli bir süre açık kalan bağlantılar sonlandırılmalıdır.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
173	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.16 - Sunucunun Korumalı ve Ayrıştırılmış Şekilde Kurulumu	İnternete açık olarak çalışan web sunucu ayrı bir bölgede (DMZ vb.) tutulmalıdır. Bk. Tedbir No: 1.6.6
174	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.17 - Sunucuda Koruyucu HTTP Başlıklarının Kullanımı	Sunucu tarafında koruyucu HTTP başlıkları (X-Frame Options, Strict-Transport-Security vb.) yapılandırılmalıdır.
175	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.18 - Sunucunun Özel Anahtarının (Private Key) Korunması	Sunucunun özel anahtarına (private key) yapılacak yetkisiz erişimlere karşı önlemler alınmalıdır.
176	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.19 - İz Kayıtlarının Merkezi Kayıt Sistemine Gönderilmesi	Web sunucularından alınan iz kayıtları merkezi bir kayıt sistemine gönderilmelidir. Bk. Tedbir No: 1.8.6
177	**4-Sıkılaştırma Tedbirleri**	4.3-Web Sunucusu Sıkılaştırma Tedbirleri	4.3.20 - Sunucuya IP Adresi Üzerinden Erişimlerin Engellenmesi	Sunucuya IP adresi üzerinden yapılan erişimler engellenmelidir.
178	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.1 - Güncel Sanallaştırma Yazılımının Kullanılması	Sanallaştırma sunucusunda kullanılan sanallaştırma yazılımı güncel olmalı ve mevcut güvenlik yamaları yüklü olmalıdır.
179	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.2 - Konteynerların /Sanal Makinelerin Çalıştığı Ana Makine Üzerinde Sıkılaştırmaların Yapılması	Konteynerların/sanal makinelerin çalıştığı ana makine üzerinde sıkılaştırmalar yapılmalıdır. Bk. Bölüm 4
180	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.3 - Sanal Makineler Arasında Zaman Senkronizasyonunun Sağlanması	Bk. Tedbir No: 4.1.11
181	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.4 - Sanal Makineler için İz Kayıtlarının Yönetilmesi	Sanallaştırma ortamında çalışan sanal makineler için alınan iz kayıtları kalıcı bir şekilde saklanmalıdır. Ayrıca bu iz kayıtları merkezi bir kayıt sistemine gönderilmelidir. Bk. Tedbir No: 1.8.1 Bk. Tedbir No: 1.8.6

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
182	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.5 - Mantıksal Birim Numarası (LUN) Maskelemesi Yapılması	Depolama alanı ağı (SAN) etkinliğini ayırmak için imar ve mantıksal birim numarası (LUN) maskeleme kullanılmalıdır.
183	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.6 - Sanallaştırma Ünitesi Üzerinden Konsol Erişimlerinin Kısıtlanması	Sanallaştırma ünitelerine erişim sağlayabilen kullanıcıların, sanal makinelerin sahibi olan kullanıcıların ekranlarını yetkisiz olarak görüntülemesi engellenmelidir. Ayrıca yetkisiz konsol erişimleri de engellenmelidir. Her kullanıcı kimlik doğrulaması sonrasında erişim sağlamalıdır.
184	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.7 - Sanallaştırma Ünitesinde Kullanıcı Yetkilendirme	Sanallaştırma ünitesinde kullanıcılar en az yetki prensibine uygun şekilde ilgili kullanıcı rollerine atanmalıdır.
185	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.8 - Gereksiz Hizmetlerin ve Kullanılmayan Donanımların Kaldırılması	Ana bilgisayardan ve sanal makinelerden gerekli olmayan tüm hizmetler/donanımlar kaldırılmalıdır. Örneğin, kullanılmayan sanal donanımlar (sürücüler, ağ adaptörleri vb.) devre dışı bırakılmalıdır. Ayrıca gereksiz hipervizör hizmetleri (pano paylaşımı, dosya paylaşımı vb.) devre dışı bırakılmalıdır.
186	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.9 - Sanal Makineler Üzerindeki Diskler için Disk Küçültme Konfigürasyonuna Erişimin Kısıtlanması	Sanal disk küçültme (disk shrinking) işleminin sürekli olarak yapılması, sanal diskin kullanılamamasına ve veri kaybına sebebiyet verebileceği için bu ayarı yönetebilecek kullanıcılar belirlenerek, sadece bu kullanıcıların erişimine izin verilmelidir.
187	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.10 - Sanallaştırma Yazılımının Merkezi Olarak Güncellenmesi	Sanallaştırma yazılımı çalıştığı tüm sunucularda merkezi olarak eş zamanlı güncellenmelidir.
188	**4-Sıkılaştırma Tedbirleri**	4.4-Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	4.4.11 - Sunucu Yedeklerinin Alınması	• Düzenli olarak sunucu sistem yedekleri alınmalıdır. Yedekler yetkisiz erişime karşı güvenli ortamlarda muhafaza edilmelidir. Belirli aralıklarla yedekten geri dönme testleri gerçekleştirilmelidir. • Sistemde depolanan verilere ilişkin yedekleme planı hazırlanmalı, bu planda verilerin önem dereceleri, hangi verilerin hangi sıklıkla yedekleneceği ve önem derecelerine göre ilave alınacak önlemlere yer verilmelidir.

S.N.	Ana Madde Grubu	Madde Grubu	Uyumluluk Maddesi	Tanımı
				• Sunucu bilgisayarların işletim sistemi dosyaları, uygulamalara ait veriler (Dosya halindeki veya veri tabanındaki veriler) yedeklenerek, sistemin mümkün olan en az kesintiyle hizmet vermesi sağlanmalıdır. • Birbirinden fiziki olarak ayrı yerlerde tutulan en az iki ayrı yedek bulunmalıdır. • Yedekleme işleminde kullanılan yoğun disk (CD vb.), disket, teyp kartuşu gibi birimlerin üzerine, içlerinde taşıdıkları bilginin gizlilik derecesine göre güvenlik etiketleri yapıştırılmalı ve muhafaza edilmelidir. • Yedekleme yapıldıktan sonra, yedeklemenin doğru yapılıp yapılmadığı kontrol edilmelidir.

KAYNAKÇA
ANA KAYNAKLAR:

1. 29 Haziran 2004 tarihli ve 5201 sayılı "Harp Araç ve Gereçleri ile Silah, Mühimmat ve Patlayıcı Madde Üreten Sanayi Kuruluşlarının Denetimi Hakkında Kanun".

2. 5202 sayılı "Savunma Sanayi Güvenliği Kanunu".

3. 06 Mayıs 2007 tarihli ve 26514 sayılı Resmî Gazetede Yayımlanan "Harp Araç ve Gereçleri ile Silah, Mühimmat ve Patlayıcı Madde Üreten Sanayi Kuruluşlarının Denetimi Hakkında Yönetmelik".

4. 04 Haziran 2010 tarihli ve 27601 sayılı Resmî Gazetede Yayımlanan "Savunma Sanayi Güvenliği Yönetmeliği".

5. MSY.: 317-2 (B) MSB Savunma Sanayii Güvenliği Yönergesi (2003). Bu Yönergenin yayımı ile yürürlükten kaldırılmıştır.

6. C-M (2002) 49 "NATO Güvenlik Politikası Dökümanı."

YASAL DÜZENLEMELER:

1. 3212 sayılı "Silahlı Kuvvetlerin İhtiyaç Fazlası Mal ve Hizmetlerinin Satış, Hibe, Devir ve Elden Çıkarılması; Diğer Devletler Adına Yurt Dışı ve Yurt İçi Alımların Yapılması ve Eğitim Görecek Yabancı Personel Hakkında Kanun".

2. 6136 sayılı "Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanun" ve Kanuna ilişkin 91/1179 No'lu Yönetmelik.

3. 5188 sayılı "Özel Güvenlik Hizmetlerine Dair Kanun".

4. 2565 sayılı "Askerî Yasak Bölgeler ve Güvenlik Bölgeleri Kanunu".

5. 244 sayılı "Milletler Arası Andlaşmaların Yapılması, Yürürlüğü ve Yayımlanması ile Bazı Anlaşmaların Yapılması İçin Bakanlar Kuruluna Verilmesi Hakkında Kanun".

6. 2000/284 sayılı "Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği".

RESMÎ ASKERÎ YAYINLAR:

1. MY:412-1 (A) Türk Silahlı Kuvvetleri MEBS Güvenliği Yönergesi.

2. MY:114-1 (B) Silahlı Kuvvetler İstihbarata Karşı Koyma, Koruyucu Güvenlik ve İş Birliği Yönergesi.

3. MY: 405-1 (A) Türk Silahlı Kuvvetleri Kripto Yönetimi Yönergesi.

4. MY:75-1 (B) Türk Silahlı Kuvvetleri Karargâh Hizmetleri Yönergesi.

SİVİL YAYINLAR:

1. Türkçe Sözlük (TDK-2005)

2. İmla Klavuzu (TDK-2005)