SİVİL HAVACILIK SEKTÖRÜ İŞLETMELERİNE YÖNELİK SİBER GÜVENLİK TALİMATI (SHT-SİBER)

BİRİNCİ BÖLÜM
Amaç, Kapsam, Tanım ve Kısaltmalar, Hukuki Dayanak

Amaç

MADDE 1 -(1) Bu Talimatın amacı; sivil havacılık sektörü işletmelerinin siber tehditlere karşı alması gereken önlemleri ve havacılık sektörü işletmelerince kurulması gereken Kurumsal Siber Olaylara Müdahale Ekibi'nin işletme organizasyonu içerisindeki yerini, kapasite planlamasını, personelin niteliklerini, alması gereken eğitimleri, işletmelerin siber olay öncesi, esnası ve sonrasında yapması gereken çalışmaları, iç ve dış paydaşlar ile iletişime ilişkin usul ve esaslarını belirlemektir.

Kapsam

MADDE 2 -(1) Bu Talimat, Genel Müdürlük tarafından yetkilendirilen tüm sivil havacılık sektörü işletmelerini kapsar.

Dayanak

MADDE 3 -(1) Bu Talimat; 20/10/2012 tarih ve 28447 sayılı Resmi Gazetede yayımlanan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararına, 11/11/2013 tarih ve 28818 sayılı Resmi Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğine, 14/10/1983 tarih ve 2920 sayılı Türk Sivil Havacılık Kanunu'na, 15/07/2018 tarihli ve 30479 sayılı Resmi Gazetede yayımlanan Bakanlıklara Bağlı, İlgili, İlişkili Kurum Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında 4 sayılı Cumhurbaşkanlığı Kararnamesine, 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'na ve Milli Sivil Havacılık Güvenlik Programı Ek 19- Siber Tehditlere Karşı Yapılacak İşlemler Talimatı'na dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 -(1) Bu Talimatta geçen tanımların açıklamaları aşağıda belirtildiği gibidir;

a) **1. Grup Havacılık Sektörü İşletmeleri:** Havayolu işletmeleri, havalimanı işletmeleri, terminal işletmeleri, seyrüsefer hizmet sağlayıcıları,

b) **2. Grup Havacılık Sektörü İşletmeleri:** Yer hizmeti kuruluşları, 10 kişiden daha fazla kişinin çalıştığı hava aracı bakım ve üs bakım kuruluşları,

c) **3. Grup Havacılık Sektörü İşletmeleri:** 1. ve 2. Grup havacılık sektörü işletmeleri dışında kalan tüm sivil havacılık sektörü işletmeleri,

ç) **7x24 Esası:** Bir haftanın 7 günü 24 saat boyunca aralıksız olarak ilgili sistemim işletilmesi,

d) **Balküpü :** Bilgi sistemlerine yetkisiz erişim sağlamak isteyen saldırganlar ya da kullanıcılar hakkında bilgi toplamaya yarayan tuzak sistemler (sunucu, uygulama, servis vb.),

e) **Beyaz Liste:** İşletme bilgi teknolojileri ve operasyonel teknolojileri varlıklarına yüklenmesi uygun bulunan yazılımların listesi,

f) **Bilinmesi Gerektiği Kadar Prensibi:** Bir bilginin sadece kişinin görevi kapsamında bilmesi gerektiği ölçüde verilmesi,

g) **BT Varlıkları:** Bilgi teknolojileri varlıkları,

ğ) **Genel Müdür:** Sivil Havacılık Genel Müdürü,

h) **Genel Müdürlük:** Sivil Havacılık Genel Müdürlüğü,

ı) **Görevler Ayrılığı İlkesi:** Görevler ayrılığı ilkesi hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak için faaliyetler ile karar ve işlemlerin onaylanması, uygulanması, kaydedilmesi ve kontrol edilmesi amacıyla görevlerin farklı personel tarafından yapılmasının sağlanması,

i) **Havacılık Sektörü İşletmeleri:** Sivil havacılık sektöründe faaliyet gösteren işletmeler,

j) **Hizmet Alınan Kuruluş:** Siber güvenlik ile ilgili işletmeye hizmet veren kurum veya kuruluşlar,

k) **İşletme:** Sivil havacılık sektöründe faaliyet gösteren işletmeler,

l) **İşletme Yönetimi:** İşletme üst yönetimi ve varsa yönetim kurulu,

m) **İz kaydı:** Operasyonel bir işlemin başlangıcından bitişine kadar adım adım takip edilmesini sağlayacak kayıtlar,

n) **Kara Liste:** İşletme bilgi teknolojileri ve operasyonel teknolojileri varlıklarına yüklenmesi uygun bulunmayan yazılımların listesi,

o) **Katmanlı Güvenlik Mimarisi:** Bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği güvenlik mimarisi,

ö) **Kırmızı Takım Çalışması:** Bir işletmenin güvenlik cihazlarını, ağlarını, çalışanları, uygulamalarını ve fiziksel güvenlik kontrollerini gerçekte bir saldırıya ne kadar dayanabileceğinin ölçülmesi için tasarlanan tam kapsamlı ve çok katmanlı saldırı simülasyon çalışmalarının tümü,

p) **Kişisel Veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi,

r) **Kritik Bilgi veya Veri:** Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, gizlilik, bütünlük ve erişilebilirliğinin olumsuz yönde etkilenmesinin işletmeye çok ciddi maddi veya manevi zarar vereceği yada iş sürekliliği kesintisine uğratabilecek her türlü bilgi, veri ve kişisel verilerin tümü,

s) **Kritik Varlıklar:** İşletmenin iş sürekliliğini ciddi anlamda sekteye uğratabilecek ve çalışmaması durumunda Türk Sivil Havacılık Sektörünü veya işletmeyi maddi ve itibari yönden zedeleyebilecek sistem, bilgi, belge vb. bütünü,

ş) **Kurumsal SOME:** Temel görevleri Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ'inde ve bu talimatta yer alan, görev yaptığı işletmelerde bulunan siber güvenlik risklerini azaltan ve siber olay meydana geldiğinde görev tanımında yer alan çalışmaları yapan Kurumsal Siber Olaylara Müdahale Ekibi,

t) **Kurumsal SOME Yöneticisi:** 1. Grup havacılık sektörü işletmelerinde siber güvenlikten sorumlu yetkili yönetici, 2. Grup havacılık sektörü işletmelerinde bilgi teknolojileri birimindeki en yetkili yönetici,

u) **Minimum Yetki Prensibi:** Bir varlığa veya kişiye sadece iş ihtiyacını karşılayacak ölçüde yetki verilmesi,

ü) **Minimum Zaman Prensibi:** Bir varlığa veya kişiye sadece iş ihtiyacını karşılayacak sürede yetki verilmesi,

v) **OT Varlıkları:** Havacılık sektörü operasyonlarının sürdürülebilmesi için kullanılan tüm sistem, uygulama ve verileri sağlayacak kayıtları,

y) **Siber Güvenlik Durumsal Farkındalığı:** Bulunulan zaman diliminde işletme sistemlerinin gizlilik, bütünlük ve erişilebilirlik açısından durumu,

z) **Siber Olay:** Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi veya ihlal teşebbüsünde bulunulması,

aa) **Some İletişim Platformu:** USOM tarafından SOME'lerin iletişimi için oluşturulmuş güvenli iletişim platformunu (www.sip.gov.tr),

bb) **Tebliğ:** 11 Kasım 2013 Tarihli ve 28818 Sayılı Siber Olaylara Müdahale Ekiplerinin

Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği,

cc) **Tedarikçi Çıkış Stratejisi:** Hizmet alınan bir tedarikçi firmanın hizmet veya servis verememesi yada işletmenin bir tedarikçi firma ile çalışmayı durdurma kararı alması durumunda alınması planlanan aksiyonların dokümante edilmiş hali,

çç) **Tehdit Avcılığı :** Tehdit istihbarat verilerini temel alan, mevcut güvenlik çözümlerinden kaçan olası siber güvenlik ihlal olaylarının reaktif, proaktif ve tekrarlı olarak arama, tespit etme ve izole etme süreci,

dd) **Trafik Işığı Protokolü:** İşletmenin iç veya dış paydaşlarıyla bilgi paylaşması durumunda, paylaşılacak bilginin gizlilik derecesini ifade eden protokol (bknz. https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol),

ee) **Veri İşleme:** Verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem,

ff) **Yetkili Otorite:** Sivil Havacılık Genel Müdürlüğü

(2) Bu Talimatta geçen kısaltmaların açıklamaları aşağıda belirtildiği gibidir**;**

a) **ATM:** Hava Trafik Yönetimi,

b) **BGYS:** Bilgi Güvenliği Yönetim Sistemi,

c) **BT:** Bilgi teknolojileri,

ç) **CEH:** Etik Hacker Sertifikası (Certified Ethical Hacker),

d) **CISA:** Bilgi Sistemleri Denetçi Sertifikası (Certified Information System Auditor),

e) **CISM:** Bilgi Sistemleri Yöneticisi Sertifikası (Certified Information System Manager),

f) **CISSP:** Bilgi Sistemleri Profesyoneli Sertifikası (Certified Information System Professional),

g) **CRISC:** Risk ve Bilgi Sistemleri Kontrol Sertifikası (Certified Risk and Information Systems Control),

ğ) **DMZ:** Savunmasız bölge,

h) **ECSA:** EC-Council Güvenlik Analisti Sertifikası (EC-Council Certified Security Analyst),

ı) **EKS:** Endüstriyel Kontrol Sistemi,

i) **FKM:** Felaket Kurtarma Merkezi,

j) **GIAC:** Küresel Bilgi Güvencesi Sertifikasyonu (Global Information Assurance Certification),

k) **GSEC:** GIAC Güvenlik Temelleri (GIAC Security Essentials),

l) **IEC:** Uluslararası Elektroteknik Komisyonunu (International Electrotechnical Commission),

m) **ISO:** Uluslararası Standartlar Organizasyonunu (International Organization for Standardization),

n) **MBCO:** En küçük iş sürekliliği hedefi,

o) **NTP:** Ağ zaman protokolü,

ö) **OT:** Operasyonel teknoloji,

p) **RPO:** Olası bir felaket anında kabul edilebilir kayıp miktarı,

r) **RTO:** Olası bir felaket anında normal düzene geri dönüş için kabul edilen kesinti süresi,

s) **SCADA:** Merkezi denetleyici kontrol ve veri toplama sistemi,

ş) **SGSYY:** Siber Güvenlikten Sorumlu Yetkili Yönetici,

t) **SHGM:** Sivil Havacılık Genel Müdürlüğü,

u) **SİP:** SOME İletişim Platformu,

ü) **SLA:** Hizmet seviyesi anlaşması,

v) **SOME:** Siber Olaylara Müdahale Ekibi,

y) **TSE:** Türk Standartları Enstitüsü,

z) **USOM:** Ulusal Siber Olaylara Müdahale Merkezi.

(3) Bu Talimatta belirtilmeyen tanımlar için, 14/10/1983 tarihli ve 2920 sayılı Türk Sivil Havacılık Kanunu ile 10/11/2005 tarihli ve 5431 sayılı Sivil Havacılık Genel Müdürlüğü Teşkilat ve Görevleri Kanunu'nda, ilgili diğer mevzuatta ve ülkemizin üyesi bulunduğu uluslararası sivil havacılık kuruluşları tarafından yayımlanan dokümanlarda belirtilen tanımlar geçerlidir.

İKİNCİ BÖLÜM
Genel Hususlar ve Uygulama Esasları

Siber Güvenlik Kapsamında Yönetim Sorumluluğu

MADDE 5 -(1) Havacılık sektörü işletmeleri aşağıdaki belirtilen durumlardan sorumludur:

a) Bilgi sistemlerinin yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele alır.

b) Bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağını tahsis eder.

c) Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesini sağlar.

ç) Bilgi sistemlerinin kullanımından kaynaklanan siber risklerin yönetilmesi için etkin bir gözetim yürütür.

(2) İşletme bünyesinde siber güvenliğin sağlanmasında nihai sorumluluk işletme üst yönetimi ve varsa yönetim kurulundadır. İşletme yönetimi, bilgi sistemlerine ve operasyonel sistemlere ilişkin siber güvenlik önlemlerinin alınması hususunda gerekli kararlılığı göstermekle ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmekle yükümlüdür. Bu sorumluluk kapsamında işletme yönetimi, işletmenin tamamında, SHGM düzenlemelerine uygun olarak, uygulanmasını gözetmekle yükümlü olduğu bir ISO 27001 Bilgi Güvenliği Yönetim Sistemi tesis eder. Söz konusu yönetim sisteminin aşağıdaki faaliyetleri de içermesi esastır:

a) Etkin bir varlık değerlendirme sürecinin oluşturulması ve bu sürecin sürekli olarak güncel kalmasını sağlanması,

b) İşletme varlıklarına yönelik olarak düzenli bir şekilde siber güvenlik risk ve tehdit değerlendirme çalışmalarının yapılması,

c) Siber güvenliğin sağlanması amacıyla oluşturulan politika, prosedür ve süreç dokümanlarının işletmenin tamamında uygulanmasının sağlanması,

ç) Olası siber güvenlik ihlallerini tespit etme, engelleme ve olay müdahale mekanizmalarının kurulması,

d) İşletme genelinde belirlenen varlık veya süreç envanterine uygun olarak tüm bilgi teknolojileri ve havacılık sektörü hizmetleri, EKS ve SCADA sistemlerinde görevler ayrılığı prensibi ile tutarlı etkin bir kimlik doğrulama ve erişim yönetiminin tesis edilmesi,

e) Siber güvenliğin sağlanmasına ilişkin kontrollerin ve tesis edilen yapıların siber güvenlik açısında test edilmesi, denetlenmesi ve sonuçlarının takip edilerek raporlanması sürecinin oluşturulması ve işletilmesi,

f) İşletme varlıklarına yönelik güncel güvenlik açıklarının takip edilmesi ve gerekli güncellemelerinin ve yama işlemlerinin gerçekleştirilmesi,

g) Üst yönetim de dahil olmak üzere tüm işletme çalışanları, dış hizmet sağlayıcılar ve müşteriler gibi işletmenin siber güvenliğini ilgilendiren tüm paydaşlarına yönelik siber güvenlik farkındalığını artıracak çalışmalar yapılması,

ğ) İşletme siber güvenlik kritik süreçlerin veya operasyonların sürekliliğini sağlamak üzere iş sürekliliği yönetimi ve planının bir parçası olan bilgi sistemleri süreklilik yönetimi süreci ve işletme yönetimi onaylı bir bilgi sistemleri süreklilik planı hazırlanması, süreç sorumlusu atanması ve İş Süreklilik Komitesi tesis edilmesi,

h) Dış hizmet alımlarının yönetimi kapsamında siber güvenliği ilgilendiren hususlarda Kurumsal SOME biriminin değerlendirme süreçlerinde yer almasının sağlanması ve tedarikçi değerlendirme süreçlerinde siber güvenlik unsurlarının değerlendirilmesi,

ı) Havacılık sektörü işletmelerinin dış hizmet alımlarında yüklenici firmadan alacakları hizmet ve sistemi sağlayan birimleri kapsaması zorunlu olmak koşuluyla en az işletmenin siber güvenlik seviyesine uygun hizmet talep edilmesi ve denetim faaliyetleri icra edilmesi.

Siber Güvenlik Strateji Planı

MADDE 6 -(1) 1. Grup havacılık sektörü işletmeleri, işletme yönetimi tarafından onaylanacak bir Siber Güvenlik Strateji Planı oluşturur.

(2) Siber Güvenlik Strateji Planı;

a) Mevcut siber güvenlik yapılanması analizi,

b) Siber güvenlik yapılanması kaynak-ihtiyaç analizi,

c) Güncel siber tehditler ve siber atak yüzeyi değişimi değerlendirilmesi,

ç) Siber güvenlik yapılanmasının iyileştirilmesi için planlanan eylem maddelerinin; proje başlangıç tarihi, proje bitiş tarihi, sorumlu paydaşlar ve proje içeriği detayları

hususlarını içerecek şekilde hazırlanır.

ATM Güvenlik Planı

MADDE 7 -(1) ATM Güvenlik Planı Ek-1'de yer alan ATM Güvenlik Planı Kapsamına uygun olarak;

a) Havacılık Acil Durum Koruma ve Güvenlik Şefliği Birim Sorumlusu,

b) Elektronik Şefliği Birim Sorumlusu,

c) Terminal Elektronik ve BT Şefliği Birim Sorumlusu,

ç) Hava Seyrüsefer Şefliği Birim Sorumlusu

Koordinesi ile oluşturulur ve,

d) Kurumsal SOME Yöneticisi,

e) Havalimanı Müdürü

tarafından imzalanır.

(2) ATM Güvenlik Planı, Ek-2'de yer alan ATM Güvenlik Planı Kontrol Formunun eksiksiz doldurulmuş hali ve SHGM Hizmet Tarifesinde belirtilen ücret dekontu ile birlikte SHGM'ye onay için resmi yazı ile gönderilir.

(3) ATM Güvenlik Planında bir değişiklik olması durumunda Seyrüsefer Hizmet Sağlayıcı İşletmeler güvenlik planını revize ederek SHGM onay işlemlerini tekrarlar.

Siber Güvenlik Kapsamında Organizasyonel Yapı

MADDE 8 -(1) 1 ve 2 inci grup Havacılık Sektörü İşletmeleri, işletme siber güvenlik faaliyetlerini yürütecek bir Kurumsal SOME birimi kurmakla yükümlüdür.

(2) 1 ve 2 inci grup Havacılık Sektörü İşletmeleri, Ek-3'te yer alan Kurumsal SOME Kurulum ve Yönetim Rehberi'nin Ek-5'inde yer alan Kurumsal SOME' ler için Gereksinim Listesi'ne uygun şekilde görevlerini icra eder.

(3) 1 inci grup Havacılık Sektörü İşletmeleri, doğrudan işletmenin Yönetim Kurulu Başkanına veya Genel Müdürüne bağlı bir Siber Güvenlikten Sorumlu Yetkili Yönetici (SGSYY) atayarak, bu yönetici liderliğinde Kurumsal SOME yapılanmasını oluşturur. Bu yönetici, yapacağı uygulamalardan işletme yönetimine ve SHGM'ye karşı sorumludur. SGSYY işletmenin organizasyon şemasında yer alır ve şirket toplantılarında bulunur.

(4) İşletme yönetimi tarafından atanmış olan SGSYY Kurumsal SOME yönetim görevini üstlenir, işletme bünyesinde başka bir görevi bulunamaz.

(5) 2 inci grup havacılık sektörü işletmeleri Kurumsal SOME birimlerini bilgi teknolojileri

birimindeki en yetkili yöneticiye bağlı bir yapıda oluşturur.

(6) 3 üncü grup Havacılık Sektörü İşletmelerinin Kurumsal SOME birimi oluşturma zorunluluğu bulunmamakla birlikte, söz konusu işletmeler mevcut bilgi teknolojileri yapılanmaları kapsamında siber güvenlik yapılanmalarını oluşturur.

MADDE 9 -(1) İşletmenin, Kurumsal SOME kapsamında sorumlu olduğu görevler konunun önemi ve hassasiyeti nedeniyle işletme bünyesinde yürütülmelidir. Ancak zorunlu hallerde Kurumsal SOME yönetim fonksiyonu dışında kalan görevler hizmet alımı yoluyla temin edilebilir.

(2) Kurumsal SOME görevlerinin bir firmadan hizmet alımı yoluyla temin edilmesi durumunda firma ile SLA ve gizlilik sözleşmesi yapılır.

(3) Kurumsal SOME Yöneticisi hiçbir şekilde hizmet alımı yoluyla temin edilemez. Bu nedenle, Kurumsal SOME Yöneticisi işletme çalışanı olmak zorundadır.

(4) İşletmeler, Kurumsal SOME görevlerini yerine getirmek üzere yeteri kadar personel görevlendirir veya yeteri kadar personel ile hizmet alımı yapar.

(5) Bu talimatta belirtilen Kurumsal SOME Görev ve Sorumlulukları işletme içerisindeki başka birimlere devredilemez.

(6) 1.Grup Havacılık Sektörü İşletmelerinde, Kurumsal SOME yapılanması kapsamında görevlendirilmesi planlanan personelin nitelik ve nicelik anlamında yeterliliği SGSYY tarafından değerlendirilir.

(7) Kurumsal SOME' de görev yapan personelin görev tanımları yazılı olarak dokümante edilerek ilgili personele tebliğ edilir.

(8) Kurumsal SOME' de görev yapması planlanan personelin görev tanımlarında bu talimatın Kurumsal SOME Görev ve Sorumlulukları başlığı altında yer alan Kurumsal SOME görevleri dışında görev yapmalarına olanak sağlayacak hiçbir madde bulunamaz.

(9) 2. grup işletmelerde kurulması planlanan Kurumsal SOME birimlerinde yönetim görevini yerine getirecek Kurumsal SOME Yöneticisi Madde 9.8'de istenen zorunluluktan muaftır.

(10) Kurumsal SOME yapılanması hususunda değişiklik olması durumunda en geç 5 iş günü içerisinde SHGM'ye resmi yazı ile bildirim yapılır.

Siber Güvenlikten Sorumlu Yetkili Yönetici

MADDE 10 -(1) 1. Grup havacılık sektörü işletmeleri, faaliyette bulundukları sürece SGSYY bulundurur. Bu yönetici, yapacağı uygulamalardan işletme yönetimine ve SHGM'ye karşı sorumludur.

MADDE 11 -(1) SGSYY'nin uygunluğu, SHGM tarafından aşağıdaki belge ve bilgiler değerlendirilerek belirlenir, uygun olanlara "Siber Güvenlikten Sorumlu Yetkili Yönetici Personel Onay Belgesi" düzenlenir. SGSYY'nin onaylanmasında aranacak şartlar ve istenilen belgeler şunlardır:

a) En az lisans derecesine sahip olduğunu gösteren diploma,

b) Doldurulmuş ve imzalanmış Ek-4'te yer alan Form-4,

c) İş Sözleşmesi,

ç) İletişim bilgilerini de içerecek şekilde hazırlanmış özgeçmiş,

d) Nüfus cüzdanı örneği,

e) Tüm Havaalanları Giriş Kartı Yönetmeliğinin (SHT-17.1) 14'üncü maddesindeki şartları taşımak,

f) Ek-5'de yer alan uluslararası geçerliliğe sahip siber güvenlik sertifikalarından en az 1 tanesine sahip olmak,

g) SHGM Hizmet Tarifesine göre yatırılmış ücret dekontu

MADDE 12 -(1) SGSYY'nin başlıca görevleri ve sorumlulukları aşağıda belirtilmiştir.

a) Kurumsal SOME birimini yönetmek,

b) Havacılık sektörünü etkileyen ulusal ve uluslararası siber güvenlik mevzuatını takip ederek, yeni kuralları ve tavsiyeleri yürürlüğe koymak,

c) Yürürlüğe koyulan politika, prosedür ve uygulamaların yerine getirildiğini denetlemek,

ç) Politika ve prosedürlerin yeterliliğini ve işletme içi uyumu gözlemlemek,

d) Siber güvenlik konusunda, işletmeye ait merkez ve temsilciliklerde sorumlu olmak,

e) İşletmenin siber güvenlik strateji planını hazırlamak, yazılı olarak hazırlanan stratejik planı üst yönetime onaylatmak, onaylanan strateji planını SHGM'ye iletmek,

f) Siber güvenlik strateji planı ile belirlenmiş eylem maddelerinin gerçekleştirilmesini takip etmek, ilgili eylem maddelerinin gerçekleşmemesi veya değiştirilmek istenmesi durumunda işletme üst yönetimine ve SHGM'ye durumu Ek-6'da yer alan formu kullanarak raporlamak,

g) İşletme öz kaynakları veya hizmet alım yöntemi ile temin edilen hizmetlerin siber güvenlik denetimlerini gerçekleştirilmesini sağlamak, düzeltici faaliyetlerin yerine getirilmesini koordine etmek,

ğ) Düzeltici faaliyetler ile ilgili raporlama ve kayıt sistemini oluşturmak,

h) ISO 27001 bilgi güvenliği yönetim sistemi standardı standardı dahilinde yapılan iç denetlemelerin ve tetkiklerin koordinasyonunu sağlamak,

ı) Siber güvenlik alanında gereksinim duyulan kaynakları araştırılarak üst yönetime sunmak,

i) SHGM ile iletişim noktası olup koordinasyonu sağlamak,

j) Gerek Kurumsal SOME personelinin gerekse diğer işletme bünyesinde görev alan personelin siber güvenlik farkındalığını ve işletme siber güvenlik kültürünü artıracak eğitim, seminer vb. programları düzenlemek,

k) Siber güvenlik risk analizi ve tehdit değerlendirmesi yaparak, alınacak ilave önlemleri belirlemek, planlamak ve uygulamak,

l) Siber güvenlik ile ilgili diğer faaliyetlerin kayıtlarının tutulmasını sağlamak,

m) İşletme siber güvenlik faaliyetlerini denetlemek ve iyileştirme çalışmaları gerçekleştirmek,

n) Olası bir siber ihlal durumunda siber olay müdahale sürecini yönetmek,

o) Kurumsal SOME ve ISO 27001 faaliyetlerinin yeterlilik ve uygunluğunu ölçmek amacıyla performans değerlendirmeleri yapmak, sonuçları üst yönetime ve SHGM'ye raporlamak.

MADDE 13 -(1) SHGM tarafından yapılan inceleme ve denetlemelerde, siber güvenlik yönetiminde gerekli faydayı belirli bir süreçte sağlayamayan veya uygulamalarda olumsuzluk ya da havacılık güvenliğini direk etkileyen bir kusur tespit edildiğinde, işletme SGSYY'sinin değiştirilmesi veya siber güvenlik yapılanmasının gözden geçirilmesi, SHGM tarafından istenebilir.

(2) SHGM tarafından görevden alınan SGSYY görevden alınması tarihi itibari ile 5 yıl süre boyunca hiçbir havacılık sektörü işletmesinde görev alamaz.

(3) SGSYY'nin değiştirilmesi veya istihdamın sonlandırılması durumunda Madde 11.1'de belirtilen bilgi ve belgeler ile 30 gün içinde SHGM'den onay istenir.

Kurumsal SOME Personel Nitelikleri

MADDE 14 -(1) Kurumsal SOME'nin görev ve sorumluluklarının gerçekleştirilebilmesi için, Kurumsal SOME' de çalışacak personelin en az ön lisans programlarından mezun olması ve en az iki yıl bilgi işlem veya siber güvenlik konusunda bilgi ve tecrübeye sahip olması gerekmektedir.

(2) Lisans programı mezunu personelde en az bir yıl bilgi işlem veya siber güvenlik alanında bilgi ve tecrübeye sahip olması gerekmektedir.

(3) Siber güvenlik alanında yüksek lisans veya doktora yapmış personelde tecrübe aranması zorunlu değildir.

MADDE 15 -(1) İşletme, Kurumsal SOME personellerinin Kurumsal SOME'de görevlendirilmesinden itibaren 6 ay içerisinde birimdeki görevleri kapsamına uygun olarak Ek-7'de yer alan eğitimleri eksiksiz bir biçimde almalarını ve belirtilen süreler dahilinde tazeleme eğitimlerinin alınmasını sağlar.

(2) İşletme, siber güvenlik faaliyetlerinde görev alacak personellerinin görevlerini icra edebilmesi için gerekli her türlü eğitimi almalarını sağlar.

(3) İşletme, Kurumsal SOME personelinin görev ve sorumluluklarını yerine getirebilmesi için gerekli olan temel yetkinliklere sahip olabilmesi amacıyla güncel teknolojiyi takip etmesini sağlar.

ÜÇÜNCÜ BÖLÜM
Kurumsal SOME Görev ve Sorumlulukları

Kurumsal SOME Yönetim Görevi

MADDE 16 -(1) 1.grup havacılık sektörü işletmelerinde Kurumsal SOME yönetim görevi SGSYY tarafından gerçekleştirilir.

(2) 2.grup havacılık sektörü işletmelerinde Kurumsal SOME yönetim görevi bilgi teknolojileri birimindeki en yetkili yönetici tarafından gerçekleştirilir.

(3) Kurumsal SOME Yöneticisi, Kurumsal SOME birimi görevlerinin etkin ve sürdürülebilir bir şekilde yerine getirilmesinden sorumludur.

Siber Güvenlik Politika ve Prosedürleri Oluşturma ve Güncel Tutma Görevi

MADDE 17 -(1) Kurumsal SOME, bilgi sistemlerinin ve operasyonel sistemlerin kullanımından kaynaklanan siber güvenlik risklerini yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden siber güvenlik politika, prosedür ve süreç dokümanlarını oluşturur. Bu madde kapsamında oluşturulan tüm dokümanlara, dokümanların gizlilik derecesi ve işletme çalışanlarının görev ve sorumluluklarının uygunluğu nispetinde erişim imkanı verilir. Dokümantasyon içerisinde ilgili teknik veya idari tedbirler dışında, asgari olarak doküman kodu, dokümanın gizlilik derecesi, dokümanı onaylayan, yenilenme tarihi, gözden geçirme tarihi, yenilenme tarihçesi bilgileri yer alır.

(2) Siber güvenlik politika, prosedür, süreç ve siber güvenlik strateji planının gerekleri, işletmenin organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir, bunların işlerliğine ilişkin gözden geçirme faaliyetleri senede az 1 kere gerçekleştirilir ve gerekli görülmesi durumlarında iyileştirme çalışmaları yapılır. Bu kapsamda, politika ve prosedürlerin işletilmesinin takibinden Kurumsal SOME Yöneticisi sorumludur.

(3) Oluşturulan veya güncellenen tüm siber güvenlik ile alakalı politika ve prosedürler Kurumsal SOME Yöneticisinin yazılı veya dijital onayından geçerek işletme yönetimi onayına sunulur.

MADDE 18 -(1) İşletme siber güvenlik politika veya prosedürlerine uygun hareket edilmemesi durumunda ilgili personele uygulanacak disiplin mekanizması belirlenir, dokümante edilir ve işletilir.

(2) 1.grup işletmelerde, İşletme siber güvenlik politika veya prosedürlerine uygun hareket edilmemesi durumunda personele uygulanacak disiplin cezasına karar verilecek heyette SGSYY'de asil üye olarak görev alır.

Siber Güvenlik Kültürü Oluşturma ve Takip Etme Görevi

MADDE 19 -(1) Kurumsal SOME, işletme bütününde bir siber güvenlik kültürü oluşturmak amacıyla siber güvenliğini ilgilendiren tüm iç ve dış paydaşlarına yönelik siber güvenlik farkındalık programı oluşturur, yürütür ve denetler.

(2) Kurumsal SOME, bilgi teknolojileri kaynaklarına ve sistemlerine fiziksel veya dijital erişimi olan iç ve dış kaynaklı tüm personelin siber güvenlik farkındalık seviyesini artırmak ve işletme genelinde siber güvenlik kültürü oluşturmak için kapsamlı bir siber güvenlik farkındalığı eğitim programı oluşturur.

(3) Siber güvenlik farkındalığı eğitim programı, siber güvenlik politikaları ve standartları ile birlikte, siber güvenlik konusundaki bireysel sorumlulukların neler olabileceği, bilgi varlıklarını korumak için alınması gereken önlemler ve ilgili siber güvenlik politika veya prosedürlerine uyulmaması halinde işletme personelinin karşılaşacağı disiplin süreçleri hakkında bilgi içerir.

MADDE 20 -(1) Kurumsal SOME, işletme içi siber güvenlik farkındalık çalışmaları kapsamında aşağıda belirtilen hususları içerecek bir çalışma programı hazırlar.

a) İşletme personeline örgün, uzaktan veya bütünleşik eğitim yöntemi ile rol ve sorumluluk kriterlerine göre sınıflandırılmış bir siber güvenlik farkındalık eğitim programının hazırlanması ve bu eğitimlerin en az senede bir tazeleme eğitimlerinin verilmesi,

b) İşletme personeline rol ve sorumluluklarına göre maruz kalabilecekleri siber saldırı çeşitlerinin tanıtılması ve örnekler üzerinden bilgilendirme yapılması,

c) İşletme personeline sunulmak üzere siber güvenlik farkındalığı ve siber hijyen ile ilgili el kitaplarının oluşturulması ve personel kullanımına sunulması,

ç) Siber güvenlik eğitim materyallerinin en az senede bir gözden geçirilmesi ve güncel siber tehditler kapsamında güncellenmesi,

d) Siber güvenlik farkındalık eğitimi sonrasında eğitimi alan personelin yetkinlik seviyesinin Kurumsal SOME tarafından değerlendirilmesi,

e) İşletme çalışanlarına yönelik siber güvenlik ile ilgili bilgilendirme bültenlerinin hazırlanması ve çalışanlar ile paylaşılması,

f) 1.grup havacılık sektörü işletmelerinde; İşletmenin bilişim sistemlerine erişimi olan bütün çalışanlarına yönelik 3 ayda bir sosyal mühendislik testlerini yapması veya yaptırması ve yönetici özetlerinin testin bitiminden en geç 1 ay sonra SHGM'ye gizli resmi yazı ile bildirmesi,

g) 2.grup havacılık sektörü işletmelerinde; İşletmenin bilişim sistemlerine erişimi olan bütün çalışanlarına yönelik 6 ayda bir sosyal mühendislik testlerini yapması veya yaptırması ve yönetici özetlerinin testin bitiminden en geç 1 ay sonra SHGM'ye gizli resmi yazı ile bildirmesi,

ğ) Siber güvenlik farkındalığı konusunda yetersiz görülen personellerin tespit edilmesi ve bu personellerin siber güvenlik farkındalığının arttırılabilmesi için eğitim süreçlerinin gözden geçirilerek işletme çalışan profiline uygun eğitim doküman ve yöntemleri ile siber güvenlik farkındalık eğitimlerinin tekrarlanması,

h) İşletme personelinin gözlemledikleri siber ihlal durumlarını, şüpheli hareketleri ve işletme siber güvenlik kültürünü arttırma yönündeki önerilerini raporlayabilecekleri bir raporlama sisteminin oluşturulması gerekmektedir.

Siber Güvenlik Risk Analizi ve Yönetimi Görevi

MADDE 21 -(1) İşletme tüm bilgi teknolojileri varlıklarına ilişkin varlık envanterini oluşturmak, bu varlıkları EK-8'de yer alan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi madde 2.1.'e uygun bir şekilde gruplamak ve yönetmek ile yükümlüdür.

MADDE 22 -(1) Kurumsal SOME, alan uzmanları ile birlikte, siber güvenlik risklerini analiz eder, azaltmak, takip etmek ve raporlamak üzere bir siber güvenlik risk yönetim süreci tesis eder.

(2) Kurumsal SOME, siber güvenlik risk analizi sonuçlarına göre tespit edilen her bir siber güvenlik riskine ilişkin, bu risklerin ilişkili olduğu varlıkların değerine ve işletmenin risk limitlerine uygun olacak şekilde risk indirgeme ve kontrol stratejileri belirler. Söz konusu bu varlıkların değerleri ele alınırken bu varlıkların ilişkili olduğu iş hedeflerini ve iş süreçleri ile bunların bağlı olduğu diğer iş hedeflerini ve iş süreçlerini dikkate alır. Risk indirgeme ve kontrol stratejilerinin

belirlenmesi aşamasında, Kurumsal SOME koordinesinde riskin ilgili olduğu iş tarafının temsilcileriyle beraber siber güvenlik risk analizi sonucu oluşturulur.

MADDE 23 -(1) Söz konusu siber güvenlik risk analizi kapsamında aşağıda belirtilen faaliyetler yerine getirilir:

a) Tespit edilen varlıklara veya süreçlere ilişkin tehdit ve güvenlik açıklarının tespit edilmesi suretiyle siber güvenlik risklerin belirlenmesi,

b) Tespit edilen tehdit ve güvenlik açıklarına göre bilgi varlıklarının riske maruz kalma olasılıklarının belirlenmesi,

c) Siber güvenlik risklerin gerçekleşmesi durumunda ilişkili varlığın gizlilik, bütünlük, erişilebilirlik kriterlerine yönelik etki ve risk hesaplaması yapılması,

ç) Siber güvenlik risk analizinde gerçekleştirilen çalışmaların bütününü temsil ederek özetleyecek ve aşağıdaki hususları içerecek şekilde yazılı veya dijital bilgi varlıklarına ilişkin siber güvenlik risk değerlendirme raporunun oluşturulması:

1) Varlık veya süreç,
2) Varlık veya süreç sahibi,
3) Varlığın veya sürecin etkilediği diğer varlıklar veya süreçler,
4) Risk kategorisi,
5) Tehdit,
6) Güvenlik açığı,
7) Mevcut kontroller,
8) Risk seviyesi,
9) Etki analizi sonucu,
10) Alınması planlanan kontroller.
11) Risk indirgeme planlanan tarihi,
12) İndirgeme faaliyeti durumu.

MADDE 24 -(1) Risk indirgeme ve kontrol stratejilerinin belirlenmesi aşamasında risklerin nasıl ele alınacağına Kurumsal SOME biriminin önderliğinde karar verildikten sonra bu kararların uygulanmasını sağlayacak siber güvenlik risk aksiyon planları oluşturulur. Alınacak aksiyonlar için yapılacak kaynak aktarımında ve aksiyonların tamamlanma tarihlerinin belirlenmesinde , risk analizi aşamasında tespit edilen risk dereceleri dikkate alınır.

(2) Risk aksiyon planında belirlenen aksiyonların alınması risk analizi sonucu tespit edilen riskleri ortadan kaldırmıyorsa, aksiyon planının uygulanması sonucu kalacak artık riskler tespit edilir ve risk aksiyon planı güncellenir.

MADDE 25 -(1) Risk analizleri sonucu hazırlanan güncel risk değerlendirme raporu ve güncel risk aksiyon planı birleştirilerek işletmenin siber güvenlik risk envanteri oluşturulur.

(2) İşletme, yılda en az bir defa siber güvenlik risk analizlerini tekrarlar. Tekrarlanan risk analizi sonuçlarına göre risk aksiyon planı ve siber güvenlik risk envanterinin güncellenmesi sağlanır.

(3) İşletme bünyesinde gerçekleştirilen siber güvenlik iç kontrol-iç denetim çalışmalarının, tüm Kurumsal SOME faaliyetlerinin, iç ve dış kaynaklar ile gerçekleştirilen sızma testi sonuçlarının, sistem test sonuçlarının ve SHGM denetimleri sonucunda tespit edilen bulguların risk envanterine girdi teşkil etmesi sağlanır.

(4) İşletme bilgi sistemlerinde meydana gelecek önemli değişikliklerden sonra siber güvenlik risk değerlendirmesini tekrarlar.

(5) İşletme, siber güvenlik risk yönetimi çalışmalarına, bütüncül bir güvenlik bakış açısıyla, işletme varlıklarına yönelik olarak gizlilik, bütünlük, erişilebilirlik kriterleri doğrultusunda aktif katkı

sağlar.

MADDE 26 -(1) 1.Grup havacılık sektörü işletmelerinde bir siber güvenlik riskinin kabul edilebilmesi için SGSYY'nin, söz konusu siber güvenlik riskine sahip iş tarafının en üst düzey yöneticisinin ve İşletme Genel Müdürünün yazılı veya dijital inkar edilemez onayının bulunması ve söz konusu riskin Sivil Havacılık Genel Müdürlüğü mevzuatlarına aykırılık teşkil etmemesi şarttır.

(2) 2.Grup havacılık sektörü işletmelerinde bir siber güvenlik riskinin kabul edilebilmesi için söz konusu siber güvenlik riskine sahip iş tarafının en üst düzey yöneticisinin ve İşletme Genel Müdürünün yazılı veya dijital inkar edilemez onayının bulunması ve söz konusu riskin Sivil Havacılık Genel Müdürlüğü mevzuatlarına aykırılık teşkil etmemesi şarttır.

(3) Kurumsal SOME, kabul edilen siber güvenlik riskleri için, sonradan telafi edici yeni kontrol tekniklerinin ya da yeni güvenlik çözümlerinin ortaya çıkmış olması veya riskin önceki siber güvenlik risk değerlendirmelerine göre artıp artmadığı yönünde koşulların değişmiş olması ihtimaline karşı, önceden kabul edilmiş olan siber güvenlik risklerini periyodik olarak yılda en az bir defa gözden geçirir ve yapılan çalışmaları dokümante eder.

MADDE 27 -(1) Kurumsal SOME, detaylı siber güvenlik risk değerlendirmesini işletme yönetimine ve BGYS iç paydaşlarına Yönetim Gözden Geçirme toplantılarında aktarır.

BT Kritik Alanların Fiziksel Güvenliğinin Sağlanması Görevi

MADDE 28 -(1) Kurumsal SOME, hassas veya kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırlarını belirler.

(2) Kurumsal SOME, belirlemiş olduğu hassas veya kritik bilgi ve bilgi işleme olanaklarını barındıran alanları korumak için gereken güvenlik kontrollerini işletme fiziksel güvenliğinden sorumlu birim veya birimler ile birlikte belirleyerek dokümante eder.

(3) Kritik bilgi sistemleri, uygun güvenlik engelleri ve giriş kontrollerine sahip veri merkezleri, sistem odaları, ağ ekipman odaları gibi güvenli alanlarda barındırılır. Bu alanlara erişim, sadece erişim yetkisine sahip olması gereken personelle sınırlandırılır, Kurumsal SOME erişim haklarını düzenli olarak gözden geçirir ve günceller.

(4) Kritik bilgi sistemlerini içeren fiziksel alanda görev yapan personel dışında herhangi bir işletme personeli, ziyaretçi, dış hizmet sağlayıcı ya da yüklenici firma personelinin veri merkezlerine ve kritik bilgi sistemlerine erişimleri onay mekanizmasına tabi tutulur, bunların erişim ve sonrası faaliyetleri detaylı bir şekilde izlenir ve veri merkezindeki çalışmaları boyunca mutlaka kendilerine refakat edilir. Bu çerçevede, veri merkezlerine ve sistem odalarına yapılan erişim talepleri ve onayları ile bu erişimler kapsamında gerçekleştirilen işlemler ve giriş çıkışlar için iz kaydı tutulur.

(5) Kurumsal SOME, işletme fiziksel güvenlik birimi ile koordineli bir şekilde çalışarak, kritik BT ve OT varlıklarının bulunduğu alanlara yönelik alınan fiziksel güvenlik kontrollerinin yeterliliğini, etkinliğini ve uygulanmasını denetler.

Siber Güvenlik Kapsamında Erişim Yönetimi Görevi

MADDE 29 -(1) Kurumsal SOME, işletme tüm bilgi varlıklarına olan erişimlerin, görevler ayrılığı prensibine göre belirlenmiş kullanıcılarca ve bu kullanıcıların sorumluluğu gereği kendileri için tanımlanan erişim kontrol kuralları uyarınca, ilişkili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirilmesini sağlar.

(2) Kurumsal SOME, bilgi sistemleri üzerindeki kullanıcılara uygulanacak kimlik doğrulama mekanizması, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde tesis edilmesini sağlar ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alındığını denetler.

(3) Kurumsal SOME, bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama

bilgilerinin gizliliğine ve güvenliğine yönelik gerekli önlemleri aldırır.

MADDE 30 -(1) Kurumsal SOME, son kullanıcıların işletme kritik varlıklarını etkileyebilecek sistemler üzerindeki erişim hakları matrisini ilgili iş birimleri ile koordineli bir şekilde oluşturur ve bu yetki erişim matrisini en az 3 ayda bir gözden geçirir.

(2) Kurumsal SOME, varlıklarının kritiklik seviyesini de göz önünde bulundurarak, her bir işletme varlığı için yetki erişim denetleme süre ve süreçlerini belirler.

(3) Kurumsal SOME, işletme ayrıcalıklı kullanıcılarının erişim hakları matrisini ilgili iş birimleri ile koordineli bir şekilde oluşturur ve bu yetki erişim matrisini en az ayda bir gözden geçirir.

(4) Kurumsal SOME, ayrıcalıklı erişim hakkına sahip kullanıcıların standart kullanıcı hesaplarının olmasını ve ayrıcalıklı erişim haklarına ihtiyaç duyulmayan işlerde standart kullanıcı hesaplarının kullanmasını sağlar ve denetler.

MADDE 31 -(1) İşletme verilen tüm erişim haklarında en az yetki prensibini uygular.

(2) İşletme verilen tüm erişim haklarında işin gereksinimini dikkate alarak minimum süre kapsamında yetki tanımlaması yapar.

(3) Erişim hakkı verilme ve alınma işlemleri değişiklik yönetimi sürecine dahil edilerek Kurumsal SOME Yöneticisi koordinasyonunda yürütülür.

MADDE 32 -(1) Kurumsal SOME, Kurum içi paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin güvenli kanallar üzerinden olduğunu denetler.

Siber Güvenlik Kapsamında İşletim Güvenliği Görevi

MADDE 33 -(1) Kurumsal SOME, işletme bilgi teknolojileri varlıklarına ait kaynakların kullanımı izler, ayarlar ve gerekli sistem performansını temin etmek için gelecekteki kapasite gereksinimleri ile ilgili çıkarımlar ve analizler yapar.

MADDE 34 -(1) Kurumsal SOME, BT ve OT varlıklarına yüklenebilecek uygulamalar için beyaz liste ve kara liste oluşturur ve uygulandığını denetler.

(2) Beyaz liste sadece iş gereksinimleri kapsamında ihtiyaç duyulan uygulamaları içerir. Geçerli bir iş gereksinimi bulunmayan uygulamalar beyaz listeye eklenemez.

(3) Kurumsal SOME 7X24 esasına göre kullanılan uygulama ve sistemlerin en güncel versiyonlarının kullanıldığını takip eder.

(4) İhtiyaç duyulan versiyon güncellemeleri merkezi bir yapıdan uygulanır.

(5) İşletme lisanssız yazılım kullanmamalıdır.

MADDE 35 -(1) Zorunlu bir iş gereksinimi olmadıkça ve Kurumsal SOME Yöneticisi tarafından yazılı veya elektronik bir şekilde onaylanmadıkça personelin ya da dış hizmet sağlayıcıların yerel yönetici haklarına sahip olması engellenir.

MADDE 36 -(1) İşletme, meydana gelen değişiklikler sebebiyle gerçekleşebilecek hata ve sorunların sayısını ve etkisini en aza indirecek, değişikliklerin etkili, hızlı ve kontrollü bir şekilde gerçekleştirilmesini ve değişiklikler sırasında yapılan işlemlerin değişiklik sonrasında da denetlenebilir olmasını sağlayacak etkin bir siber güvenlik değişiklik yönetimi süreci tesis eder.

(2) İşletme bilgi teknolojileri veya siber güvenlik süreçlerini etkileyen her değişiklikte siber güvenlik değişiklik yönetim sürecini uygular.

(3) Değişiklik yönetimi çalışmaları, görevler ayrılığı prensibine uygun olarak icra edilir, test

edilir, gerçekleştirilir, kayıt altına alınır, geri dönüş planları hazırlanır ve tüm süreç dokümante edilir.

(4) Değişiklik yönetimi kapsamındaki tüm değişikliklerin kimlik doğrulaması uygun tekniklerle gerçekleştirilmiş yetkili kullanıcılar tarafından yapılır, bunlar için yeterli iz kaydı tutulur ve tutulan iz kayıtları düzenli olarak gözden geçirilir.

MADDE 37 -(1) BT, OT veya siber güvenlik süreçlerini etkileyen değişikliklerde Kurumsal SOME Yöneticisi onayı alınır.

MADDE 38 -(1) Kurumsal SOME, havacılık sektörü faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığını azaltmak için sistem, yazılım ve cihazlardaki güvenlik açıklarını hızlı ve etkin bir şekilde ele alacak bir yama yönetimi süreci tesis edilmesini sağlar. Yama yönetim süreci kapsamında aşağıdaki faaliyetleri yerine getirir;

a) Uygulanacak yamaların güvenilir bir kaynaktan gelmesini sağlayacak ve bunu doğrulayacak teknikler kullanılması,

b) İşletme tarafından kullanılan sistem, yazılım ve cihazlarda yer alan güvenlik açıklarının ve bu açıklara yönelik yamaların tespit edilmesi,

c) Tespit edilen yamaları uygulamanın ya da uygulamamanın etkisinin değerlendirilmesi,

ç) Yamaların nasıl uygulanacağına ilişkin metotların tanımlanması,

d) Uygulanacak yamaların uygulama öncesi test edilmesi,

e) 1. Grup işletmelerde uygulanan ya da uygulanmamasına karar verilen yamalarla ilgili SGSYY'nin yazılı veya dijital onayının alınması,

f) Yamaların uygulanması ya da yanlış uygulanması sırasında sorun çıkması halinde sorunun ne şekilde çözüme kavuşturulacağına dair metotların tanımlanması,

g) Uygulanamayan yamaların gidermeye çalıştığı güvenlik açıklarına ilişkin riskleri azaltmaya yönelik telafi edici kontrollerin tesis edilmesi.

(2) Sağlayıcı veya üretici desteği biten sistem, yazılım ve cihazlar artık yamalanamadığında, bunlar için yüklenebilen en son güncellemelerin günün şartlarına göre artık güvenli olmaması ve telafi edici kontroller ile de makul seviyede bir güvenlik sağlanamaması halinde söz konusu sistem, yazılım ve cihazlar kullanımdan kaldırılır.

Siber Güvenlik Tedarikçi Yönetimi Görevi

MADDE 39 -(1) İşletme, siber güvenlik direncinin arttırılması ve iş sürekliliğinin sağlanması amacıyla BT, OT ve havacılık sektörü süreçlerinin işleyişini veya güvenliğini etkileyen tüm tedarikçilerinin kapsama dahil edildiği etkin bir siber güvenlik tedarikçi yönetim süreci tesis eder.

(2) Kurumsal SOME, işletme kritik tedarikçilerini ve bu tedarikçilerin etkilediği süreçleri Ek-9'da yer alan Siber Güvenlik Kritik Tedarikçi Envanteri'ne uygun bir şekilde dokümante eder.

(3) Kurumsal SOME, siber güvenlik kritik tedarikçi envanterini en az senede bir gözden geçirir ve ihtiyaç halinde günceller.

MADDE 40 -(1) Kurumsal SOME, İşletmenin verisine erişebilen, verilerini işleyebilen, depolayabilen, iletebilen veya işletmenin bilgisi için bilgi teknolojileri altyapı bileşenlerini temin edebilen tedarikçilerine yönelik siber güvenlik gereksinimlerini belirler.

MADDE 41 -(1) Kurumsal SOME, senede en az 1 kere kritik tedarikçilerinin sunduğu hizmeti siber güvenlik açısından denetler veya denetlettirir.

MADDE 42 -(1) İşletme tarafından yapılan siber güvenlik ve iş sürekliliği risk ve etki çalışmaları tedarikçi yönetim süreçlerini de içerir.

MADDE 43 -(1) İşletme tedarikçi hizmetlerindeki değişiklikleri yönetmek için tedarikçi çıkış stratejileri oluşturur.

MADDE 44 -(1) Siber güvenlik tedarikçi yönetim süreci kapsamında, Kurumsal SOME birimi tarafından belirlenmiş olan siber güvenlik kriterlerinin sözleşmelere dahil edilmesi sürecinin işletme genelinde uygulanması Kurumsal SOME tarafından denetlenir, tespit edilen uygunsuzluklar işletme üst yönetimine yazılı bir şekilde iletilir, tedarikçi yönetim süreci işletilir.

İç ve Dış Kaynaklı Sistem Temin, Geliştirme Görevi

MADDE 45 -(1) Bilgi sistemlerinin tasarımı, geliştirilmesi, test edilmesi ve sürdürülmesinde, görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlanır. Bu kapsamda sistem ve uygulamaların geliştirilme süreci, kaynak kodlarının tek bir kişi tarafından hazırlanıp derlenerek geliştirme, test ve üretim ortamları arasında taşınmasına imkân vermeyecek şekilde görevler ayrılığı prensibine uygun olarak işletilir.

MADDE 46 -(1) İç veya dış kaynaklar kullanılarak geliştirilmesi planlanan her tür yazılım ve sistem geliştirme veya temin etme süreçlerinde Kurumsal SOME'den söz konusu geliştirmenin siber güvenlik açısından uygunluğu kapsamında yazılı veya dijital onay alınır.

MADDE 47 -(1) İşletme iç veya dış kaynaklar kullanılarak geliştirilen uygulamalarda Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Geliştirme Rehberine uygun bir şekilde süreci yönetir.

BT Süreçlerinde İş Sürekliliğinin Sağlanması Görevi

MADDE 48 -(1) 1. Grup işletmelerde havacılık sektörü faaliyetlerini yürütmede kullanılan bilgi teknolojileri ve süreçlerinin sürekliliğini sağlamak üzere, SGSYY ve İşletme Genel Müdürü veya Yönetim Kurulu tarafından onaylı iş sürekliliği yönetimi ve planının bir parçası olan bir bilgi sistemleri süreklilik planı hazırlanır, süreç sorumluları atanır ve İş Sürekliliği Komitesi tesis edilir.

(2) 2. Grup işletmelerde Havacılık sektörü faaliyetlerini yürütmede kullanılan Bilgi Teknolojileri süreçlerinin sürekliliğini sağlamak üzere, İşletme Genel Müdürü veya Yönetim Kurulu tarafından onaylı iş sürekliliği yönetimi ve planının bir parçası olan bir bilgi sistemleri süreklilik planı hazırlanır, süreç sorumluları atanır ve İş Sürekliliği Komitesi tesis edilir.

(3) İş Sürekliliği Komitesi ilgili alan uzmanları ve teknik uzmanlarda dahil olmak üzere tüm paydaşların temsilcilerinden oluşur ve işletme Genel Müdürü veya Yönetim Kurulu Başkanı bu komiteye başkanlık eder. İş Sürekliliği Komitesi meydana gelen siber olaylarla ilgili bütün faktörleri göz önünde bulundurarak kriz durumu olduğunu ilan etmekle, planın devreye alınmasına karar vermekle ve diğer kurtarma, süreklilik ve müdahale ekipleriyle koordinasyonu sağlamakla yükümlüdür.

(4) İş sürekliliği komitesi ilgili iş sürekliliği yönetim sürecini tesis ederken kendisini etkileyen tüm iç ve dış etkenleri değerlendirir.

MADDE 49 -(1) BT süreçlerinde iş sürekliliğinin sağlanmasında işletme, ISO 22301 İş Sürekliliği Yönetim Sistemi Standardını temel alır ve bu standardın gereksinimlerini yerine getirir.

MADDE 50 -(1) Kurumsal SOME, BT iş sürekliliği çalışmaları kapsamında aşağıdaki faaliyetlerin yerine getirilmesini koordine eder;

a) İş etki analizi, risk değerlendirmesi, risk yönetimi, izleme ve test faaliyetlerini içeren bir bilgi sistemleri iş sürekliliği yönetim sürecinin tesis edilmesi,

b) İş birimlerinin de katılımıyla gerçekleştirilen iş etki analizi ve önceliklendirilen iş hedefleri çerçevesinde bilgi sistemleri iş sürekliliği planının geliştirilmesi, Ek-11'de yer alan forma uygun olarak dokümante edilmesi ve kurtarma için gerekli olan kritik işlemlerin belirlenmesi,

c) Bilgi sistemleri iş sürekliliği planının uygulanabilir olmasının sağlanması,

ç) Yılda en az bir defa, iş sürekliliği denetimleri, tatbikatları ve risk analiz çalışmaları sonucu tespit edilen bulgular ve testlerden öğrenilen derslere göre veya iş süreçlerini ya da bilgi sistemlerinin sürekliliğini etkileyen değişikliklerden sonra planın gözden geçirilerek güncellenmesi,

d) Bilgi sistemleri iş sürekliliği planının ilgili diğer planlarla ve mevzuat gereksinimleriyle uyumlu olmasının sağlanması,

e) Yaşanan acil durum ve felaketlerden kaynaklanan yasal konuların ele alınması, halkla ilişkiler ve basın ile olan iletişimin yürütülmesi,

f) İlgili ekiplere ve çalışanlara iş sürekliliği planı kapsamında eğitim verilmesi ve iş sürekliliği farkındalığın artırılması,

g) İş sürekliliği çalışmalarının görevler ayrılığı ilkesi de gözetilerek objektif bir şekilde değerlendirilmesi.

MADDE 51 -(1) İşletme, bir yada daha fazla kritik sürecin beklendiği gibi çalışmadığı durumlarda, tüm sistemin veya havacılık sektörü faaliyetlerinin bir bölümünün çalışamaz hale gelmesini önlemek adına kritik sistem ve uygulama süreçleri için veri yedekleme, yedekli çalışma ve hazırda bekleme mekanizmalarını kurar.

MADDE 52 -(1) İşletme, olası bir felaket, kriz veya kesinti yaşanması durumunda iş sürekliliğinin aksamaması amacı ile farklı bir risk bölgesinde yer alan bir felaket kurtarma merkezi kurar veya yurtiçinde farklı bir risk bölgesinde felaket kurtarma merkezi hizmeti veren firmalardan hizmet alır.

(2) İşletme, FKM kurulumu sürecinde Ek-12'de yer alan Felaket Kurtarma Merkezi Kurulumu Rehberine uygun bir şekilde hareket eder.

(3) İşletmeler, veri merkezlerinin ve felaket kurtarma merkezlerinin yerlerini seçerken doğal riskleri ve çevresel tehditleri göz önünde bulundurur. Binaların, barındırdıkları bilgi işlem tesislerinin varlığını açık edecek işaretler ve bilgiler bulundurmamasını sağlar.

(4) İşletme, veri merkezlerinin çalışmasını olumsuz etkileyebilecek elektrik kesintisi, yangın, duman, sıcaklık, su, toz ve nem gibi çevresel koşulları izleyecek sistem ve sensörler kullanır, bunların bakımlarını düzenli olarak yapar. Bu destek sistemi ve sensörlerin ilgili veri merkezlerinin bütünüyle devre dışı kalmalarına neden olabilecek tek bir arıza noktası içermemesi sağlanır.

Siber Güvenlik Tehdit İstihbaratı Toplama ve Değerlendirme Görevi

MADDE 53 -(1) 1. Grup havacılık sektörü işletmelerinde; Kurumsal SOME, işletmenin siber güvenliğini tehdit eden mevcut ve potansiyel saldırılar hakkında bilgilerin toplanacağı ve analiz edileceği bir siber istihbarat toplama ve değerlendirme süreci oluşturur ve yürütür.

Siber Olay İzleme ve Tespit Etme Görevi

MADDE 54 -(1) Kurumsal SOME; Ek-3'de yer alan Kurumsal SOME Kurulum ve Yönetim Rehberi'nde bulunan "Olay Sonrasında İncelenmek Üzere Güvenilir Delillerin Elde Edilmesi İçin Tutulacak Kayıtların Asgari Nitelikleri" dokümanına uygun olarak, iz kayıtlarının merkezi bir şekilde tutar ve yönetir. Görevler ayrılığı prensibi çerçevesinde, merkezi iz kayıt sistemi yönetilerek korale edilir ve bu işlem iz kayıtlarını üreten bilişim sistemlerinin sorumlularından bağımsız olarak yapılır.

(2) İz kayıtlarının yönetimi; iz kayıtlarının üretilmesi, transfer edilmesi, depolanması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi aşamalarını kapsar. Bu süreçlerde sistem, veri tabanı, ağ ve güvenlik yöneticileri, Kurumsal SOME personeli, yazılım geliştiriciler ve denetçilere ait görev ve

sorumluluklar görevlerin ayrılığı ilkesi kapsamında belirlenir.

(3) Kurumsal SOME, iz kayıtlarını ve oluşan alarmları günlük olarak izler ve incelemesini yaparak inceleme sonuçlarını dokümante eder.

(4) Kurumsal SOME, iz kayıtları üzerinde aylık analiz ve ilişkilendirme çalışması yapar; çalışma sonucunda oluşturduğu raporu Kurumsal SOME Yöneticisine sunar.

(5) Kurumsal SOME, aylık olarak yaptığı iz kayıt analiz ve ilişkilendirme çalışmasında olağan dışı herhangi bir duruma rastlarsa, bu konuda düzeltici veya önleyici aksiyon alır.

MADDE 55 -(1) Siber olaylara ilişkin tutulan iz kayıtlarına, "bilinmesi gerektiği kadar" prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşması sağlanır.

(2) Kayıt üreten ortamların teknolojisine uygun olarak kimlik doğrulama ve yetkilendirme sistemleri yapılandırılır.

(3) Kayıt üreten ortamlarla iz kayıtları saklama merkezleri arasında teknik imkanlar dahilinde verinin şifreli olarak transfer edilmesi sağlanır.

(4) İz kayıtlarının tek yönlü kriptografik özet değerleri hesaplatılır ve iz kayıtları güvenli ortamlarda saklanır.

(5) Merkezi iz kaydı sunucuları bt ve ot sistemlerinden ayrık bir yapıda oluşturulur.

(6) Merkezi iz kaydı sunucusunun kayıtları, olayların olduğu sistem dışında merkezi bir sunucuda saklanır.

(7) İşletme kritik olaylarını belirler. Kritik olayların iz kayıtları merkezi sunucuya anlık olarak gönderilir, kritik olarak değerlendirilmeyen olayların iz kayıtları da işletmenin belirlediği aralıklarda merkezi sunucuya iletilir.

(8) Kritik sistemlerde oluşan iz kayıtları eş zamanlı olarak merkezi sunucularda yedeklenir, silinmelerine ve değiştirilmelerine izin verilmez.

(9) Merkezi iz kaydı sunucuları sadece yeni iz kayıtlarının saklanması için fonksiyonlar içerir, iz kayıtlarının silinmesi veya değiştirilmesi amaçlı erişimlere kapalı olur.

(10) İz kayıtları periyodik olarak yedeklenir ve yedekler uygun şekilde muhafaza edilir.

MADDE 56 -(1) İz kayıtlarının saklanma süresi belirlenmesinde; iz kayıtlarından sağlanacak fayda ve ilgili iz kaydının kritikliği parametreleri göz önünde bulundurulur. İşletmelerin tabi oldukları yasal mevzuatları gereği uyması gereken süreler saklıdır.

MADDE 57 -(1) Kayıtların toplandığı bütün sistemlerin aynı zaman değerine sahip olması sağlanır. Bütün sistemlerin zamanlarının aynı yapılması işlemi için Ağ Zaman Protokolü sunucusu kurulup kayıt üreten farklı sistemlerin zamanlarını bu sunucu ile senkronize etmesi sağlanır. Bunun yanında farklı ülkelerde birimleri olan işletmeler için saat dilimi de dikkate alınır.

MADDE 58 -(1) 1.grup havacılık sektörü işletmelerinde, Kurumsal SOME, işletme siber güvenlik durumsal farkındalığını sağlamak amacıyla 7x24 prensibine uygun bir tespit ve müdahale mekanizması kurar veya kurdurur.

(2) 2.grup havacılık sektörü işletmelerinde, Kurumsal SOME, işletme siber güvenlik durumsal farkındalığını sağlamak amacıyla 7x24 prensibine uygun tespit mekanizması kurar veya kurdurur.

MADDE 59 -(1) 1. grup havacılık sektörü işletmeleri, tehdit avcılığı ve balküpü mekanizmalarını kurar veya kurdurur.

MADDE 60 -(1) 1. grup havacılık sektörü işletmelerinde Kurumsal SOME, kullanıcı ve network bazında anomali tespit sistemlerini kurar ve işletir.

Siber Olay Müdahale ve Yönetimi Görevi

MADDE 61 -(1) İşletme bünyesinde yaşanabilecek bir siber olay ihlal durumuna karşın, Kurumsal SOME siber olay ihlal durumlarını önceden belirler, olay müdahale senaryolarını oluşturur ve dokümante eder.

(2) Kurumsal SOME, siber güvenlik saldırı eğilimlerini takip eder ve siber olay müdahale süreçlerini ve dokümanlarını güncel tutar.

(3) Kurumsal SOME, işletmenin olası bir siber olay durumunda faaliyetlerinin en az etkilenmesini ve mümkün olan en kısa sürede hizmetlerin normal işleyişine döndürülmesini sağlayacak bir siber olay müdahale süreci yürütür.

(4) Kurumsal SOME, gerçekleşen siber olaylar için bir kök neden ve etki analizi yapar ve benzer olayların tekrarlanmasını önlemek için iyileştirici önlemler alır ve dokümante eder.

MADDE 62 -(1) Olası bir siber güvenlik ihlal durumunda olay yönetim sürecini Kurumsal SOME Yöneticisi yönetir.

MADDE 63 -(1) İşletme aşağıda belirtilen durumlarda SHGM'yi ivedilikle bilgilendirir.

a) Yaşanan bir siber olayın büyüyerek bir krize dönüşmesi,

b) Kritik verilerin ya da kişisel verilerin sızması ya da ifşası ile sonuçlanması,

c) Kritik bilgi teknolojileri varlıklarının gizliliğinin etkilenmesi,

ç) Kritik bilgi teknolojileri varlıklarının bütünlüğünün etkilenmesi,

d) Kritik bilgi teknolojileri varlıklarının erişilebilirliğinin etkilenmesi,

e) Bilgi Sistemleri İş Sürekliliği Planı'nın devreye alınması,

f) FKM sistemlerinin devreye alınması

(2) Madde 64.1'de bahsedilen siber güvenlik ihlallerinin olması durumunda işletme, ivedilikle yaşanan siber güvenlik olayı hakkında bir adli bilişim çalışması yürütür ve olay kök neden analizi yapar.

(3) İşletme, yapılan çalışma sonucunda söz konusu olayın bir daha tekrarlanmaması adına alınması gereken önlemleri de belirleyerek SHGM'ye siber olay gerçekleşme tarihinden itibaren en geç 10 iş günü içerisinde Ek-13'de yer alan formata uygun siber olay analiz raporunu gizli resmi yazı ile sunar.

(4) İşletme, madde 64.1 dışında kalan siber güvenlik olaylarını ve teşebbüslerini dokümante eder ve Ek-14'de bulunan form ile çeyrek bazında SHGM'yi bilgilendirir.

Siber Güvenlik Test ve Denetleme Görevi

MADDE 64 -(1) Bilişim sistemleri güvenlik testleri Ek-15'de belirtilen şekilde gerçekleştirir.

MADDE 65 -(1) Kurumsal SOME, yılda en az bir defa TSE onaylı sızma testi firmalarına Ek-16'da yer alan TSE Sızma Test Metodolojisine uygun bir şekilde geniş kapsamlı sızma testlerini yaptırır.

(2) Geniş Kapsamlı sızma testleri en az Ek-17'de yer alan Geniş Kapsamlı Sızma Testi Kapsam Dokümanı içeriğine uygun bir şekilde gerçekleştirilir.

(3) Kurumsal SOME'nin yılda en az bir kez TSE tarafından belgelendirilmiş onaylı sızma testi firmalarına yaptırması gereken geniş kapsamlı sızma testleri iki sene üst üste aynı kişiler tarafından gerçekleştirilemez.

(4) Kurumsal SOME, geniş kapsamlı sızma testlerini yaptırdığı firma ve bu testlerde görev alan firma personelleri ile gizlilik sözleşmesi imzalar.

(5) İşletme, Kurumsal SOME fonksiyonlarını icra etmek için hizmet aldığı kuruluşlara ve o

kuruluşların hisse sahibi olduğu diğer kuruluşlara hizmet alımı süresince Geniş Kapsamlı Sızma Testi yaptıramaz.

MADDE 66 -(1) Kurumsal SOME, dar kapsamlı sızma testi kapsamında; en az 6 ayda bir test ve denetimleri yapar veya yaptırır.

(2) Dar kapsamlı sızma testi aşağıdaki hususları içerir.

a) İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması,

b) Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması,

c) Dışa açık web uygulamalarının sızma testleri,

ç) Etki alanı ve son kullanıcı bilgisayarları yapılandırma testleri ayarları,

d) Veri tabanı yapılandırma testleri ayarları.

(3) Kurumsal SOME, işletmenin bilgi işlem altyapısında köklü bir değişiklik olması durumunda 6 aylık süreyi beklemeden dar kapsamlı sızma testini yapar veya yaptırır.

MADDE 67 -(1) Kurumsal SOME, dar ve geniş kapsamlı sızma testleri sonrasında tespit edilen zafiyetler kapatıldıktan sonra doğrulama testlerini yapar veya yaptırır. Zafiyetin kapatıldığının doğrulaması zafiyeti kapatan kişi tarafından yapılamaz.

MADDE 68 -(1) Kurumsal SOME, işletme personeli veya hizmet alımı yoluyla temin edilen, üretilen, güncellenen yazılımların kullanıma geçmeden önce yazılımın siber güvenliği ile ilgili testleri yapar veya yaptırır ve bu test sonuçlarını dokümante eder.

(2) Kurumsal SOME, iç veya dış kaynaklar ile geliştirilen veya güncellenen yazılımların siber güvenlik testlerinin yapılması veya yaptırılması sürecinde Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Geliştirme Rehberini kullanır.

MADDE 69 -(1) 1. grup havacılık sektörü işletmeleri en az 2 senede bir kez olmak üzere işletme bünyelerinde yer alan EKS ve SCADA sistemlerinin sızma testini yaptırır.

MADDE 70 -(1) Kurumsal SOME, ISO 27001 kapsamında yapılması gereken siber güvenlik iç tetkik süreçlerini yürütür.

MADDE 71 -(1) Kurumsal SOME, işletme BT ve OT süreçlerinin gizlilik, bütünlük ve erişilebilirlik unsurlarının güvenlik seviyesini arttırmak, sürdürülebilir bir siber güvenlik operasyon süreci oluşturmak ve mevcut siber güvenlik ekosisteminde aksayan noktaları zamanında tespit ederek, gerekli düzeltici eylemleri zamanında uygulamak amacıyla sürekli bir kırmızı takım siber güvenlik denetim süreci kurgular ve uygular.

MADDE 72 -(1) Kurumsal SOME, işletmenin iç veya dış ağlardan gelebilecek siber güvenlik tehditlerinden korunması için proaktif yapıda ağ kontrol ve güvenlik sistemlerini tesis etmesini sağlar ve denetler. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisini esas alır.

(2) Hassas verilere sahip tüm sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanır. DMZ sistemleri, özel iç ağdaki sistemlerle yalnızca vekil uygulamalar veya güvenlik duvarı cihazları üzerinden iletişim kurar.

(3) İnternet üzerinden veya işletme dış ağından görünür olan tüm sunucu ve sistemler, görünür olmalarını gerektirecek geçerli bir iş ihtiyacının olup olmadığı açısından düzenli olarak kontrol edilir ve eğer gerekli değilse bu sunucu ve sistemlerin işletme iç ağına taşınır.

(4) İşletme, dış ağı ve iç ağı arasındaki trafiği kontrol altında tutmak için gerektiği şekilde

konfigürasyonu yapılmış ve sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıları tespit edebilecek ve önleyebilecek günün teknolojisine uygun sistemler kullanır.

(5) İç ağdan gelebilecek tehditlerin etkisini azaltmak ve işletme iç ağının farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere işletme iç ağındaki her bir servise ilişkin trafiğin yalnızca kendisi için gerekli olan ağ segmentlerine ulaşmasını sağlayacak şekilde kurum iç ağına kritiklik ve görev bazında ağ segmentasyonu uygulanır. Farklı ağ segmentleri arasındaki hassas veri trafiği kontrol edilir ve güvenliği sağlanır.

(6) İç ağa sadece yetkilendirilmiş cihazların erişebilmesi sağlanır. Dış hizmet alım yöntemi ile icra edilen havacılık ve bilgi teknolojileri operasyonlarının yürütülmesi de bu madde kapsamında değerlendirilir.

(7) EKS ve Scada sistemleri BT networkünden ayrılır.

(8) EKS ve Scada sistemlerine kritiklik veya görev bazlı bir ağ segmentasyonu uygulanır.

MADDE 73 -(1) Kritik ağ segmentlerine yapılan tüm bağlantılar sürekli olarak izlenerek bu bağlantıların her biri için gereksinim değerlendirmesi yapılır ve gereksiz tüm bağlantıların sonlandırılması sağlanır. Benzer şekilde, ağa bağlı her bir sistem üzerindeki portların, protokol ve servislerin sadece gerekliliği onaylanmış iş ihtiyaçlarına istinaden açık ve çalışıyor olması sağlanır. Bu doğrultuda, güvenli bir baz konfigürasyonu temel alarak önemli tüm sunucu ve sistemler için düzenli olarak port taraması gerçekleştirilir ve güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portlar kapatılır.

MADDE 74 -(1) Kurumsal SOME, tüm masaüstü, dizüstü, mobil cihazlar, iş istasyonu makineleri ve sunucuları üzerindeki işletim sistemi, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi tüm kritik bilgi teknolojileri varlıkları için sıkılaştırılmış ve test edilmiş güvenli standart yapılandırma bilgilerini oluşturur ve dokümante eder.

MADDE 75 -(1) Kurumsal SOME, tüm masaüstü, dizüstü ve iş istasyonu makineleri ile sunucularını, sürekli bir şekilde izleyerek üzerindeki zararlı yazılımları tespit edecek etkin araçlar kullanır.

MADDE 76 -(1) Kurumsal SOME, bilginin gizliliği, aslına uygunluğu ve bütünlüğünün korunması için kriptografinin doğru ve etkin kullanımın temin edildiğini denetler.

MADDE 77 -(1) Kurumsal SOME, yaptığı veya yaptırdığı tüm sistem test ve denetim faaliyetleri sonrasında kurumsal siber güvenlik değerlendirme ve risk analizi raporunda gerekli güncellemeleri yapar.

MADDE 78 -(1) Kurumsal SOME, tüm sistem test ve denetim faaliyetleri sonrasında tespit edilen zafiyetlerin ilgili bilgi işlem personeli veya hizmet alınan firma tarafından kapatılması sürecini yönetmek üzere dokümante edilmiş bir bulgu yönetim süreci tesis eder.

(2) Kurumsal SOME tarafından oluşturulmuş siber güvenlik bulgu yönetim süreci aşağıdaki unsurları içerir:

a) Bulgu No,

b) Bulgu Açıklama,

c) Bulgu Tespit Edilme Yöntemi,

ç) Bulgu Tespit Edilme Tarihi,

d) Bulgunun İlgili Birime Bildirilme Tarihi,

e) Zafiyet Sonucu Etkilenmesi Muhtemel Sistem veya Süreçler,

f) Bulgu Kök Neden,
g) Bulgunun İlişkilendirildiği Siber Güvenlik Risk No,
ğ) Bulguyla İlgili Oluşturulan Siber Güvenlik Risk No,
h) Varlık veya Süreç Sahibi Birim,
ı) Kapatmak İçin Alınacak Aksiyonlar,
i) Bulgu Kapatma Son Tarihi,
j) Bulgu Kapatma Aksiyonunu Gerçekleştirecek Kişi veya Birim,
k) Bulgu Takibini Gerçekleştiren Kurumsal SOME Personeli,
l) Bulgu Son Durum Açıklama

MADDE 79 -(1) Kurumsal SOME, yapılan siber güvenlik testleri sonucunda suç olabilecek iz, delil ve emare (zararlı yazılım, sızma vb.) görülmesi durumunda Kurumsal SOME Yöneticisi ve işletmenin hukuk müşavirliği ile görüşerek gecikmeksizin kanunen soruşturmaya yetkili makamlara (savcılık veya kolluk), SHGM'ye ve USOM'a bildirimde bulunur.

İç ve Dış Paydaşlarla İletişim Görevi

MADDE 80 -(1) Kurumsal SOME, bir prosedür veya talimatta Kurumsal SOME'lerin kurum içi ve dışı paydaşlar ile iletişim esaslarını oluşturur.

(2) Kurumsal SOME; siber olay öncesi, esnası ve sonrasında, siber güvenlik çalışmalarını yönetmek amacıyla kurumdaki bilgi işlem birimi ve varsa hukuk ve basın ve halkla ilişkiler müşavirlikleri ve benzeri birimler ile birlikte çalışır.

MADDE 81 -(1) İşletme dış paydaşlar ile gerçekleştireceği siber güvenlik ile alakalı ihlal olayı, istihbarat ve bilgi paylaşımlarında trafik ışığı protokolü esasına göre bir sınıflama yapar.

(2) SHGM ile yapılan veri paylaşımlarında işletmenin trafik ışığı protokolüne göre olan tercihi değerlendirilmeye alınır. SHGM gerekli gördüğü hallerde söz konusu bu sınıflandırmayı göz ardı edebilir.

MADDE 82 -(1) Kurumsal SOME, tüm Kurumsal SOME personelinin iletişim bilgilerini USOM ve SHGM'ye SİP uygulaması üzerinden bildirmek ve güncel tutmak ile yükümlüdür.

(2) Kurumsal SOME, yıllık Siber Güvenlik Faaliyet Raporlarını Ek-18'de yer alan Yıllık Siber Güvenlik Faaliyet Raporu Formatına uygun bir şekilde hazırlayarak SHGM'ye en geç izleyen yılın 31 Ocak tarihine kadar eksiksiz bir şekilde gönderir.

DÖRDÜNCÜ BÖLÜM
Diğer Hükümler

Yasal Uyum

MADDE 83 -(1) İşletme kendisini siber güvenlik alanında etkileyen tüm yasal mevzuat ve sözleşmeden doğan şartlarını değerlendirir mevcut süreç ile karşılaştırarak dokümante eder.

(2) 1. ve 2. grup havacılık sektörü işletmeleri, Ek-3'de yer alan Kurumsal SOME Kurulum ve Yönetim Rehberi'nde belirtilen gereksinimlere uyar.

(3) Havacılık sektörü işletmeleri, Cumhurbaşkanlığı Dönüşüm Ofisi Tarafından hazırlanan Ek-8'de bulunan Bilgi ve İletişim Güvenliği Rehberine uyum sağlamakla yükümlüdür.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Uyumluluğu

MADDE 84 -(1) 1. ve 2. grup havacılık sektörü işletmeleri İşletme bilgi teknolojileri

varlıkları, operasyonel teknoloji varlıkları ve havacılık sistemlerini etkileyen tüm süreçlerini ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı kapsamında belgelendirir.

İç Denetim

MADDE 85 -(1) İşletme, siber güvenlik faaliyetlerinin yeterliliğini ve siber direncini ölçmek için görevler ayrılığı ilkesini gözeterek senede en az 1 defa olmak üzere Ek-19'da yer alan Havacılık Sektörü Siber Güvenlik İç Kontrol Metodolojisini kullanarak iç denetim faaliyeti gerçekleştirir.

Yönetim Gözden Geçirme

MADDE 86 -(1) İşletme, siber güvenlik faaliyetlerinin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek için en az senede bir olmak üzere Genel Müdür veya Yönetim Kurulu Başkanı başkanlığında ve tüm BGYS paydaşlarının katılım sağlayacağı bir gözden geçirme toplantısı düzenler.

(2) Yönetim Gözden Geçirme toplantıları aşağıdaki hususları kapsar.

a) Önceki yönetimin gözden geçirme toplantılarında belirlenmiş görevlerin durumu,

b) Kurumsal SOME görev ve sorumluluklarını ilgilendiren iç ve dış konulardaki değişiklikler,

c) En az aşağıdaki hususları kapsayacak şekilde işletme siber güvenlik faaliyetleri performansına dair geri bildirim:

1) Uygunsuzluklar ve düzeltici faaliyetler,

2) İzleme ve ölçme sonuçları,

3) İç ve dış kaynaklı tüm tetkik ve denetim sonuçları ve

4) Siber güvenlik Stratejik Plan hedeflerinin durumu,

ç) İç ve dış paydaşların siber güvenlik süreçleri ile ilgili geri bildirimleri,

d) Siber güvenlik risk değerlendirme sonuçları ve risk işleme planının durumu ve sürekli iyileştirme için fırsatlar,

e) Ek-19'da yer alan Havacılık Sektörü Siber Güvenlik İç Kontrol Metodolojisine göre yapılmış değerlendirme sonuçlarının analizi.

(3) Tüm toplantı katılımcılarının ıslak imzasını içeren yönetim gözden geçirme toplantısı sonuç tutanağı, toplantının bitiminden itibaren en geç 5 iş günü içerisinde gizli resmi yazı ile SHGM'ye gönderilir.

Yerli Milli Ürün Kullanımı

MADDE 87 -(1) İşletme bilgi teknolojileri süreçlerinde dışa bağımlılığın ve dışa bağımlılığın oluşturabileceği siber risklerin azaltılması amacıyla yerli-milli ürün kullanımına önem verir.

BEŞİNCİ BÖLÜM
Cezai Yaptırımlar

MADDE 88 -(1) 1. ve 2. Grup havacılık sektörü işletmeleri SHGM tarafından haberli veya habersiz olarak denetlenir. Yapılan siber güvenlik denetimleri sonucunda;

a) Tespit edilen bulgular, SHGM tarafından belirlenen bulgu kapatma sürelerine uygun bir şekilde kapatılması için işletmeye bildirilir.

b) SHGM tarafından uygun görülen tarihte eksiliklerin giderilmemiş olması durumunda ilgili işletmeden savunma talep edilir. Söz konusu savunmanın incelenmesi ve SHGM tarafından yeterli görülmemesi durumunda SHGM, ilgili işletmeye 2920 sayılı Türk Sivil Havacılık Kanunu'nun 143 üncü maddesi gereği Sivil Havacılık Genel Müdürlüğü Tarafından Verilecek İdari Para Cezaları Hakkında Yönetmelik (SHY-İPC) hükümlerine göre idari para cezası uygular.

c) Tespit edilen eksikliklerin önemi göz önüne alınarak bu maddede belirlenen adımlardan bir veya daha fazlası Genel Müdür onayı ile atlanabilir.

(2) SHGM tarafından yapılan inceleme ve denetlemelerde adli soruşturmaya konu olabilecek hususlara rastlanılması durumunda adli makamlara suç duyurusunda bulunulur.

ALTINCI BÖLÜM
Son Hükümler

Yürürlükten Kaldırılan Genelge

MADDE 89 -(1) 02/08/2016 tarihli Genel Müdürlüğümüz HGD/2015-1 Genelgesi 31.12.2022 tarihinde yürürlükten kalkacaktır.

Yürürlük

MADDE 90 -(1) Bu talimat 01.01.2023 tarihinde yürürlüğe girer.

Yürütme

MADDE 91 -(1) Bu Talimat hükümlerini Sivil Havacılık Genel Müdürü yürütür.

EKLER:

EK-01 - ATM Güvenlik Planı Kapsamı
EK-02 - ATM Güvenlik Planı Kontrol Formu
EK-03 - Kurumsal SOME Kurulum ve Yönetim Rehberi
EK-04 - Siber Güvenlikten Sorumlu Yönetici Başvuru Formu (Form-4)
EK-05 - SGSYY Siber Güvenlik Sertifikası Kabul Listesi
EK-06 - Siber Güvenlik Strateji Planı Durum Bildirim Formu
EK-07 - Kurumsal SOME Eğitim Listesi
EK-08 - Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi
EK-09 - Siber Güvenlik Kritik Tedarikçi Envanteri
EK-10 - Havacılık Sektörü Güvenli Yazılım Geliştirme Rehberi
EK-11 - BT Süreçleri İş Sürekliliği Planı
EK-12 - Felaket Kurtarma Merkezi Kurulumu Rehberi
EK-13 - Siber Olay Analiz Formatı
EK-14 - Siber Olay İstatistiksel Bildirim Formu
EK-15 - Bilişim Sistemleri Güvenlik Test Süreci
EK-16 - TSE Sızma Test Metodolojisi
EK-17 - Geniş Kapsamlı Sızma Testi Kapsam Dokümanı
EK-18 - Yıllık Siber Güvenlik Faaliyet Raporu Formatı
EK-19 - Havacılık Sektörü Siber Güvenlik İç Kontrol Metodolojisi