Doküman Dağıtımı ve Sahipliği

Bilgi Güvenliği Yönetiminden sorumlu BGYS Komitesi ekip üyesi, bu politikayı intranette veya e-posta üzerinden güvenli bir şekilde yayınlamak suretiyle, ASG ve iştiraklerine dağıtımını sağlayacaktır.

Politikanın ASG ve iştirakleri için tüm çalışanlara ve yüklenicilere elektronik veya basılı olarak sunulmasını sağlamak için Ülke BT başkanları ve İK başkanları ile birlikte çalışacak Bilgi Güvenliği Görevlileri atanmıştır.

Doküman Sözleşmesi

Bu belgedeki tüm ifadelerin zorunlu gereklilikler olduğu ve bunlardan sapmanın, istisna yönetimi süreci aracılığıyla onaylanmadıkça uyumsuzluk olarak kabul edileceğine dikkat edilmelidir.

DOKÜMAN DEĞİŞİKLİK TARİHÇESİ

Versiyon	Dokumanı Yazan	Ünvanı	Yapılan Değişikliklerin Açıklaması	Tamamlanma Tarihi
1.0		*Kalite Sorumlusu*	*İlk Yayın*	

DOKÜMAN ONAY MEKANİZMASI

	İsim	*Ünvanı*	*Tarih*	*İmza*
Hazırlayan		*Kalite Sorumlusu*		
Gözden Geçiren				
Onaylayanlar				

1. Amaç

Bu politika, yönetimin ASG ve iştiraklerine (bundan böyle "kuruluş" olarak anılacaktır) yönelik tutum yönergesini özetlemektedir. Ayrıca "ASG", Bilgi Güvenliği Yönetim Sistemi (BGYS) – ISO/IEC 27001:2022 Standardı doğrultusunda, bilgi güvenliği politikaları, ilgili prosedürler, ASG'nın görev ve sorumlulukları ile ilgili zorunlulukları ve en iyi uygulamaları da bünyesinde barındırmaktadır. Devralınan politika, ilgili onaylarla ülke düzeyinde geçerli yasal ve düzenleyici uyumlulukların karşılanması nedeniyle değiştirilebilir.

2. Kapsam

Bu politika ASG genelinde geçerlidir ve aşağıdakiler için geçerlidir:

ASG bilgilerine ve teknolojilerine erişimi olan tüm bireyler ASG'nın bilgilerini işlemek için kullanılan tüm tesisler, teknolojiler ve hizmetler ASG'nın operasyonel faaliyetleri kapsamında işlediği her türlü bilgiyi, ASG'nın bilgilerini işlemek için kullanılan iç ve dış süreçler ve ASG İştiraklerine bilgi işlem hizmeti veren ve yukarıda sayılmayan dış taraflar referans olarak kullanabilir

3. Bilgi Güvenliği İlkeleri

Bilgi güvenliği, bilgi kaynaklarını yetkisiz erişime veya zarara karşı koruma ve finansal kayıplar, itibar zedelenmesi ve düzenleyici sorunlar riskini azaltma uygulamasıdır. İzlenen temel ilkeler şunlardır:

a) Gizlilik:

Bilgilere erişme veya bilgileri değiştirme yeteneği, yalnızca yetkili amaçlar için yetkili kullanıcılara sağlanır.

b) Bütünlük:

Sağlık hizmetleri veya yönetimi sırasında kullanılan bilgilerin, temsil ettiği gerçeği doğru bir şekilde yansıtacağına güvenilebilir.

c) Erişilebilirlik:

ASG'nin bilgi kaynakları, ağ, donanım, yazılım, tesisler, altyapı ve diğer tüm kaynaklar dahil olmak üzere, sağlık hizmetlerini desteklemek veya atanmış oldukları idari görevleri yerine getirmek için kullanılabilir.

4. Genel Bakış

4.1. Bu Politikanın Yapısı

- ASG, artan siber tehditleri göz önünde bulundurarak ISO/IEC 27001:2022 standardına uyum sağlayan bir yaklaşım benimsemiştir.
- Bu politikanın yapısı, Bilgi Güvenliği Yönetim Sistemleri için ISO/IEC 27001:2022 standardının yapısına uygun olarak hazırlanmıştır.
- Bu politikanın 1'den 4'e kadar olan bölümleri, amacını, kapsamını, Bilgi Güvenliği ilkelerini ve Genel Bakış'ı tanımlar.
- Bu politikanın 5. Bölüm ile 8. Bölüm, standartta aşağıdaki kategoriler altında belirtilen etki alanlarını ve kontrolleri ele almaktadır
    1. Organizasyonel Kontroller
    2. İnsan Kontrolleri
    3. Fiziksel Kontroller

4. Teknolojik Kontroller

4.2. Sahiplik ve Yönetim

Bilgi güvenliği politikası, işletim ortamında, teknolojilerde, sektördeki en iyi uygulamalarda, yasal ve düzenleyici gereksinimlerde veya iç/dış denetçilerin önerilerinde önemli değişiklikler olduğunda uyumunu sağlamak için yıllık bir gözden geçirme sürecinden geçecektir.

Kuruluşun bilgi güvenliği politikalarının sürekli ihlali durumunda, ihlal eden kişi(ler), bu politikada belirtilen ASG'nın disiplin sürecine uygun olarak uygun disiplin cezasına tabi tutulacaktır.

4.3. İstisna Yönetimi

Bu politika ile uyumun teknik veya ticari olarak uygulanabilir olmadığı durumlarda, süre sınırlı bir istisna talep edilmelidir. İstisnalar, geçerli onaylara tabi olarak ve ASG **İstisna Yönetimi Kılavuzu**'nda tanımlanan izin verilen süre için gündeme getirilecektir.

Onaylanan tüm istisnalar, periyodik olarak veya önemli değişiklikler meydana geldiğinde, devam eden uygunluk ve etkinliklerini sağlamak için düzenli olarak gözden geçirilecektir. Herhangi bir istisna talep etmek ve onaylamak için lütfen istisna yönetimi kılavuz belgesini izleyin.

İstisna Yönetimi Kılavuzu'na başvurun.

5. Organizasyonel Kontroller

Bu bölüm, ASG tarafından ISO 27001:2022 ile uyumlu olarak benimsenen organizasyonel kontrolü tanımlar. İlk versiyondan sonraki bu bölümdeki kontrollerde yapılan herhangi bir değişiklik, aşağıdaki tabloda ve ilgili yürürlük tarihleriyle birlikte belgelenecektir.

Versiyon	İlgili Kontrol	Geçerlilik Tarihi	Değişiklikler
1.0	NA	NA	İlk Versiyon

5.1. Bilgi Güvenliği için Politikalar

a. Bu politika, ASG Yönetiminin, organizasyonun bilgi varlıklarını tespit edip güvence altına alma niyetini vurgular. Bu, düzenlemelere uygun, önde gelen uygulamaları ve iş ihtiyaçlarını karşılayan, yetkisiz kullanım, ifşa veya tahribattan koruyan bir şekilde gerçekleştirilir.

b. ASG'deki bilgi güvenliği yönetim sistemi, ayrıntılı bilgi güvenliği politikaları, prosedürler, çerçeve ve kılavuzlar ile desteklenir. Bilgi güvenliği prosedürleri, politika beyanlarından türetilir ve hedeflere ulaşmak için gerekli eylemlerin ayrıntılarını sağlar.

c. Bilgi güvenliği politikalarının sahipliği Bilgi güvenliği komitesi' ne aittir. Bu politikanın içeriği hakkında herhangi bir soru, iyileştirme önerileri durumunda BGYS Komitesi ile iletişime geçilmelidir.

d. ASG'nin bilgi güvenliği politika beyanı şöyledir:

"ASG, bilgi varlıklarını tüm belirlenen bilgi ve siber güvenlik tehditlerinden, kasıtlı veya kazara, korumayı taahhüt eder. Bu, bilginin gizliliğinin korunmasını; bilginin bütünlüğüne güvenilmesini;

bilginin erişilebilirliğinin sağlanmasını; yasal, düzenleyici, yasal ve sözleşmeye dayalı yükümlülüklerin karşılanmasını ve organizasyon çapında Bilgi Güvenliği Yönetim Sistemi'ne sürekli iyileştirme sağlanmasını içerir."

5.2. Bilgi Güvenliği Rolleri ve Sorumlulukları

Bilgi güvenliği rollerinin ve sorumluluklarının, bireylerin rollerin önemini anlamasını sağlamak amacıyla her seviyede tanımlanması ve atanması gerekmektedir. ASG'deki BGYS yönetimi için roller, sorumluluklar ve yetkiler Bilgi Güvenliği Yönetim Çerçevesi'nden öğrenilebilir. Bu çerçeve, aşağıdakileri daha ayrıntılı olarak açıklar:

e. ASG'deki bilgi güvenliği organizasyon yapısı, başkanlık gruplarını tanıtma.

f. ASG'deki ISMS yetkilendirme seviyeleri.

Bilgi Güvenliği Yönetim Çerçevesi 'ne başvurun.

5.3. Görevlerin Ayrılığı

Kullanıcıların görevleri ve çelişen sorumluluk alanları, bilgi varlıklarının yetkisiz veya kasıtsız olarak değiştirilmesi veya kötüye kullanılması fırsatlarını azaltmak için uygun şekilde ayrılmalıdır. Fonksiyon başkanı, görev ayrımı matrisinin kendi fonksiyonları tarafından korunmasını ve yetkili personel tarafından düzenli aralıklarla gözden geçirilmesini sağlamalıdır.

5.4. Yönetim Sorumlulukları

ASG yönetimi, tüm çalışanların ve üçüncü tarafların, kuruluşun belirlediği bilgi güvenliği politikalarına, prosedürlerine ve kılavuzlarına uymasını sağlayacaktır. ASG Yönetimi, yasal, operasyonel ve sözleşmeye dayalı gereksinimlerin yerine getirilmesini sağlamak amacıyla tüm fiziksel ve elektronik bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı taahhüt eder. Aşağıda belirtilenler amaçlardır:

g. ASG'nin bilgi varlıklarını ve diğer zarar ve kayıpları korumak için kontroller oluşturmak.

h. ASG bilgilerini işleyen paydaşlar arasında, organizasyon içinde uygun bir düzeyde bilgi güvenliği farkındalığını, bilgisini ve becerisini sürdürerek güvenlik olayları riskini en aza indirmek.

i. ASG'nin, büyük güvenlik olayları sırasında iş hizmetlerini sürdürmesini sağlamak.

j. Hastaların ve çalışanların sağlık bilgileri de dahil olmak üzere kişisel bilgilerin korunmasını sağlamak (veri gizliliği). Gizlilik uyum yükümlülükleri için yerel gizlilik yasalarına ve ilgili politikalara başvurun

k. ASG tarafından sağlanan ve işletilen ağ altyapısının ve hizmetlerin erişilebilirliğini ve güvenilirliğini sağlamak.

l. Dış hizmet sağlayıcıların gereksinimlere uygunluğunu sağlamak.

m. Bilgi sistemlerine uzaktan erişimde esneklik ve kabul edilebilir bir güvenlik düzeyini sağlamak.

n. Güvenlik kontrollerinin hasta ve iç kullanıcı deneyimi üzerindeki etkisini dikkate almak ve dengelemek

5.5. Otoritelerle İletişim

Uygun iletişimler, kolluk kuvvetleri, düzenleyici kurumlar, üçüncü taraf satıcılar, donanım satıcıları ve yazılım satıcıları ile kurulacaktır.

Tesis yönetimi, itfaiye ve acil servisler dahil ancak bunlarla sınırlı olmamak üzere yetkililerle iletişimi sürdürmelidir. Bu kurumların iletişim bilgileri korunmalı ve belirgin yerlere yerleştirilmelidir

5.6. Özel İlgi Gruplarıyla İletişim

İlgili bölümler, bilgi güvenliği ve veri gizliliğine adanmış özel ilgi grupları ve yetkili forumlarla etkili iletişim kanalları kurmalı ve sürdürmelidir. Bu, yeni açıklar, güvenlik ve süreklilik tehditleri, düzenlemeler ve risklerle ilgili güncellemelerin zamanında alınmasını ve dağıtılmasını sağlar.

Bilgi güvenliği alanındaki en son gelişmeler hakkında bağlantıda kalmak ve bilgilendirilmek için CERT gibi tanınmış özel ilgi gruplarıyla iletişim kurmak ve sürdürmek hayati önem taşır.

5.7. Tehdit İstihbaratı

ASG, kuruluşa yönelik güvenlik tehdit istihbaratını toplayacak ve analiz edecek, bu sayede tehditlerin gerçekleşmesini önlemek için eylemleri belirleyebilecektir.

Tehdit detayları, kuruluşun tehdit ortamını anlamasını sağlayacak şekilde derinlemesine olmalı ve içgörüler sunmalıdır. Tehdit istihbaratı, iç ve dış kaynaklardan toplanmalı ve SIEM aracında otomatik uyarı oluşturmak için önceden tanımlanmış kurallar ve eşikler yapılandırmak üzere kullanılmalıdır. ASG, tehdit istihbaratını gerekli olduğu durumlarda satıcılar veya hizmet sağlayıcılarla paylaşacaktır.

5.8. Proje Yönetiminde Bilgi Güvenliği

ASG, projeleri (bilgi sistemlerinin dahil olduğu projelerle sınırlı olarak) yürüten bireylerin, projeleri kapsamında temel bilgi güvenliği kavramlarına aşina olmalarını sağlayacaktır. Proje güvenlik gereksinimleri belirlenmeli ve gözden geçirilmelidir.

Tüm fonksiyonlar, tüm yeni projeler, ürünler, uygulamalar, hizmetler vb. için güvenlik onayı almak zorundadır.

5.9. Bilgi Envanteri ve Diğer İlgili Varlıklar

Bölümlerdeki tüm fonksiyon başkanları, kendi fonksiyonlarında bu politikaya uygun olarak Varlık Yönetimi Prosedürünü tasarlamaktan ve uygulamaktan sorumludur. ASG'nin varlıkları ve stratejik ortaklarında/üçüncü taraflarda bulunan geçerli varlıklar tanımlanmalı ve varlığın kritikliğine dayalı olarak kapsamlı koruma sağlanmalıdır.

Bilgi ve bilgi işleme tesisleri ile ilişkili varlıklar tanımlanmalı ve bu varlıkların envanteri oluşturulup sürdürülmelidir. Bilgi varlığının yaşam döngüsü, oluşturulma ile başlayıp işleme, depolama, iletim, silme veya sona erme ve yok etme gibi farklı aşamaları içerir. Spesifik veya güncel envanterlerin belgelenmesi ihtiyaca göre sürdürülür.

Envanterde tutulan varlıklar sahiplenilmeli ve sahiplik envanterde belgelenmelidir. Bilgi sahibi, bilginin bakım ve korunma sorumluluğunu 'bilgi emanetçisi' olarak adlandırılan bir bireye/fonksiyona devredebilir.

Varlık envanteri, tanımlanmış aralıklarla, en az yılda bir kez ve bir varlığın kurulumu, değiştirilmesi ve kaldırılması durumlarında gözden geçirilmeli/güncellenmelidir. Bilgi varlıkları aşağıdaki kategoriler altında gruplanmalıdır:

Kategori	**Açıklama**
Bilgi Varlığı	Bu, aşağıdaki gibi dijital formdaki bilgileri içerecektir: Veritabanları ve veri dosyaları (yerel masaüstü bilgisayarlarda/laptoplarda bulunan önemli veriler dahil), sistem belgeleri, kullanıcı belgeleri, eğitim materyalleri, operasyonel/destek prosedürleri, süreklilik planları, arşivlenmiş bilgiler, bulut varlıkları ve sanal makineler vb.
Fiziksel Varlık	Bu, aşağıdaki gibi bilgisayar ekipmanlarını içerecektir: İşlemciler, monitörler, sunucular, dizüstü bilgisayarlar, modemler, yazıcılar vb. İletişim ekipmanları: Ağ cihazları, santraller, faks makineleri vb. Kullanılmayan manyetik medya: Bantlar, diskler, CD'ler vb.
Yazılım Varlığı	Bu, aşağıdaki gibi yazılımları içerecektir: Uygulama yazılımları, sistem yazılımları, yazılım lisansları, SSL sertifikaları, geliştirme araçları ve yardımcı programlar vb.
Hizmet Varlığı	Bu, dış kaynaklardan temin edilen süreçler veya satıcı/üçüncü taraf tarafından sağlanan hizmetleri içerecektir.
Döküman Varlığı	Fiziksel kopya formunda olan, operasyonlar sırasında kullanılan/gereken/oluşturulan ve iş süreçlerini yönetmek için kullanılan bilgiler. Örneğin, malzeme listesi, sözleşmeler, anlaşmalar, faturalar, kılavuzlar.
İnsan Varlığı	Bu, diğer varlıkları desteklemek ve işletmek için gereken personeli içerecektir.

Bilgi varlık envanteri, her varlık hakkında en az aşağıdaki bilgileri içermelidir:

- Varlığın türü ve konumu.
- Bu varlığı kullanan fonksiyonun adı.
- Varlık Sahibi, Emanetçi ve Kullanıcı bilgileri.
- Varlığın Bilgi Teknolojisi Varlık Değerleme Standardına göre sınıflandırılması.
- MAC ve IP yapılandırması, seri numarası, ana bilgisayar adı, çalışan hizmetler vb. gibi ek bilgiler (uygulanabilir olduğu durumlarda).

Bilgi Teknolojisi Varlık Değerleme Standardı' na başvurun.

a) Bilgi Varlığının Devreye Alınması ve Devreden Çıkarılması

o. Yeni dağıtılan bilgi varlıkları, ASG bilgi güvenliği gereksinimlerine uymak için gerekli tüm özelliklere ve işlevselliklere sahip olmalıdır.
p. Bilgi varlıkları, güvenlik onaylarından sonra devreye alınmalı ve devreden çıkarılmalıdır.
q. Bölümler, güncelliğini yitirmiş ve artık desteklenmeyen bilgi varlıklarının devreden çıkarılmasını sağlamalıdır.

5.10. Bilgi ve Diğer İlişkili Varlıkların Kabul Edilebilir Kullanımı

ASG, bilgi ve bilgi işleme tesisleriyle ilişkili varlıkların kabul edilebilir kullanımı için kuralların belirlenmesini, belgelenmesini ve uygulanmasını sağlayacaktır.

Bilgi ve BT varlıklarının Kabul Edilebilir Kullanımı Politikası' na başvurun.

5.11. Varlıkların İadesi

Tüm çalışanlar ve dış taraf kullanıcıları, istihdam, sözleşme veya anlaşmalarının sona ermesi veya feshi durumunda, sahip oldukları tüm örgütsel varlıkları geri iade etmelidir. ASG' ye ait herhangi bir kayıp veya iade edilmeyen malın maliyeti çalışan tarafından karşılanacaktır. İlgili işlevler, işten ayrılma/değişiklik veya çalışan transferi sırasında, ASG' ye ait tüm varlıkların çalışanlar ve dış taraf kullanıcıları tarafından geri iade edilmesini sağlamalıdır.

5.12. Bilginin Sınıflandırılması

Bilgi güvenliği bağlamında bilgi sınıflandırması, bilginin hassasiyet seviyesi, yasal önem ve bu bilginin yetkisiz bir şekilde ifşa edilmesi, değiştirilmesi veya yok edilmesinin ASG'ye olan etkisine dayalı olarak sınıflandırılmasıdır. Bilginin sınıflandırılması, bu bilgiyi korumak için uygun temel güvenlik kontrollerinin belirlenmesine yardımcı olur.

Tüm ASG bilgileri, dört hassasiyet seviyesi veya sınıflandırmadan birine dahil edilmelidir:

a. Sınıflandırılmamış (Unclassified)
b. Kısıtlı (Restricted)
c. Gizli (Confidential)
d. Çok Gizili (Secret)

a. Sınıflandırılmamış: Herkese açık alanda bulunan ve yetkisiz erişimin düşük etkisi olan bilgiler. ASG için yetkisiz ve/veya istenmeyen ifşanın etkisi: Yok veya önemsiz.
Örneğin, yıllık rapor, kurs bilgileri ve halka açık olarak yayınlanmak üzere hazırlanan gönderiler, broşürler, basın bültenleri, haber bültenleri gibi bilgiler ve halka açık organizasyon web siteleri (www.acibadem.com.tr)

b. Kısıtlı: ASG'nin genişletilmiş işletme içinde serbestçe paylaşmak istediği dahili bilgiler, yani aktif Gizlilik Anlaşması (NDA) bulunan herkesle dağıtılabilen bilgiler. Bu bilgilere erişim, personel (tüm dereceler) ve akredite doktorlarla sınırlıdır. ASG için yetkisiz ve/veya istenmeyen ifşanın etkisi: Küçük veya orta düzeyde.
Kısıtlı bilgiler, ASG'nin tüm çalışanları tarafından "Dahili" olarak da adlandırılacaktır.
Örneğin, hedeflenen halka yönelik yayınlar (bültenler, dahili telefon rehberleri, dahili politikalar ve prosedürler vb.).

c. Gizli: Bilgilerin yalnızca belirli bireyler veya gruplarla "bilmesi gereken" esasına göre paylaşılması gerektiği durumlar. Bilgi/veri sahibi, bu ilkenin hangi bireyler veya gruplar için geçerli olduğunu belirlemelidir. Bu tür bilgiye erişim, yetkili personel ile sınırlıdır; örneğin, bölüm bilgileri için fonksiyon başkanları ve üstü, diğer bilgiler için Başkan Yardımcıları ve üstü. ASG için yetkisiz ve/veya istenmeyen ifşanın etkisi: Büyük
Örneğin:

r. Satıcılarla yapılan gizlilik anlaşmaları
s. İşletme fikri mülkiyeti
t. Tüm tesisler/Stratejik İş Birimleri toplantı tutanakları
u. Tıbbi kayıtlar
v. Genel dahili e-posta iletişimleri
w. Denetim bulguları ve raporları
x. Hukuki sözleşmeler
y. Personel dosyaları (Derece 1'den 10'a kadar)
z. Kredi kartı numaraları
aa. Kişisel veriler (PDPA gibi geçerli gizlilik yasalarına tabi veriler)
bb. ASG BT Sistemlerine/kaynaklarına erişim şifreleri

d. Çok Gizli: Bilgilerin yalnızca açıkça adı belirtilen alıcılarla paylaşılması gerektiği durumlar ve bilginin dağıtımının onaylanmasından yalnızca bilgi sahibi sorumludur. Bu bilgiler, yalnızca bir gizlilik anlaşması imzalandıysa üçüncü taraflarla paylaşılabilir. Bu tür bilgiye erişim, SBU CEO'ları/COO'ları/Başkan Yardımcıları ve üstü ile sınırlıdır. ASG için yetkisiz ve/veya istenmeyen ifşanın etkisi: Ağır.
Örneğin:
cc. Finansal/Yönetim hesapları
dd. Strateji planları
ee. Yönetim kurulu toplantı tutanakları

5.12.1. Bilgi Toplama

Bilgi sahipleri, amacı veya işlevi ortak olan bir bilgi topluluğuna tek bir sınıflandırma atamak isteyebilirler. Bilgi topluluğunu sınıflandırırken, bireysel bilgi unsurlarından herhangi birinin en kısıtlayıcı sınıflandırması kullanılmalıdır.

Örneğin, bir bilgi topluluğu Kısıtlı ve Gizli seviyelerde bilgi içeriyorsa, bilgi topluluğu Gizli olarak sınıflandırılmalıdır.

5.12.2. Yeniden Sınıflandırma

Belirli aralıklarla, organizasyonel bilgilerin sınıflandırmasını yeniden değerlendirmek önemlidir. Bu, yasal ve sözleşmesel yükümlülüklerdeki değişiklikler ile bilginin kullanımı veya ASG organizasyonu için değerindeki değişikliklere dayalı olarak atanan sınıflandırmanın hala uygun olup olmadığını sağlamak içindir. Bu değerlendirme, ilgili Bilgi Sahibi tarafından yapılmalıdır. Değerlendirmenin yıllık olarak yapılması teşvik edilir; ancak, Bilgi Sahibi, mevcut kaynaklara dayalı olarak en uygun sıklığı belirlemelidir. Bir Bilgi Sahibi, belirli bir bilgi setinin sınıflandırmasının değiştiğini belirlerse, mevcut güvenlik kontrollerinin yeni sınıflandırma ile tutarlı olup olmadığını belirlemek için bir güvenlik kontrol analizi yapılmalıdır. Mevcut güvenlik kontrollerinde boşluklar bulunursa, bu boşluklar, sunulan risk seviyesine uygun olarak, zamanında düzeltilmelidir.

5.13. Bilginin Etiketlenmesi

Tüm bilgiler, bu politikada tanımlanan sınıflandırmaya göre etiketlenmelidir. Bilgi sahipleri, bilgi ile ilişkili varlıklarının uygun şekilde etiketlenmiş (işaretlenmiş) olmasını sağlamakla yükümlüdür.

Bu, yeterli düzeyde koruma sağlamayı amaçlar. Bilginin işlenmesi ve sağlanan güvenlik düzeyi, bilginin etiketlenmesine uygun olmalıdır.

5.13.1. **Bilgi İşleme**

Bilgi Türü Type: İşleme Kriterleri:	**SINIFLANDIRILMAMIŞ**	**KISITLI**	**GİZLİ**	**ÇOK GİZLİ**
Diğer Taraflara Dağıtım	Evet	Evet, Onay Gerekli	Evet, Onay ve NDA Gerekli	Hayır
Etiket	Özel bir kontrol gerekli değil	Bilgi kolayca anlaşılabilecek şekilde kısıtlı (örneğin dahili) olarak etiketlenmelidir	Bilgi kolayca anlaşılabilecek şekilde Gizli olarak etiketlenmelidir	Bilgi, içerdiği bilgilerin detaylarını içermeksizin gizli olduğu anlaşılacak şekile etiketlenmelidir
Depolama				
Veritabanı Sunucusu	İlgili değil	İlgili değil	Veritabanının performansı göz önünde bulundurularak şifrelenmesi **önerilir**	Veri, veritabanında şifrelenmesi **zorunludur.**
Yedfekleme Ortamı	İlgili değil	Uygulama Verileri, Dosya Sunucusu, Sunucu Yedekleri şifrelenmesi **zorunludur.**		
Uç Noktalar (PC, laptop)	İlgili değil	Tam disk şifrelemesi zorunludur.		
Mobil cihazlar		Mobil cihazlarda veri depolamak için şifreleme kullanımı **önerilir.**		Kullanım, Bilgi Sahibi tarafından onaylanmalıdır. Veri şifrelenmesi **zorunludur.**
Taşınabilir depolama ortamı (USB bellek, disk veya CD gibi)	İlgili değil	Dosyalar şifrelenmeli (şifre korumalı) ve cihaz kilitli güvenli yerlerde saklanmalıdır. Dosyalar taşınabilir depolamadan kopyalandıktan sonra silinmelidir.		Onaylanmıyor
Bulut depolama (e.g., Dropbox, Google Drive)	İlgili değil	Şirket tarafından sağlanan OneDrive gibi depolama alanları, dosya şifrelemesi (şifre korumalı) ile kullanılmalıdır. Dropbox, Google Drive, Box gibi kişisel bulut depolama abonelikleri resmi amaçlar için kullanılmamalıdır.		Onaylanmıyor
İletim				
Network	İlgili değil	Güvenilmeyen ağlarda ağ iletimi şifrelenmelidir.		Tüm ağ iletişimleri için ağ iletimi şifrelenmelidir.
Eposta	İlgili değil	Eklerin şifrelenmesi önerilir (örneğin, MS Office'in şifre kilitleme özelliği ile ekleri parola korumasıyla veya 7-zip kullanarak).		'Bilgi Sahibi' onayı gereklidir. Ekler şifrelenmelidir.
İmha	İlgili değil	Kağıt tabanlı bilgiler için parçalama gereklidir. Dijital depolama ortamlarının (örneğin, sabit diskler, bantlar vb.) imha edilmeden önce manyetik alanla silinmesi (degaussing) veya ezilmesi gerekmektedir (BT personeli tarafından gerçekleştirilir).		

5.14. Bilgi Aktarımı

İlgili güvenlik kontrolleri (teknik, süreç, sözleşmeler/anlaşmalar gibi kontroller) paydaşlarla bilgi alışverişi yapmak için uygulanmalıdır. Herhangi bir gizli, özel veya ayrıcalıklı bilgi bir bilgi sisteminden başka bir bilgi sistemine aktarılmadan önce, transferi yapan kişi, hedef sistemdeki erişim kontrollerinin kaynak sistemdeki erişim kontrolleri ile eşdeğer olduğundan emin olmalıdır. Eşdeğer güvenlik erişim kontrolleri yoksa, bilgi aktarılmamalıdır.

Veri İndirme Politikası' na bakınız.

5.15. Erişim Kontrolü

ASG tarafından işletilen veya kontrol edilen herhangi bir bilgi varlığına ve tesise erişim yalnızca yetkilendirme ile olacaktır. ASG tesislerinin/bilgi varlıklarının bilgi işleme alanlarına (uygulanabilir olduğu şekilde fiziksel veya mantıksal) erişim, iş ve bilgi güvenliği gereksinimlerine göre yetkilendirmeye dayalı olacaktır. ASG'deki ilgili fonksiyon, bu politika doğrultusunda İzin Yönetimi Prosedürünün (talep eden, onaylayan ve uygulayıcı ile ilgili ayrıntıları, kapsamındaki sistemleri, erişim sonlandırma ve erişim mutabakat sürecini içerecek şekilde) tasarlanmasını ve uygulanmasını sağlamalıdır.

ASG'nin BT Sistemlerine ve kaynaklarına erişim, aşağıdaki ilkelere göre yönetilecektir:

ff. **Bilme ve kullanma gereksinimine dayalı olarak:** Bireyler, iş görevlerini yerine getirmek için gerekli olan bilgilere erişim sağlamalıdır.
gg. **En az ayrıcalık prensibi:** Kullanıcı hesabına, amaçlanan işlevi yerine getirmek için gerekli olan ayrıcalıklar verilmelidir.
hh. **Görevlerin ayrılması:** Yetkisiz veya kasıtsız değişiklik fırsatlarını azaltmak için bir süreçteki çatışan sorumluluk alanlarını farklı kullanıcılara ayırmak.

Yeni erişim talepleri ve mevcut ayrıcalıklardaki değişiklik talepleri, Bilgi Sahibi veya yetkilisi tarafından onaylanmalıdır. Talep eden, yetkilendiren ve/veya erişim yöneticisi arasındaki ayrım sağlanacaktır. Görevlerin ayrılması mümkün olmadığında, erişim haklarının kötüye kullanılmasını tespit etmek için aktif izleme, denetim izi ve yönetim gözetimi gibi uygun dengeleyici kontroller geliştirilmelidir. İş nedenleriyle birden fazla rolün tahsis edilmesi gerektiğinde, bu durum resmi olarak belgelenmeli ve onaylanmalıdır.

5.15.1. Erişim Kontrol Matrisi (ACM)

BT sistemleri/kaynakları için tüm kullanıcı rolleri ve izinlerini tanımlayan bir matris, canlıya geçmeden önce belgelenmeli ve devam eden tüm değişiklikler için güncellenmelidir. Erişim Kontrol Matrisi (ACM) Bilgi Sahibi ve ilgili fonksiyon yöneticisi tarafından onaylanmalıdır. ACM'deki tüm revizyonlar, yayınlanmadan önce uygun şekilde kontrol edilmeli, incelemeler, onaylar ve sürüm yönetimi dahil edilmelidir. Erişim haklarının devam eden onayları, onaylanmış ACM'ye göre eşleştirilecektir.

5.16. Kimlik Yönetimi

- Bilgi sistemlerine erişimi olan tüm kullanıcılar için benzersiz bir kullanıcı kimliği oluşturulmalıdır.
- Operasyonel/fonksiyonel gereksinimlere dayalı olarak oluşturulan genel kimliklerden kaçınılmalı ve böyle kimlikler oluşturulması gerekiyorsa Güvenlik Aşımı alınmalıdır.
- Etkileşimli olmayan servis hesapları yalnızca gerekli güvenlik onaylarından sonra oluşturulmalıdır.
- Fonksiyon Yöneticileri, kendi kullanıcılarının kullanıcı kimliklerinin oluşturulmasından önce erişim taleplerini onaylamalıdır.

- Hiçbir kullanıcı kendi erişimini onaylamamalıdır. Yetkilendirme talebi ile onay arasında görev ayrımı bulunmalıdır.
- Kullanıcıya yönetici hakları da dahil olmak üzere erişim ayrıcalıkları yalnızca kullanıcının rolüne ve uygun meşru iş amaçlarına göre verilmelidir ve artık gerekli olmadığında iptal edilmelidir.
- Kullanıcının kimliği, kullanıcı adı ve alan adı kombinasyonu ile belirlenmelidir. Kullanıcı hesaplarının/kimliklerinin ve erişim haklarının eklenmesi, değiştirilmesi veya silinmesi için yapılan tüm taleplerin denetim izleri tutulmalıdır.
- Aynı kullanıcı kimliğiyle yapılan simülasyon oturumlarından kaçınılmalıdır.

5.17. Kimlik Doğrulama Bilgileri

ASG'nın bilgi sistemlerindeki tüm hesaplar şifre ile korunmalı ve gizliliği, bütünlüğü ve bilgilerin kullanılabilirliğini sağlamak için (uygun olduğu yerlerde) Çok Faktörlü Kimlik Doğrulama kullanılmalıdır. Bu politikaya uyum sağlamak amacıyla bilgi sistemlerinde şifre yönetimi için uygun teknik şartnameler uygulanmalıdır.

Şifreler, bilgi güvenliğinin önemli bir yönüdür. Kötü seçilmiş bir şifre, yetkisiz erişim ve/veya ASG'nın kaynaklarının kötüye kullanımıyla sonuçlanabilir. ASG sistemlerine erişimi olan tüm kullanıcılar, çalışanlar, yükleniciler ve satıcılar dahil olmak üzere, aşağıda belirtilen adımları izleyerek şifrelerini seçmek ve güvence altına almakla sorumludur.

5.17.1. **Şifre Oluşturma**

a. Şifreler aşağıdaki kurallara uygun olmalıdır:

Şifre uzunluğu (en az)	a) Normal Kullanıcı:8 karakter b) Servis Kullanıcısı 16 karakter c) Genel Kullanıcı 16 karakter d) Ayrıcalıklı Kullanıcı: Seçenek#1: 8 karakter şifre + :SMS, yazılımsal anahtar veya biyometrik vb. iki faktör doğrulama Seçenek#2: 16-karakter şifre
Şifre Karmaşıklığı:	a) Büyük ve Küçük harf içerir b) En az bir rakam içerir c) Kullanıcı isminden farklı d) Özel karakterler içerir ($, #, @ gibi)

b. İlk ve Varsayılan Şifreler:

- İlk şifreler yalnızca ilgili kullanıcının ilk giriş oturumu için geçerlidir. Kullanıcı, ilk başarılı girişten sonra şifreyi değiştirmelidir, böylece kullanımına devam edebilir.
- Sistem yöneticileri, yönetimsel hesaplar için varsayılan şifreleri kullanmamalıdır.
- Bilgi sistemlerinin devreye alınması sırasında satıcı varsayılan şifresini kaldırmalı/değiştirmelidir.
- Giriş kimliği ve ilk şifre aynı e-postada kullanıcıya verilmemeli, güvenli kanallar kullanılmalıdır.

c. Tüm hesaplar için, kullanıcıların hatırlaması kolay ancak hacker'ların tahmin etmesi zor olan en az 16 karakter uzunluğunda uzun cümleler olan şifre cümleleri kullanmaları önerilir. Örneğin, "5 dolarlık milkshake içmek istiyorum."

d. Kullanıcılar kişisel e-posta/IT sistemleri ve iş e-posta/IT sistemleri için farklı şifreler kullanmalıdır. Aynı şifre kişisel e-posta kırıldığında (örneğin, Gmail, Yahoo vb.) ve bu şifre iş e-postası/IT sistemine denendiğinde siber suçluların işini kolaylaştırır, bu da izinsiz erişime yol açabilir.

f. Mümkün olduğunda, kullanıcılar farklı ASG erişim ihtiyaçları için aynı şifreyi kullanmamalıdır.

e. Sistem düzeyi ayrıcalıkları grup üyelikleri veya sudo gibi programlar aracılığıyla verilen kullanıcı hesapları, sistem düzeyi ayrıcalıklarına erişmek için diğer tüm hesaplardan farklı bir şifre kullanmalıdır.

f. Kullanıcılar, hacker'ların izinsiz erişime yol açabilecek zayıf şifreler kullanmamalıdır. Aşağıdaki zayıf şifre türlerinden kaçınılmalıdır:

- Sekiz karakterden az olması.
- Sözlükte bulunabilen kelimeler içermesi, yabancı dil veya dil argosu, lehçe veya jargon içermesi (hacker'lar basit şifreleri kırmak için sözlük saldırıları kullanabilir).
- Doğum tarihi, adres, telefon numarası veya aile üyelerinin, evcil hayvanların, arkadaşların veya hayalî karakterlerin adları gibi kişisel bilgiler içermesi.
- İşle ilgili bilgiler içermesi, bina adları, sistem komutları, siteler, şirketler, donanım veya yazılım gibi.
- aaa, bbb gibi sayı desenleri, qwerty, zyxwvuts veya 123321 gibi.
- Yaygın kelimelerin ters yazılmış versiyonları veya bir sayı ile önce veya sonra (örneğin, secret1 veya 1secret).
- "Welcome123", "Password123", "Changeme1" gibi versiyonları içermesi.

g. Kullanıcılar şifrelerini yazmamalıdır. Bunun yerine, hacker'ların tahmin etmesi veya kırması zor olacak şekilde kolayca hatırlayabilecekleri şifreler oluşturmaya çalışmalıdırlar. Bunun bir yolu, şarkı başlığına, olumlama cümlesine veya başka bir kolay hatırlanabilir ifadeye dayanan bir şifre cümlesi oluşturmaktır.

h. Mümkün olduğunda, kullanıcılar ASG altyapısındaki bilgi varlıklarına güvenli erişim için çok faktörlü kimlik doğrulama kullanmalıdır. Bu uygulanamadığı durumlarda (örneğin, servis hesapları için), telafi edici kontroller değerlendirilmelidir.

5.17.2. Şifre Değiştirme

a. Şifreler aşağıdaki periyotlarda değiştirilmelidir:

- Kullanıcı hesabı: 90 gün
- Genel hesaplar: 90 gün
- Ayrıcalıklı hesap: 60 gün

- Servis hesabı: (süresiz) muaf tutulmuştur

b. Servis hesapları şifre süresinin dolduğu durumlarda hizmet kesintilerini önlemek için şifre değişimi gerektiren süreçlerle ilgili olarak muaf tutulmuştur, ancak bu tür hesaplar sunuculara/sistemlere etkileşimli giriş için kullanılmamalıdır.

c. Şifre kırma veya tahmin etme işlemleri periyodik veya rastgele olarak IT Güvenlik ekibi veya yetkilileri tarafından gerçekleştirilebilir. Bu taramalardan birinde bir şifre kırılırsa veya tahmin edilirse, kullanıcının bu politikaya uygun olarak değiştirmesi gerekecektir.

d. Mümkün olduğu her yerde, uygulamalar/altyapı, şifrenin periyodik olarak değiştirilmesini zorunlu kılacak bir mekanizma sağlamalıdır ve şifre uygulama kaynak kodunun bir parçası olmamalıdır (yani, uygulama içine kodlanmamalıdır).

5.17.3. **Şifre Koruma**

• Şifreleri kimseyle paylaşmayın. Tüm şifreler, Hassas, Gizli ASG bilgisi olarak ele alınmalıdır.

• Şifreleri e-posta mesajlarına, sohbet mesajlarına veya diğer elektronik iletişim biçimlerine eklemeyin, iletmeyin veya depolamayın.

• Şifreleri telefonla IT destek masası dahil hiç kimseye açıklamayın.

• Şifreleri anketlerde veya güvenlik formlarında açıklamayın.

• Şifrenin formatını ima etmeyin (örneğin, "aile adım").

• ASG şifrelerini, yönetici yardımcıları, sekreterler, yöneticiler, tatildeyken iş arkadaşları ve aile üyeleri dahil olmak üzere kimseyle paylaşmayın.

• Şifreleri yazıp ofisinizde herhangi bir yerde saklamayın. Şifreleri şifrelenmeden bilgisayar sistemlerinde veya mobil cihazlarda (telefon, tablet) bir dosyada saklamayın.

• Uygulamaların "Şifreyi Hatırla" özelliğini kullanmayın (örneğin, web tarayıcıları).

• Şifresinin tehlikeye girdiğini düşünen her kullanıcı, olayı IT yardım masasına bildirmeli ve derhal tüm şifrelerini değiştirmelidir.

5.17.4. Uygulama Geliştirme ve Sistem Kurulumu

Uygulama geliştiricileri ve Sistem yöneticileri, programlarının aşağıdaki güvenlik önlemlerini içermesini sağlamalıdır:

- Uygulamalar, gruplar yerine bireysel kullanıcıların kimlik doğrulamasını desteklemelidir. Tüm parolalar, bu belgede belirtilen Parola oluşturma politikası ve Parola yaşlandırma politikasına uygun olmalıdır.

- Uygulamalar, parolaları açık metin veya kolayca geri çevrilebilir bir biçimde depolamamalıdır.

- Uygulamalar, parolaları ağ üzerinden açık metin olarak iletmemelidir.

- Uygulamalar, bir kullanıcının başka birinin parolasını bilmeden o kişinin işlevlerini üstlenebilmesini sağlayan bir rol yönetimi sağlamalıdır.

- Sistem izin veriyorsa, kullanıcının son on parolasının kullanılmasına izin vermemelidir (parola geçmişi).
- Parola minimum yaşı, tercih edilen bir parolaya geri dönmek için önceki parolaları döngüye sokmayı önlemek için '1 gün' olarak ayarlanmalıdır.
- Hesap kilitleme eşiği, '5 veya daha az başarısız oturum açma girişimi' olarak ayarlanmalıdır.

5.17.5. Ayrıcalıklı Hesap Yönetimi

- İki faktörlü kimlik doğrulama gibi güçlü kimlik doğrulama, uygun olduğu durumlarda Ayrıcalıklı Kimliklerde kullanılmalıdır. İki faktörlü kimlik doğrulama mümkün değilse, Parola oluşturma politikasına göre 16 karakterlik uzun parolalar (parolafraze) kullanılarak risk azaltılmalıdır.
- SA, Yönetici, Kök vb. varsayılan yönetici hesapları, acil durumlar dışında günlük işlemler için kullanılmamalıdır. Altyapı (Sunucular, Veritabanı, Ağ cihazları) için varsayılan yönetici hesaplarının parolaları, güvenli elektronik bir kasada saklanmalı veya iki kişi tarafından benzersiz olarak oluşturulmalı (parola bölünmesi) ve ülke/İş Birimi BT Yöneticisi veya eşdeğer yetkili tarafından zarfa mühürlenmelidir. Tüm sunucular/cihazlar için aynı parolanın kullanılması yasaktır, çünkü bir sunucu/cihazın ele geçirilmesi tüm sunucular/cihazlara erişim sağlayabilir.
- Bu kullanıcı kimliklerine ve parolalarına erişim verilen kişilerin kayıtları tutulmalıdır.
- Ayrıcalıklı kullanıcıların gerçekleştirdiği faaliyetler izlenmeli ve başarılı ve başarısız oturum açma girişimlerinin ve parola değişikliklerinin izlenmesi için kontroller konulmalıdır.
- Ayrıcalıklı Hesap kilitleme eşiği, 5 veya daha az geçersiz oturum açma girişimi olarak ayarlanmalıdır. Hesap, kullanıcı tarafından yapılan 5 ardışık yanlış girişimden sonra kalıcı olarak kilitlenmelidir.
- Varsayılan yönetici hesabı erişiminin gerekli olduğu acil durumlarda, parola BT yöneticisinin onayıyla zarftan alınmalıdır. Faaliyet tamamlandıktan sonra, varsayılan hesap parolası iki kişi tarafından (parola bölünmesi) her iki yarısı için de değiştirilmeli ve ardından bölüm/İş Birimi BT Yöneticisi ile yeniden mühürlenmelidir.

Mümkün olduğu durumlarda, ASG, kimlik doğrulama mekanizmasını güçlendirmek için aşağıdakilerin uygulanmasını ek kontroller olarak değerlendirecektir**:**

- CAPTCHA gibi güvenlik özelliklerini veya sektör en iyi uygulamalarını uygulayın
- Kullanıcı faaliyetlerinin ayrıntılı günlüğünü tutun
- Güvenliğin ek bir katmanını uygulayın

5.17.6. Sorumluluklar

- Etki alanındaki sistemlere/hizmetlere erişmek için hesabı olan tüm bireysel kullanıcılar ve sunucuların/ağların sistem/ağ yöneticileri, bu politikanın uygulanmasından sorumludur.
- Site/uygulama geliştirmesinden sorumlu tüm tasarımcılar/geliştiriciler, bu kontrolün uygulamalarına dahil edilmesini sağlamalıdır.

5.17.7. Şifresiz Kimlik Doğrulama

Şifresiz kimlik doğrulama yöntemleri, geleneksel şifrelerden başka doğrulama biçimlerine dayanır. Aşağıdaki yöntemler/kombinasyonlar kullanılabilir:

- **Biyometrik Kimlik Doğrulama**: Using fingerprint, facial recognition, or other biometric methods.
- **Donanım Anahtarları**: FIDO gibi bir kerelik kod üreten bir donanım belirteci kullanma.
- **Mobil Kimlik Doğrulama**: Bir kerelik kod üreten veya alan bir mobil uygulama kullanma, örneğin Microsoft Authenticator.

Aşağıdakiler ek olarak dikkate alıabilir:

- **Yedek Yöntem:** Kullanıcıların, birincil yöntem başarısız olduğunda kullanılabilecek ikincil bir kimlik doğrulama yöntemi olmalıdır.
- **İsteğe Bağlı –** Cihaz Kaydı: Kimlik doğrulama için kullanılan cihazlar (örneğin, akıllı telefonlar) BT departmanı tarafından kaydedilmeli ve onaylanmalıdır.
- **Kayıp Cihazlar**: Kullanıcılar, bu tür kimlik doğrulama için kullanılan kayıp veya çalınan cihazları derhal BT departmanına bildirmelidir.
- **Şüpheli Aktivite**: Herhangi bir yetkisiz erişim denemesi veya şüpheli faaliyet derhal bildirilmelidir.

5.18. Erişim Hakları

a. Atama ve Değişiklik

Bilgi sistemlerine erişim hakkının atanması ve değiştirilmesi, bu Politika'nın 5.15 ve 5.16 numaralı kontrollerine uygun olmalıdır.

b. Erişim Haklarının İptali

Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve bilgi işleme tesislerine erişim hakları, istihdamlarının, sözleşmelerinin veya anlaşmalarının sona ermesi üzerine kaldırılmalı veya değişiklik durumunda güncellenmelidir.

Çalışanların tüm erişim hakları, işten ayrılmalarının son gününden itibaren 72 saati aşmayan bir süre içinde askıya alınmalı/kaldırılmalı ve kritik sistemlere erişim (CMDB ile uyumlu olarak) çalışanların son çalışma günü itibarıyla iptal edilmelidir.

c. Kullanıcı Erişimi ve Erişim Kontrol Matrisi (ACM)'nin İncelenmesi

Bilgi sahibi veya atanmış kişi, erişim kontrol matrisinin (KCM) uyumluluğunu ve tüm IT sistemleri/kaynaklarının (hizmet hesapları dahil) erişim haklarını, normal ve ayrıcalıklı kullanıcılar için en az yarı yıllık olarak, geçersiz ve/veya kullanılmayan atamaları da içerecek şekilde incelemelidir.

KCM, İK tarafından işten çıkarılan ve bölümlerin BT fonksiyonu tarafından düzenli olarak belirlenen sıklıkta çalışanların hesaplarının sonlandırılması için gözden geçirilmelidir. Tüm KCM ve kullanıcı erişimi incelemeleri belgelendirilmelidir.

Düzenli aralıklarla (en az yılda iki kez), pasif veya kullanılmayan kullanıcı kimliklerini tespit etmek için bir inceleme yapılmalıdır. Artık gerekli olmayan pasif veya kullanılmayan kullanıcı kimlikleri uygun şekilde kaldırılmalı veya devre dışı bırakılmalıdır.

Tüm erişim hakları ihlalleri, inceleme ve iyileştirme için bölümün BT fonksiyonuna ve güvenlik ekibine zamanında bildirilmelidir.

5.19. Tedarikçi İlişkilerinde Bilgi Güvenliği

ASG, aşağıdaki tedarikçi yaşam döngüsünün tedarikçi kabulü/çalıştırılmasından hizmetlerinin sonlandırılmasına kadar takip edilmesini sağlamalıdır:

• Risk değerlendirmesi

• Ekranda

• Anlaşma

• Erişim kontrolü

• Izleme

• Sonlandırma

Ekipman, malzeme, ürün, hizmet ve bakım satın alan tüm bireyler, bu işlemlerin Bilgi Güvenliği Politikası'na uygun bir şekilde yürütüldüğünden emin olmalıdır. Bilgi sistemleri ve hizmetleri, ASG çevresinin güvenliğine önemli bir etkisi olacak şekilde depolanan ve işlenen bilgiyi sağlamalıdır. İlgili Tedarikçiler aşağıdaki hedeflere ulaşmalıdır:

• Uygulamaları gerektiğinde ASG'nın bilgi güvenliği hedeflerine ve diğer yasal ve düzenleyici gerekliliklere uyum sağlamak

• Gerekli kontrolleri uygulamak için bilgi kaynaklarının gizliliğini sağlamak

• Potansiyel tehditlere veya tehlikelere karşı korumak

• Yetkisiz erişime veya kullanıma karşı korumak

• ASG'nın güvenlik denetimleri yapmasına ve risk değerlendirmelerini teslim etmesine izin vermek

5.20. Tedarikçi Sözleşmelerinde Bilgi Güvenliğinin Ele alınması

ASG, tedarikçi sözleşmelerine uygun IT/Güvenlik ve gizlilik yükümlülüklerini (ASG Kişisel Veri Koruma Politikası gereği) dahil etmeli ve tedarikçilerle uyum için gerekli bilgi güvenliği kontrol listelerini paylaşmalıdır; bu değerlendirmeler için ASG güvenlik ekiplerini de dahil etmelidir.

Özel Hizmet Seviyesi Anlaşmaları (SLA) ve Uygulama Performans Göstergeleri (KPI), ilgili olabilecek şekilde belirlenmiş olan katılımları dikkate alarak, Tedarikçilerle anlaşılmalıdır. ASG Sistem sahibi, tedarikçilerinin hizmet seviyesi anlaşmalarını ("SLA") gözden geçirmek için özel kaynaklar atamalıdır ki bu sağlamış olduklarını yükümlülükler anlatıldı. Tedarikçi hizmet düzeyleri periyodik olarak izlenmeli ve performansı uygun bir IT personeli tarafından izlenmelidir, bu sayede SLA ihlalleri zamanında raporlanmalı ve araştırılmalıdır.

ASG'nın bilgi ve destek ile ilgili herhangi bir güvenlik ihlalini bilgilendirmesi ve bu tür ihlallerin etkisini minimize etmek için uygun koruma önlemlerini alması gerekmektedir.

Gizlilik Anlaşmaları (“NDA”), ASG, çalışanları, müşterileri, alt yüklenicileri ve/veya diğer üçüncü taraflarla ilgili bilgilerin Tedarikçiler tarafından kullanılması, depolanması ve işlenmesi için kurulmalıdır.

Lütfen ASG Kişisel Veri Koruma Politikası'na başvurun.

5.21. Bilgi ve İletişim Teknolojisi (ICT) Tedarik Zincirinde Bilgi Güvenliğinin Yönetimi

Tamamlanan ASG risk değerlendirmesi, her risk unsuru için aşağıdaki risk derecelendirmesi ile tedarikçinin değerlendirilmesi sonucunu verecektir. Her risk unsuru için risk derecesi farklı olabilir ve koruma önerileri ile ilgili tavsiyeler değişebilir:

Risk Puanı – Düşük: Düşük riskli bir tedarikçi durumunda, mal veya hizmetler, Malzeme ve Malzeme Olmayan risklere dayanarak belirli koruma önerileri olmadan temin edilebilir. Ancak standart sözleşme koşulları

(güvenlik maddeleri dahil) ve şartlar geçerli olacaktır ve satın alma emri/sözleşme/anlaşma belirli SLA'ları içerecektir.

Risk Puanı – Orta: Bu durumda, onay öncesinde yerine getirilmesi gereken koruma önlemlerini önermek gerekecektir. Takımın önermesi:

- ASG çıkarlarını korumak için güvenlik ve gizlilik maddeleri ile birlikte standart sözleşme koşulları
- Tedarikçi ile anlaşmaya konulacak belirli SLA'lar
- Tedarikçinin performansının periyodik olarak gözden geçirilmesi
- Tedarikçi süreçlerinin denetlenmesi (yerinde inceleme dahil) için tedarik, İş veya İç Denetim ekibi tarafından denetim

Risk Puanı – Yüksek: Bu durumda, onay öncesinde yerine getirilmesi gereken belirli koruma önlemlerini önermek gerekecektir. Takımın önermesi:

- ASG çıkarlarını korumak için sözleşme/anlaşma içine dahil edilecek belirli sözleşme maddeleri (güvenlik ve gizlilik dikkate alınarak)
- Tedarikçi ile anlaşmaya konulacak belirli SLA'lar
- Tedarikçinin performansının periyodik olarak gözden geçirilmesi
- Danışma sonucunda belirlenen risklerin periyodik olarak gözden geçirilmesi
- Tedarikçi süreçlerinin denetlenmesi (yerinde inceleme dahil) için tedarik, İş veya İç Denetim ekibi tarafından denetim

Eğer ASG operasyonunun herhangi bir yönü üçüncü taraf tarafından alt yükleniciye dış kaynak kullanımı ile daha da dış kaynak kullanımı yapılırsa, üçüncü taraf ile alt yüklenici arasındaki anlaşma ilgili güvenlik ve gizlilik kontrollerini ve gereklilikleri kapsamalıdır.

Lütfen **ASG Üçüncü Taraf IT ve Siber Güvenlik Risk Yönetim Çerçevesi** ile ASG **Kişisel Veri Koruma Politikası**'na başvurun.

5.22. Tedarikçi Hizmetlerinin İzlenmesi, İncelemesi ve Değişiklik Yönetimi

ASG yönetimi, tedarikçilerin mevcut uyumunu ve performans sonuçlarını, tedarikçinin sağladığı malzemelerin/hizmetlerin doğası ve önemine bağlı olarak en az yılda bir kez, veya hizmet sözleşmelerinin yenilenmesinden önce, hangisi daha önce ise değerlendirmelidir. Frekans, her risk değerlendirmesi ve performans değerlendirmesi sonuçlarına dayalı olarak yeniden gözden geçirilmelidir.

Tedarikçi hizmetlerinin izlenmesi ve gözden geçirilmesi, anlaşmanın bilgi güvenliği şartlarına saygı gösterilmesini sağlar ve bilgi güvenliği ile ilgili olaylar ve sorunların dikkatli bir şekilde izlenmesini içerir.

- Anlaşma uyumluluğunu doğrulamak için hizmet performans seviyesinin izlenmesi
- Anlaşmalar gereği sağlanan tedarikçi hizmet raporlarının ve şartnamelerinin gözden geçirilmesi
- Tedarikçi denetimlerinin yapılması ve güvenlik/operasyonel sorunlar, arızalar ve hata takibi ile ilgili raporlanan problemlerin takibi

- Anlaşmalar gereği sağlanan güvenlik olaylarına ilişkin ayrıntıların kolaylaştırılması ve gözden geçirilmesi, ilgili kılavuz ve prosedürlere uygun olarak

Gerekirse ilgili loglar ASG SOC ile entegre edilmeli ve Tedarikçilerle ağ entegrasyon noktaları bu tür entegrasyonlar aracılığıyla SOC ile izlenmelidir. Uygulama kapsamına göre SOC altında ilgili kullanım durumları değerlendirilmeli ve oluşturulmalıdır ki bu ASG'nin katılım yoluyla saldırı kategorisine göre uygulanabilir.

Tedarikçi sözleşmelerinde yapılan değişiklikler bu politikaya uygun olarak gözden geçirilmeli ve onaylanmalıdır. Ve bu değişiklikler gözden geçirme aşamasında işletme sistemlerinin ve süreçlerinin kritikliğini dikkate almalıdır.

5.23. Bulut Hizmetlerinin Kullanımı İçin Bilgi Güvenliği

ASG'nin bulut hizmetlerinin sağlanmasının iş gereksinimleri, güvenlik gereksinimleri ve ilgili yasal düzenlemelere uygun olduğundan emin olması gerekmektedir. ASG için ana benimseme faktörleri:

Faktör	Fayda
Fiyat Performans Dengesi	• Maliyetleri konsolidasyon, kaynakların havuzlanması ve paylaşımı yoluyla azaltır. • "Kontrollü" ödeme sağlar. • Enerji tasarrufu ve çevre korumasına olanak tanır. • Bilgi ve İletişim Teknolojileri (ICT) yönetiminde azalma sağlayarak çekirdek hedeflere ve süreç iyileştirmelerine odaklanmayı mümkün kılar.
Esneklik	• Hızlı hizmet sağlama ve dağıtımı ile talep üzerine ölçeklenebilirlik.
Operasyonel Destek	• Yüksek erişilebilirlik ve günün her saati profesyonel destek
Güvenlik	• Bulut, güvenlik yönetiminin (örneğin, zayıflıkların test edilmesi, denetimler, güncelleme yönetimi) otomasyonunu sağlayan ve en iyi uygulamaların tutarlı olarak uygulanmasını mümkün kılan daha homojen ve birleşik bir platformdur. • Bulut platformları, kullanılabilirlik için tasarlanmış ve işletilmektedir. • Kurumsal sınıf bulut sistemlerinin kullanımı ayrıca güvenliği artırabilir. Büyük, olgun ve kurumsal sınıf bulut sağlayıcıları, dünya standartlarında güvenlik sağlayabilecek sofistike sistemlere, süreçlere ve insan kaynaklarına yatırım yapmıştır. • Operasyonun ölçeği, bulutta bireysel uygulamalara göre daha düşük maliyetlerle güvenliği artırır ve yönetimi kolaylaştırır. • Büyük ve olgun Bulut Hizmet Sağlayıcıları (CSP'ler), bireysel kuruluşlar için ekonomik olmayabilecek özelleşmiş personel işe alabilmektedirler.

Çeviklik	• Bulut tarafından sağlanan ölçek ve paylaşılan kaynaklar sayesinde (hem bir ortak hem de bir ajans olarak CSP tarafından), yenilik senaryoları bireysel ve farklı uygulamaların maliyetinin bir kesriyle mümkün olmaktadır.

ASG'nin bulut ortamını uygun güvenlik önlemleri ve çözümlerle doğru şekilde koruyacağından emin olacaksınız. Erişilebilirlik, yapılandırmalar ve bilgilerin doğru şekilde korunacağını ve sadece yetkili kişilere verileceğini sağlayacaksınız.ASG şunlardan emin olmalıdır:

- CSP'ler, hizmet haklarına, bilgi gizliliği ve koruma yasalarına ve diğer ilgili yasa ve düzenlemelere uygun olacaktır.
- Bulut ortamı için risk değerlendirme metodolojisini, süreçlerini ve araçlarını optimize etmek için çalışılacaktır.
- CSP'nin risk kontrol ve güvenlik politikasının uluslararası en iyi uygulamalara uygun olduğu sorulacak ve doğrulanacaktır.
- CSP'nin NIST SP800-125 gibi endüstri yaygın sıkılaştırma kılavuzlarına uyduğu sağlanacaktır.
- CSP'nin yalnızca yetkilendirilmiş anlık görüntülerin alındığını garanti etmek için kontrolleri bulunmaktadır ve bu anlık görüntülerin sınıflandırma düzeyi, depolama yeri ve şifreleme gücü üretim sanallaştırma ortamıyla uyumludur.
- CSP güçlü kimlik doğrulama mekanizmaları ve denetim kayıtları kullanmaktadır.
- CSP, tokenlar, tek kullanımlık şifreler, biyometrikler gibi çeşitli çok faktörlü kimlik doğrulama mekanizmalarını desteklemektedir.
- CSP, ASG'nin kendi kimliklerini yönetmesine izin vermektedir.
- CSP'nin kimlik doğrulama süreci, erişim kontrolü, hesap verebilirlik ve günlükleme (format saklama ve erişim) ASG gereksinimlerini karşılamaktadır.
- CSP'den gelen günlükler, ASG SOC (Güvenlik Operasyon Merkezi) tarafından izleme için entegre edilmektedir.
- CSP, ASG gereksinimlerine uygun olarak paylaşılan ortamda veri segmentasyonunu sağlar (Ağ, fiziksel, sistem ve uygulama).
- Verinin transitte, depolamada ve işleme sürecinde gerektiği gibi şifrelenmesini sağlar.
- CSP, paylaşılan ortamda bir müşteriden diğerine veri sızarsa dahi verinin erişilemez kalması için benzersiz şifreleme anahtarları sunar.
- Hassas bilgi alışverişi veya hizmet sağlanmadan önce CSP ile NDA (Gizlilik Sözleşmesi) imzalanır.

- ASG, yedek medya dahil olmak üzere farklı kopyalarda ASG verilerinin mülkiyetine özel haklara sahiptir ve CSP'nin veriyi izinsiz ikincil amaçlar için kullanma hakkı bulunmamaktadır.
- CSP, planlanmış veya plansız kesinti veya arızalar durumunda iş sürekliliği ve felaket kurtarma planlama ile yedekleme ve gereksizlik mekanizmalarıyla veri erişilebilirliğini (ASG BIA veya iş gereksinimlerine göre) sağlar.
- Hizmetlerin düşünüldüğü şekilde CSP'lerle SLA'lar (Hizmet Seviyesi Anlaşmaları) imzalanır.
- CSP'de herhangi bir ihlal (onaylanmış veya şüpheli) ASG'de mevcut olan Bilgi Güvenliği Olay Bildirim Prosedürüne uygun olarak yönetilir.
- CSP ile yapılan sözleşme, CSP tarafından yapılan ihlallerde sorumlulukları ve çözümleri açıkça kapsar.
- CSP, ASG'nin veri ve medya imha/atılma/temizlenme gereksinimlerine uyum sağlar.
- CSP, ASG verilerinin ASG'ye geri dönüşünü destekler.
- CSP ve ASG sorumlulukları belirlenecek ve uygun şekilde uygulanacaktır. Örneğin, hangi Bilgi Güvenliği kontrollerinin CSP tarafından yönetildiği ve hangilerinin ASG tarafından yönetildiği belirlenecektir.
- Bulut hizmetlerinin kullanımında minimal veya hiç iş etkisi olmadan göçü kapsayan çıkış/transfer stratejisi uygulanacaktır.
- CSP'nin teknik altyapısında (yer değişikliği, yeniden yapılandırma, yazılım veya donanım değişiklikleri) herhangi bir değişiklik önceden ASG'ye bildirilecek ve Bulut Hizmeti teslimatı etkilenmeyecektir.

5.24. Bilgi Güvenliği Olay Yönetimi Planlaması ve Hazırlığı

ASG yönetimi, Bilgi Güvenliği Olaylarına hızlı, etkili, tutarlı ve düzenli bir yanıt sağlamak için olay yönetim sürecini ve sorumluluklarını tanımlayacaktır. ASG, Hazırlık aşamasında aşağıdaki adımları sağlayacaktır:

- Çeşitli olaylara yanıt verecek Bilgisayar Güvenliği Olay Müdahale Ekibi (CSIRT) oluşturulması
- Tüm güvenlik olaylarının potansiyel bir olay için analiz edilmesi
- Bilgi Güvenliği Olaylarının olayın ciddiyetine göre daha fazla sınıflandırılması
- Farklı türdeki güvenlik olaylarına/olaylarına yanıt vermek için çalışma kılavuzlarının hazırlanması ve sürdürülmesi
- Tüm çalışanlar ve satıcı personeli tarafından gözlemlenen veya şüphelenilen bilgi güvenliği olaylarının/olaylarının derhal rapor edilmesi
- Ortamdaki olası saldırı senaryolarını proaktif olarak araştırmak
- BT güvenlik olayları için potansiyel senaryoların bir listesinin tutulması
- Hazırlık durumunu kontrol etmek ve roller ve sorumluluklar konusunda netlik sağlamak için BT operasyon ekibi ve iş operasyon ekibi ile senaryoları gözden geçirmek

Siber Güvenlik Kriz Yönetim Planı'na başvurun.

5.25. Bilgi Güvenliği Olaylarına İlişkin Değerlendirme ve Karar

ASG güvenlik operasyon ekibi, bilgi güvenliği olaylarını analiz ederek olayları sınıflandıracaktır. Olayların sınıflandırılması ve önceliklendirilmesi, olayın etkisini ve kapsamını belirlemeye yardımcı olabilir.

Değerlendirme sonuçları ve alınan kararlar, gelecekteki referans ve doğrulama için ayrıntılı olarak kaydedilmelidir.

5.26. Bilgi Güvenliği Olaylarına Müdahale

Bilgi güvenliği olaylarına aşağıdaki adımlara uygun olarak yanıt verilmelidir:

a. Tanımlama

- SOC ekibi veya BT yardım masası, en yüksek önceliği belirler ve bunu e-posta veya mevcut en etkili işbirliği platformu aracılığıyla Siber ve BT Güvenlik ekibine iletir.
- Siber ve BT güvenlik ekibi üyesi, özellikle Altyapı Lideri, CIO ve Uygulama Lideri (uygulanabilir ise) ile CSIRT ekibi üyeleriyle derhal bir toplantı veya telekonferans çağrısı yapar ve her ekip üyesinin eylem planı ve sorumluluklarını tartışır.
- Soruşturma: Bir olay izleme kaydı oluşturulur. Olayın etkisini ve ortamda yayılmasını anlamak için ilk analiz yapılır.

b. Kontrol ve Ortadan Kaldırma

- Olayın yayılmasını durdurmak ve hasarı en aza indirmek için uygun adımları belirleyin ve güvenlik olayına ilişkin delilleri koruyun. Olay hemen tamamen çözülemezse, mümkün olan yerlerde uygun alternatif çözümler uygulanmalıdır. Olay yanıtı ve kapanışı, mevcut altyapı, uygulamalar, ağ ve biyomedikal cihazlarda farklı değişiklikler gerektirebilir.
- ISMS (Bilgi Güvenliği Yönetim Sistemi) kapsamında tüm ilgili prosedürlerin ve eylemlerin, gerekli onaylar ve iletişim dahil olmak üzere, takip edilmesini sağlayın. Eylemler yama uygulama, kısıtlı kullanım, sistem veya uygulamanın izole edilmesi gibi adımları içerebilir. Biyomedikal cihazlar söz konusu olduğunda, önerilen eylemin güvenlik açısından bir risk oluşturmamasına özellikle dikkat edilmelidir.
- Bir olay kontrol altına alındıktan sonra, olayın bileşenlerini ortadan kaldırmak için yok etme işlemi gerekebilir. Yok etme sırasında, kuruluş içinde etkilenen tüm ana bilgisayarların belirlenmesi ve düzeltilmesi önemlidir.
- Kurtarma: Kurtarma aşamasında, sistemler normal işletime geri yüklenir, sistemlerin normal çalıştığı doğrulanır ve (uygulanabilir ise) benzer olayları önlemek için zafiyetler giderilir.
- ASG'nin fidye talebiyle karşı karşıya kaldığı durumlarda, ASG fidye müzakeresi yapmaz ve/veya fidye ödemez. Veri ve operasyonların geri yüklenmesi için müzakere yapmadan çözüm yolları mevcut olmalıdır.

5.27. Bilgi Güvenliği Olaylarından Öğrenme

ASG, tüm bilgi güvenliği olaylarının değerlendirilmesinden elde edilen bilgiler için bir bilgi tabanı oluşturacaktır. Bu bilgi tabanı, olay yönetimi için başvuru kaynağı olarak ve bilgi güvenliği olaylarından öğrenme için bir öğrenme kaynağı olarak kullanılacaktır. Öğrenilen derslere dayalı olarak iyileştirme alanlarına yönelik takip eden geliştirmeler yapılacak ve yüksek erişilebilirlik ve süreklilik gibi iyileştirmeler sağlanacaktır.

Tüm rapor edilen bilgi güvenliği olayları ve ihlallerine ilişkin bilgiler, üç (3) yıl süreyle saklanmalıdır.

5.28. Kanıtların Toplanması

Kanıtlar, ASG disiplin işlemine göre, bilgi güvenliği olayını takip eden herhangi bir kişi veya kuruluşa karşı izlenecek herhangi bir eylemi desteklemek amacıyla toplanacak, korunacak ve ilgili fonksiyonla paylaşılacaktır.

Bilgi güvenliği olaylarının soruşturması sırasında gerektiğinde kanıt toplamak için uygun adli yöntemler kullanılabilir olmalıdır.

5.29. Kesinti Süresinde Bilgi Güvenliği

ASG, kritik iş sürekliliğini sağlamak veya geri yüklemek için siber güvenlik kriz yönetim planının geliştirilmesini, uygulanmasını, test edilmesini ve gözden geçirilmesini sağlayacaktır. Bilgi güvenliği, gereken düzeyde ve gereken zaman çerçevelerinde geri yüklenecektir.

Lütfen **Siber Güvenlik Kriz Yönetim Planı** ve **İş Sürekliliği Yönetimi Politikası**'na başvurun.

5.30. İş sürekliliği için ICT Hazırlığı

İş sürekliliği hedef ve gereksinimlerine dayalı olarak, ASG'nın organizasyon bilgi varlıklarının kesinti süresince kullanılabilirliğini sağlamak amacıyla ICT hazırlık planı hazırlanacak, uygulanacak ve test edilecektir. Her önceliklendirilmiş ICT bileşeninin RTO (Gerçekleşme Zamanı Hedefi) ve RPO (Gerçekleşme Noktası Hedefi) belgelenerek İş Etki Analizi yapılacaktır.

Lütfen **İş Sürekliliği Yönetimi Politikası** ve **Teknoloji Güvenlik Risk Yönetimi Politikası**'na başvurun.

5.31. Hukuki, Yasal, Düzenleyici ve Sözleşmeye Dayalı Gerekliliklerin Belirlenmesi

Bilgi güvenliği ile ilgili yasal, kanuni, düzenleyici veya sözleşmeye dayalı yükümlülük ihlallerini önlemek için aşağıdaki önlemler uygulanmalıdır:

- Uygulanabilir yasal ve sözleşme gerekliliklerinin belirlenmesi: Hukuki fonksiyon, işletme faaliyetlerini düzenleyen ilgili yasaları, düzenlemeleri ve fikri mülkiyet haklarını belirlemelidir. Bunlar yılda bir kez veya yasal, düzenleyici veya sözleşme yükümlülüklerinde değişiklik olduğunda gözden geçirilmelidir.
- İlgili yasal, kanuni, düzenleyici yaklaşımların açıkça belirlenmesi ve belgelenmesi: Bu gereklilikler, organizasyonun her bir bilgi sistemi için açıkça belirlenmeli, belgelenmeli ve düzenli olarak güncellenmelidir.
- Kriptografik kontrollerin düzenlenmesi: Kriptografik kontroller, tüm ilgili anlaşmalara, yasalara ve düzenlemelere uygun olmalıdır. Örneğin, ödeme kartı verilerini korumak için PCI Veri Güvenliği Standartları'na uymak önemlidir. Ayrıca, geçerli olduğu durumlarda kriptografik teknolojiler veya kullanım gereksinimleri ile ilgili sınırlarda ithalat/ihracat yasalarına referans yapılmış olmalıdır.

5.32. Fikri Mülkiyet Hakları

. ASG yönetimi, ASG içinde rekabet eden çıkarları tanıyarak ve dengeleyerek maksimum koruma ve gerçekleşmeyi sağlamalıdır. Fikri mülkiyetin sahiplik ve özel yazılım ürünlerinin kullanımıyla ilgili yasal, düzenleyici ve sözleşmeye dayalı hükümlerin uygun şekilde uygulandığından emin olmak için aşağıdaki prosedürler takip edilmelidir:

- Fikri mülkiyet hakları çerçevesinde yazılım ve bilgi ürünlerinin meşru kullanımı için yönergeler yayımlanacaktır.
- Yazılımın yalnızca bilinen ve saygın kaynaklardan satın alınması sağlanarak kopya hakkı ihlalleri önlenmelidir.
- Varlık kayıtları yeterli bir şekilde tutulmalı ve tüm varlıkların fikri haklar koruma gereksinimleri belirlenmelidir.
- Lisans sahipliği, ana diskler, kılavuzlar vb. kanıtları ve lisansların tutulması sağlanmalıdır.
- Onaylanan kullanıcı sayısının maksimum sınırının aşılmamasını sağlamak için kontroller uygulanmalıdır.
- Yüklü ürünlerin ve yazılımların yalnızca lisanslı olduğunu kontrol etmek için incelemeler yapılmalıdır.
- Bilgi imha/devir stratejisi sağlanmalıdır.

a. Patent, telif hakkı ve diğer fikri mülkiyet haklarının devri: ASG çalışanları, ASG tarafından türetilen veya geliştirilen patentler, telif hakları, icatlar veya diğer fikri mülkiyet haklarında ASG'ye münhasır haklar tanırlar.

b. Bilgisayar programları ve dokümantasyonun mülkiyet hakları: Belirli yazılı yazışmalar olmaksızın, ASG'nın yararı için çalışanlar veya taşeronlar tarafından oluşturulan veya sağlanan tüm programlar ve dokümantasyonlar ASG'nın mülkiyetindedir.

c. Bilgi sistemleri dosyaları ve iletilen mesajların yasal mülkiyeti: ASG, bilgisayar ve ağ sistemlerinde depolanan tüm dosyaların içeriğinin ve bu sistemler aracılığıyla iletilen tüm mesajların yasal mülkiyetine sahiptir. ASG, gerçek iş gereği olduğunda önceden bildirim yapmaksızın bu bilgilere erişim hakkını saklı tutar.

d. Bilgi Kaynaklarına Atıf: ASG çalışanları, ASG amaçları için kullanılan bilgi kaynaklarını her zaman doğru şekilde tanıtmalıdır.

e. Fikri mülkiyet atama etiketleri: ASG web sitesinin genel alanına veya elektronik bülten tahtası sistemine bilgi sunan tüm kullanıcılar, bu bilginin düzenlenmesine, kopyalanmasına, yeniden yayımlanmasına ve dağıtılmasına ilişkin hakları ASG'ye verirler. Bilgiyi sunan kullanıcının dışında başkaları bu bilgi için telif hakkına veya başka haklara sahipse, kullanıcı bu bilginin sunulduğu sırada bu durumu belirtmelidir. Bu tür bir bildirim yapılmadığında, bilginin başka haklara sahip olmadığı veya kullanıcı tarafından talep edilmediği anlamına gelir.

f. Üçüncü tarafların telif haklarını ihlal eden e-posta mesajları veya ekleri yasaktır: Tüm çalışanlar, yasal olmayan veya üçüncü tarafların telif hakkı veya diğer fikri haklarını ihlal eden e-posta mesajlarını veya eklerini göndermek veya iletmekten kaçınmalıdır.

5.33. Kayıtların Korunması

İlgili iş, yasal ve düzenleyici gereksinimler, "Restricted" (Kısıtlı), "Confidential" (Gizli) veya "Secret" (Çok Gizli) olarak işaretlenen bilgilerin depolanması için belirlenip belgelenmelidir. PII (Kişisel Tanımlama Bilgisi) ve PHI (Korunan Sağlık Bilgisi) tanımlaması Veri Koruma Politikası'na göre yapılmalıdır.

Kurumsal kayıtlar, kaybı, imhası veya sahteciliği önlemek için güvenli bir şekilde korunmalı ve depolanmalıdır. Bu kayıtların saklama süresi belirlenmeli ve kaydedilmelidir. İlgili fonksiyon başkanları, hasta verileri, yedekleme, log depolama, mali kayıtlar vb. gibi kurumsal kayıtların yasal, düzenleyici ve sözleşmeye dayalı gereksinimlerle ve veri koruma politikası doğrultusunda saklanmasını sağlamalıdır.

İş, yasal ve/veya düzenleyici amaçlar için artık gerekli olmayan veriler güvenli bir şekilde imha edilmelidir. Olay bildirimi, adli inceleme, mali kayıtlar gibi hassas bilgiler, ilgili yasalara ve düzenlemelere uygun olarak ve uygun yetkilendirmelerden sonra hükümet kurumlarıyla belirlenen zaman çerçevesinde paylaşılmalıdır.

5.34. Kişisel Tanımlanabilir Bilgilerin (PII) Gizliliği

Bu kontrol **ASG Kişisel Veri Koruma Politikası** kapsamında ele alınacaktır.

5.35. Bilgi Güvenliğinin Bağımsız İncelemesi

Bilgi güvenliği yönetim sisteminin bağımsız incelemeleri ve denetimleri, planlanan aralıklarla en az yılda bir kez veya önemli değişiklikler olduğunda bilgi sistemleri sahibinin onayı ile gerçekleştirilecektir. Yapılan incelemelerin sonuçları ve yapılan düzeltici işlemler kaydedilecek ve bu kayıtlar korunacaktır.

5.36. Bilgi Güvenliği İçin Politikalar, Kurallar ve Standartlara Uygunluk

ASG, bilgi güvenliği politikasına uygun olarak bilgi güvenliği uyumluluğu ve güvence faaliyetlerini gerçekleştirecektir. Bu politikaya kasıtlı olarak uymama ciddi bir şekilde ele alınacak ve departman veya birey üzerinde yaptırım uygulanabilir.

İlgili fonksiyon yöneticileri, ASG Bilgi Güvenliği Politikası ve ilgili prosedürlerin, standartların ve yönergelerin uygulandığından emin olacaklar ve uyumluluk gereksinimlerini karşılamak için fonksiyonlarındaki her güvenlik politikası ve standardına karşı en az yıllık bir kez anlaşmaya varılan prosedürlere göre uyumluluk kontrolleri yapacaklardır. Herhangi bir uyumsuzluk durumunda:

- Uyumsuzluğun nedenleri belirlenecek,
- Aynı durumun tekrarlanmaması için gerekli önlemler değerlendirilecek,
- Uygun düzeltici işlem belirlenecek ve uygulanacaktır,
- Yapılan düzeltici işlemin gözden geçirilmesi yapılacaktır.

Teknik uyumluluk kontrolleri periyodik sıklıkta manuel olarak veya otomatik araçlarla yardım alınarak yapılacaktır. Teknik uyumluluk kontrolleri, tanımlanan sıklıkta (en az yılda bir kez) veya sistemde önemli bir değişiklik olduğunda kritik sistemleri kapsayacak şekilde penetrasyon testleri ve zayıflık değerlendirmelerini içerecektir. Bu kontroller, bu amaçla özel olarak sözleşme yapılmış bağımsız uzmanlar veya iç denetim ekibi tarafından gerçekleştirilebilir.

5.37. Belgelendirilmiş İşletim Prosedürü

ASG, bilgi sistemlerinin doğru ve güvenli bir şekilde işlenmesi için standart işletim prosedürlerinin belgelendirilmesini, ilgili fonksiyon yöneticilerinin onayını almasını ve uygun personel ile yüklenicilere

sunulmasını sağlayacaktır. Belgenin detay seviyesi, işlenen bilginin önem düzeyi ve ilgili operasyonların karmaşıklığı ile uyumlu olacaktır.

6. Kişi Kontrolü

Bu bölüm, ASG'nin ISO 27001:2022'ye uygun olarak benimsediği insan kontrolünü tanımlar. Bu bölümdeki kontrollerle ilgili herhangi bir değişiklik, başlangıç versiyonundan sonra aşağıdaki tabloda belgelendirilecek ve ilgili etkinlik tarihleriyle birlikte gösterilecektir.

Version	Relevant Control	Change Effective Date	Description of changes
1.0	NA	NA	Initial version

6.1. Tarama

İşe alım için tüm adayların geçmiş doğrulama kontrolleri, ilgili yasalar, düzenlemeler ve etik kurallar doğrultusunda ve erişilecek bilginin sınıflandırması ve algılanan risklerle orantılı olarak yapılmalıdır. Kontroller, kimlik kontrolü, önceki iş geçmişi kontrolü, akademik ve mesleki nitelik kontrolü ve gerektiğinde adli sicil kontrolünü içerebilir. Tüm çalışanlar ve yükleniciler, göz önünde bulundurulduklarını roller için uygun olmalı ve sorumluluklarını anlamalıdır. Organizasyon içinde pozisyon için düşünülen tüm adayların bilgileri, ASG Veri Koruma Politikası'na uygun olarak toplanmalı ve işlenmelidir.

6.2. İşe Alım Şartları ve Koşulları

ASG, işe alım için işveren ve yüklenici tarafından imzalanan Şartlar ve Koşulların, organizasyonun bilgi güvenliği gereksinimlerini yansıttığından emin olacaktır. Bu gereksinimler arasında, herhangi bir izinsiz açıklama, hırsızlık, değiştirme ve/veya yok etme durumunda sorumlu tutulacak olan gizlilik sözleşmesi (gizlilik anlaşması) imzalanması bulunmaktadır. İşten ayrıldıktan sonra dahi bilgi güvenliği ve ilgili yükümlülükler için sorumluluklar yer almalıdır.

6.3. Bilgi Güvenliği Farkındalık Eğitimi

Organizasyonun tüm çalışanları ve gerektiğinde yükleniciler, işlevlerine uygun olarak uygun güvenlik farkındalık eğitimi ve periyodik güncellemeler ile organizasyon politikaları ve prosedürlerine yönelik eğitim almalıdır. Yeni katılanlar için siber güvenlik uygulamaları, bilgi güvenliği farkındalık programının bir parçası olmalıdır. Tüm kullanıcılara periyodik yenileme eğitimleri ve yeni tehditlerle ilgili tavsiyeler sağlanmalıdır.

Bilgi güvenliği farkındalık ve eğitiminin periyodik değerlendirmeleri, tüm çalışanların ve ilgili yüklenicilerin güvenlik eğitimlerini tamamladığından ve eğitim içeriğinin gerektiğinde gözden geçirildiğinden emin olmak için yapılmalıdır. Bu güvenlik eğitimlerinin sıklığı en az yılda bir kez olmalıdır. Eğitimin kayıtları tutulmalı ve denetim için hazır olmalıdır.

Güvenlik Eğitim modülü, güncel güvenlik trendleri, geri bildirimler ve alınan önerilere dayanarak Grup COE tarafından güncellenmelidir.

6.4. Disiplin Süreci

Bilgi Güvenliği Fonksiyonu politikalarına aykırılıklar veya sapmalar herhangi bir yasal işleme yol açabilir ve tüm kullanıcı haklarını askıya alabilir. Soruşturmalar tamamlandıktan sonra, herhangi bir çalışan, yüklenici veya danışmanın herhangi bir politikayı ihlal ettiği tespit edilirse, disiplin / düzeltici işlem alınmalıdır. Bu disiplin prosedürleri, adil muamele sağlamak için bir rehber olarak hareket etmelidir:

- Danışmanlık
- Uyarı
- Geçici olarak askıya alma / sonlandırma / çıkarma

Tüm disiplin işlemleri yukarıdaki sırayı takip etmez. Bilgi ve Bilgi Varlıklarının Gizliliği, Bütünlüğü ve Erişilebilirliğini engelleyen daha ciddi durumlarda, çalışan, yüklenici veya danışman derhal askıya alınabilir veya işten çıkarılabilir ve üçüncü taraf katılımları için uygun önlemler alınabilir.

İhlallerin ciddiyeti aşağıdaki gibi sınıflandırılır:

- Yüksek Ciddiyet - Bu tür ihlaller için olası cezalar danışmanlık veya uyarı olmadan çıkarma veya askıya alma içerebilir.
- Orta Ciddiyet - Bu tür ihlaller için olası cezalar uyarı ve tekrarlanan ihlal için çıkarma veya askıya almadır.
- Düşük Ciddiyet - Bu tür ihlaller için düzeltici işlem danışmanlık ile birlikte uyarıdır ve tekrar ihlal durumunda çıkarma veya askıya almadır.

Disiplin süreci, ihlalin doğası ve ciddiyeti ile işletmeye olan etkisi gibi faktörleri dikkate alacaktır. İhlalin ilk mi yoksa tekrar mı olduğu, ihlalciye yasal, iş ve yasal gereksinimler konusunda eğitim verilip verilmediği veya gerektiğinde diğer faktörler de dikkate alınacaktır. Disiplin süreci ayrıca, çalışanların ve yüklenicilerin bilgi güvenliği politikalarını ve prosedürlerini ihlal etmelerini önlemek için caydırıcı olarak kullanılacaktır.

Aşağıdaki eylemler, disiplin işlemlerine sebep olacak ihlaller olarak kabul edilir:

a. Yüksek Ciddiyetli İhlaller

- ASG bilgi sistemleri üzerinden gönderilen veya iletilen, genel bir insanın hakaret, cinsel içerikli veya kuruluşun imajını zarar verebilecek derecede aşağılayıcı bulabileceği mesajlar veya resimler. ASG sistemleri üzerinden gönderilen veya iletilen, ırk, cinsiyet, yaş, milliyet, cinsel yönelim, kaste, din, siyasi inanç veya engellilik temelinde rahatsız edici olabilecek mesajlar veya resimler.
- ASG Bilgi Sistemleri üzerinden yetkisiz erişim sağlama veya bu sistemlerin işleyişini herhangi bir şekilde bozma, değiştirme veya kesintiye uğratma. Parola, şifreleme anahtarı veya diğer erişim kontrol mekanizmalarını ele geçirme veya bu mekanizmalar aracılığıyla yetkisiz erişim sağlama girişiminde bulunma.
- Bilgi Teknolojisi Fonksiyonu Başkanı tarafından yazılı önceden onay almadan bilgi sistem kontrollerini test etme veya dahili kontrolleri tehlikeye atma girişiminde bulunma.
- Bilgi sistemlerindeki güvenlik açıklarını veya eksiklikleri kullanarak sistemleri veya bilgileri zarar vermek, yetkilendirildikleri kaynakların ötesinde kaynakları ele geçirmek, diğer kullanıcılardan kaynakları almak veya uygun yetki verilmemiş diğer sistemlere erişim sağlamak için girişimde bulunma.
- Bilgisayar virüsü, solucan, Truva atı ve benzeri adlarla bilinen, herhangi bir ASG bilgisayarına, ağına veya bilgiye zarar verebilecek veya erişimi engelleyebilecek şekilde tasarlanmış herhangi bir bilgisayar kodu yazma, üretme, derleme, kopyalama, toplama, yayma, yürütme veya girmeye çalışma.

- Bir kullanıcının kimliğini e-posta sistemine yazarak değiştirmek, gizlemek, bastırmak veya yerine koymak yasaktır. Mesaj veya yayınların veya gönderilerin içinde yer alan kullanıcı adı, elektronik posta adresi, kurumsal bağlantı ve ilgili bilgiler, mesaj veya gönderinin gerçek göndericisini yansıtmalıdır.

b. Orta Ciddiyetli İhlaller

- Kurumsal İletişim Fonksiyonu tarafından önceden onay almadan ASG hakkında medya reklamı, internet ana sayfası, elektronik panoya gönderi, elektronik yayın mesajı veya diğer herhangi bir halka açık temsil.
- Yasadışı veya üçüncü tarafların telif hakkı veya diğer fikri mülkiyet haklarını ihlal eden e-posta mesajları veya ekler gönderme veya iletilme.
- İç elektronik posta mesajlarında çalışanlar, müşteriler veya rakipler hakkında küfürlü, cinsel içerikli veya aşağılayıcı ifadeler kullanma.
- Yetkisiz yazılım indirme ve kurma.
- ASG iç bilgisayar ve iletişim sistemlerini (elektronik panolar, veritabanı yönetim sistemleri, elektronik posta olanakları, intranet siteleri vb.) ASG organizasyonel değişiklikleri veya iş politikası konularını tartışmak için açık bir forum olarak kullanma.
- Çok kullanıcılı bir sistemden mikrobilgisayara (PC) veya iş istasyonuna hassas ASG bilgileri indirme, bilgi sahibinden önce onay alınmadan.
- Bir kullanıcının özel olarak görevlendirilmediği sürece, başka bir kişiye ait elektronik posta hesabını göndermek veya almak için kullanma.
- Bilgisayar virüsü bulaşmasını fark edildikten hemen sonra tüm şüpheli durumları rapor etmeme.

c. Düşük Ciddiyetli İhlaller

- ASG bilgisayar sistemlerini kişisel amaçlar için kullanarak ASG'nin normal iş faaliyetlerine müdahale etme.
- İlgili bir fonksiyon yöneticisinin özel izni olmadan ASG bilgisayar ve iletişim sistemlerini kişisel amaçlar için kullanma.

6.5. İstihdamın Sonlandırılması veya Değiştirilmesinden Sonra Sorumluluklar

Organizasyonun bilgi güvenliği çıkarları, istihdam sonlandırıldığında geçerli kalmaya devam edecek şekilde tanımlanmalıdır.

- İstihdamın sonlandırılması veya değiştirilmesinden sonra geçerli kalan bilgi güvenliği sorumlulukları ve görevler, İK fonksiyonu tarafından ilgili çalışan veya yükleniciye bildirilmelidir.
- İK'dan onay alındıktan sonra, ilgili çalışanın fonksiyonu ve İK, Bilgi Teknolojisi fonksiyonunu bilgilendirmelidir. Ayrıca, istifanın ardından çalışanın orijinal erişim hakları askıya alınmalı veya kaldırılmalı, değişiklikten sonra IT fonksiyonu tarafından yeni erişim hakları verilmelidir. Lütfen bu politikanın 5.15 ve 5.18 numaralı kontrollerine başvurun.

- İK'dan onay alındıktan sonra, ilgili çalışanın fonksiyonu ve İK, Bilgi Teknolojisi fonksiyonunu bilgilendirmelidir. İstifa eden çalışanın orijinal erişim hakları askıya alınmalı veya kaldırılmalıdır. Lütfen bu politikanın 5.18 numaralı kontrolüne başvurun.

- Fonksiyon yöneticisi/delege, tüm bilgilerin uygun şekilde yedeklendiğinden ve iş prosedürlerinin kaybedilmesini önlemek için aktarıldığından emin olmalıdır.

- İşten ayrılan veya değişen çalışanların tüm bilgi varlıklarını iade etmeleri gerekmektedir. Lütfen bu politikanın 5.11 numaralı kontrolüne başvurun.

6.6. Gizlilik veya Gizlilik Sözleşmesi

Bilginin korunması için ASG'nin ihtiyaçlarını yansıtan gizlilik veya gizlilik sözleşmelerinin gereklilikleri tanımlanmalı ve sürdürülmelidir. Bu gereklilikler, anlaşma etkin süresini uygun şekilde kapsamalı ve iş ortamının, yasal ve düzenleyici gerekliliklerin ve sözleşmeli yükümlülüklerin değişmesi durumunda periyodik olarak veya gerektiğinde gözden geçirilmelidir. Tüm üçüncü taraflar, çalışanlar ve yükleniciler gizlilik sözleşmesi imzalamalı ve uygulamalıdır.

6.7. Uzaktan Çalışma

Yetkili çalışanlar ve üçüncü taraflar (müşteriler, tedarikçiler vb.), "kullanıcı tarafından yönetilen" bir hizmet olan VPN'leri kullanabilir. VPN ayrıcalıklarına sahip çalışanların ve üçüncü tarafların, iç ağa yetkisiz kullanıcıların erişmesine izin verilmediğinden emin olmaları gerekmektedir. VPN erişimi, çok faktörlü kimlik doğrulama ile yetkilendirilmelidir. Bilgi güvenliğini sağlamak için uygun güvenlik kontrolleri uygulanmalıdır:

- Erişim, ilgili ASG birimi için belirlenen yetkilendirme tarafından onaylandıktan sonra kullanıcılar için ihtiyaç duyulduğunda sağlanmalıdır. Uzaktan erişim kullanıcılarının yetenekleri, ihtiyaç duyulan temel bilgileri sınırlayarak kısıtlanmalıdır.

- VPN erişimi, tanımlı bir rol erişim matrisi referans alınarak belirli bir rol için sağlanmalıdır.

- VPN erişimi, istifa, rol değişikliği vb. durumlarında artık gerekli olmadığında sonlandırılmalıdır. Uzaktan çalışma gereksinimi sona erdiğinde yetki, erişim hakları ve ASG ekipmanının iadesi sağlanmalıdır.

- Erişim listesinin yıllık olarak gözden geçirilmesi gerekmektedir, herhangi bir yetkisiz erişimi doğrulamak ve bu tür hesapları devre dışı bırakmak için. Her bağlantının bir olay durumunda izlenebilirliğini sürdürmek için kaydedilmesi gerekmektedir. Bu günlüklerin izinsiz erişimine dikkat edilmelidir. Güvenlik duvarı ve VPN cihazlarının değiştirilemez kaydı, denetim izini güvenilirliğini artırır.

- VPN aracılığıyla dahil edilen tüm bilgi sistemlerinin, en son yama ve uç nokta güvenlik çözümü ile güncellendiğinden emin olunmalıdır, buna kişisel bilgisayarlar da dahildir.

- VPN sunucuları ve uygulamaları için güvenlikle ilgili en son stabil sürüm güncellemelerinin yapılması gerekmektedir.

a. Sanal özel ağların kurulumu için aşağıdaki yapılandırma en iyi uygulamaları takip edilmelidir:

- Çift (bölünmüş) tünel izni verilmez; yalnızca bir ağ bağlantısı izinlidir.

- VPN geçitleri, ağ işletim grupları tarafından kurulmalı ve yönetilmelidir.

- VPN bağlantı oturumu ve etkinlik dışı bırakma zaman aşımı gereklidir.

- Tüm VPN bağlantıları, yalnızca ASG iş kullanımına uygun olan yaygın ve endüstri tavsiye edilen protokoller üzerinden olmalıdır.
- Tüm VPN'ler (uzaktan erişim/site-to-site), bu politikanın 8.24 numaralı kontrolünde referans gösterilen önerilen şifreleme süitleri ile güvenli olmalıdır.
- Kurumsal sahip olmayan ekipman kullanıcıları, ekipmanın ASG'nin VPN ve Ağ politikalarına uygun olarak yapılandırılmasını sağlamalıdır.
- Aynı kullanıcı kimliğinden eşzamanlı giriş devre dışı bırakılmalıdır.

Lütfen ASG_012 Kendi Cihazını Getir Politikasına başvurun.

6.8. Bilgi Güvenliği Olay Bildirimi

a. Gereken Bilgi Güvenliği Olayı Bildirimi: Tüm şüpheli bilgi güvenliği olayları, mümkün olan en kısa sürede ülke içi ASG IT yardım masası veya IT destek personeli gibi mevcut ASG iç kanalları aracılığıyla ihbar edilmelidir. Şüpheli davranış ve olaylar, ASG bilgisayarlarının yetkisiz erişimi, kullanıcı bilgisayarının anormal davranışı (kötü amaçlı yazılım bulaşma şüphesi), kullanıcı tarafından alınan şüpheli e-postalar, kaybolan şirket cihazı vb. içerebilir.

b. Bilgi Güvenliği İhlalleri ve Olaylarının İçsel Bildirimi: ASG çalışanlarının, bilgi güvenliği ihlallerini ve olaylarını zamanında ihbar etme görevleri vardır, böylece zamanında iyileştirici önlemler alınabilir. Bu, **ASGBTBilgiGuvenligi@acibadem.com** adresi aracılığıyla **Bilgi Güvenliği** ekibine bildirilmelidir.

c. Merkezi Olay Bildirimi: Bilinen tüm zafiyetler, şüpheli veya bilinen ihlallerin yanı sıra, bilgi sahiplerine ilgili ASG bilgilerinin izinsiz açıklanması, Cyber & IT Security ekibine hızlı ve gizli bir şekilde bildirilmelidir.

Dış ASG'ye güvenlik ihlallerini bildirmek (harici denetçiler hariç) kesinlikle yasaktır. Güvenlik ihlallerini ASG dışındaki herhangi bir tarafa bildirmenin özel bir ihtiyacı olduğunda, bilgi sahiplerinden ve Bilgi Teknolojisi Fonksiyonu'ndan yazılı onay alınmalıdır ve gerektiğinde Hukuk Fonksiyonu ile istişare edilmelidir. Hassas/gizli bilgilerin harici taraflarla paylaşımı sırasında kayıtların tutulması gerekmektedir.

d. Bilgi Güvenliği Olayı Bildiriminin Müdahale Edilmesi: Herhangi bir şüpheli bilgi güvenliği olayını bildirmek için çaba gösteren bir personeli engelleme, önleme, engelleme veya caydırma girişiminde bulunmak kesinlikle yasaktır ve disiplin cezasına neden olur. Bilgi güvenliği olaylarını veya ihlallerini bildiren veya araştıran kişiye karşı herhangi bir türde geri dönüşüm de yasaktır ve disiplin cezasına neden olur.

e. Bilgisayar Sistem Saldırılarının Kamuya ve Kamu Kurumlarına Bildirilmesi: Bilgisayar sistemleri veya ağlarına karşı saldırıları yasal olarak açıklamak zorunda kalınmadıkça, ASG bu olayları kamuoyuna bildirmez, ayrıca bu olayları hükümet kurumlarına da açıklamaz. Tüm durumlarda, dış iletişim uygun kanaldan yapılmalıdır. Kişisel Verilerle İlgili herhangi bir olay (ASG kişisel veri koruma politikasına aykırı veya ilgili kişisel veri koruma / Gizlilik Kanunu geçerli ülkede) Veri Koruma Görevlisine bildirilmelidir. Bu bildirimler için zaman çizelgeleri geçerli yasal ve düzenleyici gerekliliklere göre olmalıdır.

f. Müşteri / Müşteri İletişimindeki Olay Bildirimi: Müşteri hizmeti sistemlerini etkileyen olaylar özellikle müşteri anlaşmalarıyla bağlı olan sistemler için, yalnızca belirlenen kişi / rol aracılığıyla anlaşılan hizmet düzeyi sürelerinde bildirilmelidir.

g. Şüpheli Kötü Amaçlı Yazılım Bulaşımının Hemen Bildirilmesi: Kötü amaçlı yazılımlar hızla yayılabilir ve bilgisayarlar ve veriler üzerinde ciddi zararları sınırlamak için en kısa sürede yok edilmeleri gerekir. Bu nedenle, çalışanlar kötü amaçlı yazılım bulaşımını **ASGBTBilgiGuvenligi@acibadem.com** üzerinden **Bilgi**

Güvenliği ekibine derhal bildirmelidirler. Bilinen bir bulaşmanın zamanında bildirilmemesi durumunda ve bir soruşturma, belirli çalışanların bulaşmadan haberdar olduğunu ortaya koyarsa, bu çalışanlar bu politikanın 6.4 numaralı kontrolüne göre disiplin cezasına tabi olacaktır.

h. Yazılım Arızalarının Bildirilmesi Gerekliliği: Güvenlik politikası ihlalleri ile ilişkili görünen tüm yazılım arızaları, derhal hat yönetimi veya bilgi sistemleri hizmet sağlayıcısına bildirilmelidir.

i. Yetkisiz Erişim Olayı Şüphelenildiğinde veya Algılandığında Yardım İsteme: Herhangi bir yetkisiz sistem erişimi şüphelenildiğinde veya bilindiğinde, ASG personelinin erişimi sonlandırmak için derhal harekete geçmesi gerekmektedir. Bu eylemler yetkisiz faaliyeti tamamen bastırmazsa, bilgi sistemleri yardım masasından hemen yardım istenmelidir.

j. Bildirme Prosedürleri: Bildirme Mekanizması, tüm ASG çalışanlarının kolaylığı için net ve tanımlanmış prosedürleri içermelidir:

- Bir olay, danışmanlar da dahil olmak üzere herhangi bir kişi tarafından tespit edilebilir ve Gecikmeden Olay raporlama kanalı aracılığıyla derhal rapor edilebilir. Ayrıca, bir olay, personel tarafından doğrudan doğruya en yakın yöneticiye de bildirilebilir.
- Olay bileti kaydedilmeli ve ilgili bilgi varlığı sahibine atanmalıdır.
- Bir olayı bildirirken aşağıdaki bilgileri kapsayan bir prosedür olmalıdır:
    - Olayın kısa açıklaması
    - Olayın Tarihi ve Saati
    - İlgili Sanat Eserleri - Kök Neden Analizi ve Düzeltici ve Önleyici Eylem Belirlemede yardımcı olacak, ekran mesajları, meydana gelen arıza vb. ile ilgili önemli bilgiler

k. Bilgi güvenliği olaylarının bildirilmesi için düşünülen diğer durumlar şunları içerebilir, ancak bunlarla sınırlı değildir:

- Bilgi gizliliği, bütünlüğü ve erişilebilirlik beklentilerinin ihlali
- Bilgi güvenliği politika ve prosedürlerine uyumsuzluk
- Fiziksel güvenlik düzenlemelerinin ihlali
- Kontrolsüz Sistem Değişiklikleri
- Erişim İhlalleri
- Yazılım ve donanım arızaları ve çeşitli diğer durumlar

7. Fiziksel Kontroller

Bu bölüm, ASG'nin ISO 27001:2022'ye uygun olarak benimsediği fiziksel kontrol önlemlerini tanımlar. Bu bölümdeki kontrollerle ilgili herhangi bir değişiklik, ilk sürümden sonra aşağıdaki tabloda belirtilen etkinlik tarihleri ile birlikte belgelendirilecektir.

Version	Relevant Control	Change Effective Date	Description of changes

1.0	NA	NA	Initial version

7.1. Fiziksel Güvenlik Çevresi

Birimlerin Tesisler işlevi, ASG'nin bilgi varlıklarının bulunduğu tüm ofis konumları, tesisler veya tesisler içinde belirlenmiş alanlar için fiziksel güvenlik çevresini tanımlamalı ve sürdürmelidir. Bilgi varlıklarının önemine uygun olarak, bu tür konumların ve tesislerin çevresinde fiziksel erişim kısıtlamaları uygulanmalıdır.

7.2. Fiziksel Giriş

- Yalnızca yetkili personelin Veri Merkezi (VM) ve Sunucu Odalarına erişimine izin vermek için uygun giriş kontrolleri uygulanmalıdır.
- VM ve Sunucu odalarına fiziksel erişim, yalnızca yetkili ASG personeli ve hizmet sağlayıcı personeli tarafından sağlanmalıdır.
- Erişim, ihtiyaç duyulduğunda önceden tanımlanmış ASG otoritesi tarafından onaylanmalıdır.
- Artık gerekli olmadığında erişim derhal iptal edilmelidir.
- İnsan Kaynakları listesi alındığında veya İK Çıkış İzin Formu tamamlandığında istifa eden personel ve/veya başka görevlere atanmış personelin erişimi derhal iptal edilmelidir.
- Erişim yalnızca benzersiz bireyler için verilmelidir.
- Sorumluluğu sürdürebilmek için genel kullanıcı erişimi kesinlikle yasaktır.
- Kimlik doğrulama ve tanımlama, kullanıcı kimlik kartları (fotoğraflı veya fotosuz) ve erişim kontrol sistemi üzerinden yapılmalıdır.
- Vendors, sistem yöneticileri veya mühendisler gibi yetkisiz personelin geçici erişimi için bildirim ve onay süreci bulunmalıdır.
- VM ve sunucu odalarındaki ziyaretçiler her zaman yetkili bir ASG çalışanı tarafından refakat edilmelidir.
- Tüm ziyaretçiler, kimlik bilgileri, varış zamanı ve eşlik eden personel bilgilerini içeren bir kayıtla DC'ye erişimden önce kayıt yaptırmalıdır. Ayrıca, ziyaretçi kaydında ayrılma zamanı da kaydedilmelidir.
- Ziyaretçiler, girişte varlıklarını beyan etmeleri istenmelidir. Kısıtlı varlıklar girişte depolanmalı ve bunlar bir kayıtta kaydedilmelidir.
- Fiziksel erişim için yetkili kullanıcı listesi en az yılda iki kez gözden geçirilmelidir.
- Ziyaretçi kaydı, IT işlevi tarafından belirlenmiş sıklıkta denetlenmelidir.
- Teslimat ve yükleme alanları gibi giriş noktaları ve yetkisiz kişilerin tesislere girmesine izin verebilecek diğer noktalar, yetkisiz erişimi önlemek için kontrol edilmeli, izlenmeli ve mümkünse bilgi işlem tesislerinden izole edilmelidir. Güvenlik görevlisi / ekibi, böyle personeli ofis içine almadan önce uygun giriş kartı vermelidir.

7.3. Ofis Odaları ve Tesislerin Güvenliği

Birimlerin Tesisler işlevi, ofislerin, odaların ve bilgi işlem tesislerinin terk edildiğinde kilitli olduğundan emin olmalıdır. Ofislerde, odalarda ve bilgi işlem tesislerinde kilitleme yapılabilecek dolaplar veya kasalar sağlanmalıdır. Kısıtlı alanlar dışarıdan görünmemelidir.

7.4. Fiziksel Güvenlik İzleme

Kapalı devre televizyon (CCTV) kameraları gibi gözetim araçları, sunucu odası ve DC girişini izlemek için kullanılmalıdır. Gözetim sistemi, yetkisiz erişimi önlemek için korunmalıdır; böylece video beslemesine yetkisiz erişim sağlanamaz veya sistem uzaktan devre dışı bırakılamaz.

ASG, personel ve kaydedilen video saklama süresi gibi veri ve PII koruma yasaları ve düzenlemeleri dikkate alınarak izleme ve kayıt mekanizmalarının kullanılmasını sağlamalıdır.

ASG Veri Koruma Politikasına Bakınız.

7.5. Fiziksel ve Çevresel Tehlikelere Karşı Koruma

ASG, sunucu odası ve DC'nin dışsal ve çevresel tehditlere karşı korunması için uygun donanımlar ve güvenlik kontrolleri ile donatılmasını sağlamalıdır. Maliyet-fayda yaklaşımına dayalı olarak riskin azaltılması için dayanıklılık kontrolleri uygulanmalıdır. İş uygulamalarını barındıran veya kritik iş operasyonlarını destekleyen tüm veri merkezleri ve sunucu odaları için daha yüksek dayanıklılık derecesi dikkate alınmalıdır.

- Bir DC içindeki sıcaklık ve nem gibi çevresel koşulların izlenmesi ve düzenlenmesi, çalışma süresi ve sistem güvenilirliğini sağlamada kritik önem taşır.
- Ortam koşullarındaki anormallikler, yönetimi zamanında anormalliği çözmek üzere hızlı bir şekilde bilgilendirmek için derhal yükseltilmelidir.
- Bir tam ölçek yangın meydana gelirse, DC ve sunucu odasında FM200 gibi gaz tabanlı yangın söndürme sistemleri gibi uygun yangın koruma ve bastırma sistemleri uygulanmalıdır. İş uygulamalarını barındırmayan sunucu odaları, sunucu odasında bulunan ekipmanlara yangın tehlikesi riskini azaltmada maliyet-fayda sağlayan diğer türlerde yangın söndürme sistemleri benimseyebilir.
- DC'de duman dedektörleri ve el tipi yangın söndürücüler, tesisin bir kısmına yangın yayılmasını sınırlamak için DC çevresindeki yangına dayanıklı bariyerler gibi pasif yangın koruma unsurları ile birlikte kurulmalıdır.
- Kutular, plastik, köpük, karton ve sunucu/ekipman tesis alanına girilmeden önce olası diğer parçalardan oluşan yanıcı malzemeler çıkarılmalıdır. Bu tür malzemelerin kaldırılması için bir sahneleme alanı belirlemek önerilir.
- Zarar görmesini önlemek için böcek ve haşere kontrol mekanizmaları bilgi sistem varlıklarına zarar vermekten kaçınmak için uygulanmalıdır. ASG, bilgi sistem varlıklarını içeren odalarda düzenli olarak böcek ilaçlaması yapmalıdır.
- Elektrik gücü, klima, yangın bastırma ve veri iletişimi gibi alanlarda yedeklilik ve hata toleransı değerlendirilmelidir.
- DC ve sunucu odası, su baskını nedeniyle oluşabilecek zararlardan korunmalıdır.
- Tesis işlevi, fiziksel güvenlik ve çevresel tehditlerle ilgili düzenli tatbikatları en az yılda bir kez yapmalıdır.

7.6. Güvenli Alanlarda Çalışma

Tüm işlevler, Tesisler işlevine, kısıtlı alanları tanımlamak ve bu alanlara kısıtlı erişimi önlemek için güvenlik kontrollerinin uygulanmasında yardımcı olmalıdır. Tesisler işlevi, aşağıdaki hususların sağlanmasını sağlamalıdır:

- Bu alanlarda uygun fiziksel erişim kontrolleri uygulanmalıdır.
- Çalışanlara kısıtlı alanlara erişim sağlanmalıdır.
- Acil durum prosedürleri hemen görünür veya erişilebilir olmalıdır.
- Kısıtlı alanlara giriş ve çıkış ile kısıtlı alanlara herhangi bir varlığın hareketi izlenmeli ve kaydedilmelidir.
- Kısıtlı alanlara içeri alınması yasak olan ekipman/cihazlar listesi, giriş noktalarında gösterilmelidir.
- Kısıtlı alanlara giren kişilerin üst araması yapılmalıdır.

7.7. Temiz Masa ve Temiz Ekran

ASG, yetkisiz erişimi, kaybı ve bilgi elektronik, kağıt belgeleri ve elektronik ortamda normal çalışma saatleri sırasında ve sonrasında önlemek için Boş Masa ve Boş Ekran kontrollerinin uygulanmasını sağlamalıdır:

a. Temiz Masa

- Çalışanlar, belgeler, yazışmalar, bilgisayar ortamları vb. gibi bilgi varlıklarını kullanılmadığı zamanlarda güvenli bir yerde, özellikle çalışma saatleri dışında, kilitli çekmece, kilitli dolaplar, yangına dayanıklı kasa vb. gibi yerlerde saklamalıdır.
- Herhangi bir Kısıtlı/Gizli/Bilgi, masa boş olduğunda ve iş gününün sonunda çekmecede kilitli bir şekilde saklanmalıdır.
- Kullanılmadığında veya gözetlenmediğinde Kısıtlı/Gizli/Bilgi içeren dosya dolapları kapatılıp kilitlenmelidir. Bu dolapların anahtarları yalnızca yetkili kullanıcılarla paylaşılmalı ve gözetlenmemelidir.
- Her katta veya belirli bir alan için kağıt parçalayıcı veya kilitli imha bidonu sağlanmalıdır. Çalışanlar, imha edilmesi gereken gizli belgeleri sadece bu bidonlara yerleştirmelidir.
- Kullanıldığında, kağıt, kopya veya faks çekildiğinde Kısıtlı/Gizli/Bilgi hemen yazıcılardan/fotokopi makinelerinden/faks makinelerinden silinmelidir.
- Yazıcıya erişim sınırlı olmalı ve erişim kontrolü bu politikanın 5.15 numaralı kontrolüne göre tanımlanan yetkili personele göre sağlanmalıdır. Yazıcının kullanımı, yalnızca orijinatörün yazıcıya gelip print almasını sağlamak için pin kod fonksiyonunu kullanarak olmalıdır.
- İlgili işlev yöneticileri, kendi işlevleri içinde masa temizleme ve ekran temizleme politika gereksinimlerine uyumu sağlamalıdır.

b. Temiz Ekran

- ASG bilgisayarları/bilgisayar terminali gözetim altında olmadığında oturum açık bırakılmamalıdır. Ayrıca, sistemler belirli bir süre hareketsizlikten sonra otomatik olarak kilitlenmelidir.

- Şifreler, bilgisayarın üzerine veya altına yapıştırılmış notlar halinde veya erişilebilir bir konumda yazılı olarak bırakılmamalıdır.
- Sistemler, işletme nedenleriyle açık bırakılması gerekmeyen durumlarda, tesisleri terk etmeden önce kapatılmalıdır.
- Kısıtlı/Gizli/Bilgi içeren beyaz tahtalar silinmelidir.

7.8. Ekipman Yerleşimi ve Koruma

Tüm ekipmanlar çevresel tehditlere ve yetkisiz erişime karşı korunmalıdır. Tesisler işlevi, ekipmanların uygun şekilde yerleştirildiğinden, etiketlendiğinden ve sürekli operasyonları için yeterli güvenlik kontrollerinin uygulandığından emin olmalıdır.

7.9. Taşınan Varlıkların Güvenliği

- Ekipman, bilgi varlığı, izin alınmadan dışarı taşınmamalıdır. ASG bilgi depolama ve işleme için kullanılan tesislerden herhangi bir ekipmanın bakım amacıyla dışarı taşınması durumunda, ekipman uygun şekilde korunmalıdır.
- Taşınabilir cihazlar (Dizüstü Bilgisayarlar, Tabletler vb.) taşıyan / yöneten her kullanıcı, ekipmanın güvenliğinden kendisi sorumludur.
- Ağ Cihazları erişim noktaları, dış duvarlar boyunca değil, ofis alanının içine doğru yerleştirilmelidir.
- Kuruluş dışındaki ekipmanlar belirli aralıklarla izlenmelidir.
- Ekipmanın kritikliğine dayanarak, ekipman dışında sigorta kapsamı düşünülebilir.
- Kuruluş dışına taşınan herhangi bir medya veya ekipman için, tesis işlevi tarafından tanımlanan yetkili personel tarafından imzalanmış geçerli bir geçiş kartı gereklidir.

7.10. Depolama Ortamı

ASG, çıkarılabilir medya kullanımını yasaklar. Çalışanlar, iş amaçları için çıkarılabilir medya kullanımı için İHÇ Çıkarım Yönetimi Kılavuzu'na göre istisna onayı almalıdır. ASG bilgilerini depolamak için çıkarılabilir medya (bantlar, çıkarılabilir HDD'ler, CD'ler, DVD'ler, USB, SD kartlar) kullanıyorsa, medya üzerindeki içeriği yetkisiz erişimden, kötüye kullanımdan ve bozulmadan korumak için yeterli koruma sağlanmalıdır.

Verilerin gizliliği veya bütünlüğü önemli ise, çıkarılabilir medyadaki verileri güvence altına almak için kriptografik teknikler kullanılmalıdır. Önemli verilerin birden fazla kopyası farklı medyalarda depolanmalıdır, bu da kazara veri hasarını veya kaybını daha da azaltır. Çıkarılabilir medyanın, sahibi, şifreleme ve seri numarası detayları gibi bilgilerle IT işlevi tarafından kaydedilmesi, veri kaybı olasılığını sınırlamak için hesaba katılmalıdır.

a. Medya İmhası: Medya artık gerekli olmadığında güvenli bir şekilde imha edilmelidir. Güvenli medya imhası için manyetik alan temizleme gibi yöntemler kullanılmalıdır. Gizli/Gizli medya, organizasyon içinde başka bir uygulama için kullanılmak üzere güvenli bir şekilde işlenmeli ve imha edilmelidir, örneğin yakma veya parçalama yoluyla. İmha, bölümler tarafından belirlenen yetkili kullanıcılar tarafından yapılmalıdır. Denetim izini korumak için gizli/secret medya imha işlemi kaydedilecektir.

b. Fiziksel medya transferi: Bilgi içeren medya, taşınma sırasında yetkisiz erişimden, kötüye kullanımdan veya bozulmadan korunmalıdır. Uygulanabilir durumlarda, medyanın organizasyondan çıkarılması için yetkilendirme gereklidir ve bu çıkarılmaların kaydı denetim izini korumak için saklanır.

7.11. Destekleyici Hizmetler

Ekipman, destekleyici hizmetlerdeki arızalar nedeniyle güç kayıplarından ve diğer kesintilerden korunmalıdır. Uygun güç yedekleme (kesintisiz güç kaynakları, batarya dizileri ve/veya dizel jeneratörler) uygun şekilde kurulmalıdır. Gerekirse, destekleyici hizmetlerdeki arızaları vurgulamak için bir alarm sistemi kurulmalıdır. Önleyici bakımın gözden geçirilmesi yetkilendirilmiş personel tarafından yapılmalıdır.

7.12. Kablo Güvenliği

Veri taşıyan veya bilgi hizmetlerini destekleyen güç ve telekomünikasyon ağları ve ağ kabloları, kesilme, müdahale veya hasara karşı korunmalıdır. Kabloların her iki ucu da hedef bilgi ile etiketlenmelidir.

7.13. Ekipman Bakımı

Ekipmanın sürekli kullanılabilirliğini ve bütünlüğünü sağlamak için ekipmanın doğru bir şekilde bakımı yapılmalıdır. Tüm bilgi sistemleri ekipmanı, uygun bakım talimatları ve özelliklerine göre bakım yapılmalıdır, herhangi bir onarım ve servis yalnızca nitelikli ve yetkili bakım personeli tarafından yapılmalıdır.

Tüm ekipmanların Yıllık Bakım Sözleşmeleri bakımının yapılması gereklidir. Önleyici Bakım, belirli bir frekansta ilgili işlev tarafından yapılacak ve gözden geçirilecektir. Ekipmanın bakım geçmişini takip etmek için gereken tüm kayıtların saklanması gereklidir.

7.14. Ekipmanın Güvenli İmha veya Yeniden Kullanımı

Depolama medyası içeren herhangi bir ekipmanın imha edilmeden önce tüm bilgi/veri ve lisanslı yazılımın kaldırılması veya güvenli bir şekilde üzerine yazılması gerekmektedir.

- Duyarlı bilgiler içeren medyanın dış kaynaklı imhası, hizmet sağlayıcı "İmha Sertifikası" sağlamalıdır

8. Teknolojik Kontroller

Bu bölüm, ASG'nin ISO 27001:2022'ye uygun olarak benimsediği teknolojik kontrol önlemlerini tanımlar. Bu bölümdeki kontrollerle ilgili herhangi bir değişiklik, ilk sürümden sonra aşağıdaki tabloda belirtilen etkinlik tarihleri ile birlikte belgelendirilecektir.

.

Version	Relevant Control	Change Effective Date	Description of changes
1.0	NA	NA	Initial version

8.1. Kullanıcı Uç Nokta Cihazları

ASG, organizasyon veri uç nokta cihazları (örneğin masaüstü ve dizüstü bilgisayarlar, mobil cihazlar, tabletler vb.) için aşağıdaki güvenlik önlemlerini sağlamak için aşağıdaki adımları uygulamayı taahhüt eder:

- Tüm kullanıcı cihazları güvenli bir şekilde yapılandırılmalıdır. Cihaz, sadece yetkili kişilerin erişimini sınırlamak üzere yapılandırılmalıdır.
- Kullanıcılar, ihtiyaç duydukları ölçüde uç nokta cihazları üzerinde haklara sahip olmalıdır. Bu politikanın 5.15 numaralı kontrolüne bakınız.
- Kullanıcılar, yazılım yüklemeleri için yetkilendirilmemelidir. Bu, izinsiz yazılım ve kötü amaçlı programların kurulmasını önlemek içindir.
- Tüm uç nokta cihazlarına yüklenen yazılımlar, güvenlik açıkları için yamalanmalıdır. İşletim sistemleri ve uygulama yazılımları, en son güvenlik yamalarıyla güncel tutulmalıdır. Kullanıcılar, tanımlanan güvenlik açıklarının giderilmesi için gereken yeniden başlatma işlemleri de dahil olmak üzere IT ve Siber Güvenlik ekiplerine tam işbirliği ve destek sağlamalıdır.
- Tüm organizasyon sağlanan uç nokta bilgisayarları, IT tarafından önerilen uç nokta güvenlik çözümü ile donatılmalıdır. Uç nokta güvenlik çözümü, düzenli taramalar/etkinlik/davranış/deseni vb. ile zararlı yazılımları tespit edebilmelidir.
- Üçüncü taraf kullanıcılar, üçüncü taraf sağlanan uç kullanıcı cihazlarında itibarlı bir uç nokta güvenlik çözümü kullanmalı veya ASG'nin tercih ettiği çözümün bu cihazlara dağıtılmasına izin vermelidir.
- Mümkün olduğunda, kullanıcıya veri yedekleme imkanı sağlanmalıdır ve kullanıcılar düzenli olarak verilerini yedeklemeleri konusunda eğitilmelidir.
- Tüm uç nokta cihazları için tam disk şifrelemesi önerilmektedir.
- Kullanıcılar, mobil ve bilgisayarlarını gözetimsiz bırakmadan önce kilitli tutmaları veya kablo kilidi kullanmaları konusunda eğitilmelidir.
- Uç kullanıcı cihazları için güvenilmeyen ağların kullanımından kaçınılmalıdır.
- Uç nokta cihazlardaki tüm USB bağlantı noktaları devre dışı bırakılmalıdır.

Detaylar için: **ASG_012 Kendi Cihazını Getir Politikası**'na bakınız.

8.2. Ayrıcalıklı Erişim Hakları

ASG, bilgi sistemlerinde erişim ayrıcalıklarının atanmasının, kullanıcının rolüne uygun olarak yalnızca meşru iş amaçları için yapılacağını ve artık gerekli olmadığında geri alınacağını sağlamalıdır. Bilgi sistemlerinde kullanılan tüm ayrıcalık erişimleri denetim amaçları için kaydedilip korunmalıdır.

8.3. Bilgiye Erişim Kısıtlaması

Kullanıcıların ve destek personelinin bilgiye ve diğer ilişkili varlıklara erişimi, bu politikanın 5.15, 5.16 ve 5.18 numaralı kontrol ilkelerine uygun olarak kısıtlanmalıdır.

8.4. Kaynak Koda Erişim

ASG, program kaynak kodu ve ilişkili öğelere erişimin sınırlı yetkili kullanıcılara kısıtlanmasını sağlamalıdır. Program kaynak kodu ve ilişkili öğelerin güncellenmesi yalnızca yetkilendirme sonrasında yapılmalıdır. Program kaynak koduna yapılan tüm erişimler ve değişiklikler için bir denetim izi tutulmalıdır.

8.5. Güvenli Kimlik Doğrulama

ASG, oturum açma sürecinde sistem hakkında minimum bilginin açıklanmasını sağlayarak yetkisiz bir kullanıcıya gereksiz yardımların önlenmesini sağlamalıdır.

- Oturum açma başarısız olursa, hata mesajı hangi oturum açma bilgisinin yanlış olduğunu göstermemelidir.
- Uygulanabilir olduğu durumlarda, başarısız oturum açma denemelerinin sayısı sınırlandırılmalıdır.
- Parola girilirken görüntülenmemelidir.
- Oturum açma bilgileri açık metin olarak gönderilmemelidir.
- İşletim sistemleri ve uygulamalar oturum zaman aşımı ile donatılmalıdır.

8.6. Kapasite Yönetimi

Varlık sahibi, kaynakların, bilgi işleme varlıklarının kullanımının izlenmesini, ayarlanmasını ve gelecekteki kapasite gereksinimlerinin projeksiyonlarının yapılmasını sağlayarak gereken sistem performansını sağlamalıdır.

- Tüm kritik altyapı unsurları ve yazılımlar için kritik parametreler ve eşik değerler belirli aralıklarla izlenmeli ve gereken performans seviyelerini ve kullanılabilirliği sağlamak için sorunları belirten dedektif kontroller uygulanmalıdır.
- Kapasite gözden geçirme periyodu, altyapı unsurunun kritikliği, değiştirme süresi/maliyetleri ve izlenen parametreler dikkate alınarak tanımlanmalıdır.
- Kapasite planlaması, yeni iş ve sistem gereksinimlerini ve mevcut ve projeksiyon eğilimlerini göz önünde bulundurmalıdır.
- Kapasite yönetim belgesi (en azından kapsam dahilindeki sistemle ilgili ayrıntılar, eşik gereksinimleri, izleme, ayarlama vb. konuları içermelidir) varlık sahipleri tarafından hazırlanmalı ve gereken aralıklarla ancak en az yılda bir kez gözden geçirilmelidir.

8.7. Kötü Amaçlı Yazılımlara Karşı Koruma

ASG, uç nokta güvenlik kontrollerinin e-postalardan kötü amaçlı yükleri ve bağlantıları tespit edip kaldırmasını, bilinen saldırılarla ilgili konuları olan e-postaları engellemesini, kötü amaçlı URL'lere yapılan bağlantıları engellemesini tercihen otomatik olarak sağlamalıdır.

- Tüm iş istasyonları ve sunucuların uç nokta güvenlik çözümü uygulanmış olmalıdır.

- İmzalar/Defineler, politika önerileri OEM tarafından kullanıma sunulduğunda derhal güncellenmelidir.
- Ajanlar, motorlar vb. OEM tarafından önerilen bir sürüme yükseltilmeli ve minimum sürüm, mevcut en güncel sürümden en fazla iki sürüm öncesi olmalıdır. Dağıtılan çözüm veya çözümlerin kombinasyonu, sıfır gün saldırıları, dosyasız ve diğer karmaşık ve gelişmiş saldırılar gibi bilinen ve bilinmeyen saldırılarla başa çıkabilmelidir.
- Tüm tanımlar/politikalar/kurallar merkezi olarak güncellenmelidir.

Uç nokta güvenlik çözümü, düzenli taramalar/aktivite/davranış/pattern vb. yoluyla kötü amaçlı yazılımları tespit etme kapasitesine sahip olmalı ve imza ve imzasız tespit mekanizmalarını kullanmalıdır.

Kötü amaçlı yazılım tespit edildiğinde BT personeline ve ilgili alıcıya (ISO, BT Altyapı Yöneticisi, Sistem Sahibi vb.) bildirim sağlanmalıdır. Tüm bilgi sistemleri, özellikle kritik BT sistemi için sürekli olarak herhangi bir kötü amaçlı aktivite için izlenmelidir.

8.8. Teknik Güvenlik Açıklıklarının Yönetimi

ASG, kullanılan bilgi sistemlerinin teknik zafiyetlerine ilişkin bilgilerin üç aylık periyotlarla elde edilmesini ve organizasyonun bu tür zafiyetlere karşı maruz kalmasının değerlendirilip, ilişkili riskleri ele almak için uygun önlemlerin alınmasını sağlamalıdır.

- Tüm bilgi varlıkları için araç tabanlı zafiyet taramaları yapılmalıdır.
- Belirlenen sorunlar uygun şekilde kapatılmalıdır (konfigürasyonlar, yamalar vb.).
- Herhangi bir yama veya konfigürasyon sadece varlık sahibinin onayı ile uygulanmalıdır.
- Sistemin mevcut işlevselliği etkilemediğini doğrulamak için yeniden taranmalıdır.
- Zafiyetler için yama/çözüm uygulandıktan sonra, kapanışı doğrulamak için bir kontrol/zafiyet yeniden taraması yapılmalıdır.
- Kullanılan altyapı unsurları ve yazılımlardaki teknik zafiyetlere ilişkin zamanında bilgi, güvenilir kaynaklardan elde edilmelidir (örn. satıcı güvenlik danışmanlıklarına abone olarak).

Elde edilen zafiyet bilgileri, ASG altyapısına yönelik riski değerlendirmek için analiz edilmelidir. Aşağıdaki değerlendirme dikkate alınmalıdır:

- Zafiyetler şu kritiklik düzeylerine göre atanmalıdır:
    - **Kritik**: Bu zafiyet başarıyla istismar edilirse, ASG bilişim ortamının işlevselliğini etkileyebilir ve potansiyel olarak bozabilir. Zafiyeti düzeltmek için derhal takip edici bir eylem gereklidir.
    - **Yüksek**: Bu zafiyet başarıyla istismar edilirse, saldırganın bir kurbanın bilişim cihazına erişim olmadan kontrol kazanmasına olanak tanır ve ASG bilişim ortamının kullanılabilirliğine ciddi etkisi olabilir. Zafiyeti düzeltmek için hızlı bir takip eylemi gereklidir.
    - **Orta**: Bu zafiyet başarıyla istismar edilirse, yetkili olmayan bir saldırganın kontrol kazanmasına olanak tanır ve ASG bilişim ortamındaki hizmetleri kesintiye uğratabilir. Zafiyeti düzeltmek için bir takip eylemi gereklidir.

- **Düşük**: Bu zafiyet belirli ve olası olmayan bir durumda istismar edilebilir. Zafiyeti düzeltmek için diğer planlanmış bakım faaliyetleriyle birlikte bir takip eylemi tetiklenebilir.

- ASG bilgi sistemlerinin sistem kritikliği tanımlanmalıdır.
- İlişkili riskleri ele almak için uygun önlemler alınmalıdır. Zafiyet ele alınamıyorsa, riski azaltmak için kontroller uygulanmalıdır. ASG, zafiyetlerin ciddiyet sırasına göre ele alınmasını sağlamalıdır:
  - Zafiyetin ciddiyeti ASG ortamına göre bağlamsal olmalıdır.
  - Kritik zafiyetler derhal ele alınmalıdır.
  - Kritik ve Yüksek zafiyetlerin ele alınması 30 günü aşmamalıdır.
  - Orta zafiyetlerin ele alınması 90 günü aşmamalıdır.

Zafiyetin kapanışı yama dağıtımı gerektiriyorsa, yama aşağıdaki yama yönetim prosedürüne uygun olarak dağıtılmalıdır:

a. Güvenlik Yaması İzleme Danışmanlığı

- Yama yayınlarını izlemek için zafiyetler, etkilenen varlıklar ve konfigürasyonların listesini elde edin.
- Kullanılan ürün ve yazılımlara göre, Microsoft, Cisco vb. gibi önde gelen kaynaklardan güvenlik danışmanlıklarına abone olun.
- Tüm BT operasyon ekiplerine e-posta ile yama danışmanlığı yayınlayın. Danışmanlık, ciddiyet derecelendirmesi, yama açıklaması, yama ile ele alınan güvenlik zafiyetinin açıklaması, güvenlik zafiyetinin etkisi açıklaması, etkilenen yazılımlar ve sürümlerinin listesi, yama detayları için web sitesi bağlantısını içermelidir.

b. Etki Değerlendirmesi

- Güvenlik danışmanlığı için etkilenen sistemleri ve cihazları değerlendirin.
- Sunucu yamaları ve ağ cihazı yamaları mümkünse, üretim sistemine uygulamadan önce test sunucusuna/cihazına uygulanmalıdır.

c. Yamanın Dağıtımı

- Yama dağıtımı ASG değişim yönetim prosedürünü takip etmelidir. Yamalar, "Yama kritikliği derecelendirmesi"ne göre önceliklendirilmelidir.
- Tüm yamalar, zafiyetlerin istismar riskini azaltmak için makul bir zaman çerçevesinde kurulmalıdır. Güvenlik yamasının teknik veya operasyonel nedenlerle uygulanamayacağı değerlendirilirse, hafifletici önlemler veya geçici çözümler uygulanmalı ve sapma bildirilmelidir. Yamaların uygulanması için aşağıdaki zaman çizelgeleri takip edilmelidir:

Yama Seviyesi				
Cihaz sınıflandırması	Kritik	Yüksek	Orta	Düşük
Yayınlanma tarihinden itibaren yama yüklenme süresi (hafta)				

Internete açık cihaz	4 - 8	4 - 8	8-12	12-20
Dahili cihaz	8 –12	8 –12	12 –20	12 –20

Not: OEM tedarikçileri tarafından sağlanan uygulamalar için güvenlik yamaları/güncellemeler test edilmeli ve kullanıma sunulduğunda hemen kurulmalıdır. OEM tedarikçileri tarafından sağlanan işletim sistemleri için güvenlik yamaları/güncellemeler, çalıştırılan uygulamalarla uyumluluk ve etkileri açısından değerlendirilip, test edilmeli ve kullanıma sunulduğunda hemen kurulmalıdır.

d. Yama Yönetimi Raporlaması

- Son zafiyet taramaları temelinde zafiyet kapanış durumunu yeniden doğrulayın ve güvenlik yamalarının dağıtım durumunu IT Müdürü / vekiline aylık olarak raporlayın.

8.9. Konfigürasyon Yönetimi

ASG, BT sistemlerinin hedef operasyonel ortam (yerel veya bulut) için sertleştirme gereksinimlerini belirleyen konfigürasyon temel belgelerinin hazırlanmasını ve takip edilmesini sağlamalıdır. BT sistemleri, uygulanabilir olan herhangi bir tedarikçi tarafından sağlanan BT ürünlerini içerebilir, ancak bunlarla sınırlı değildir:

- Donanım, bilgisayar donanımı, ağ yazıcıları gibi.
- Yazılım, işletim sistemi (Windows, Solaris vb.), uygulama sunucusu, veritabanı sistemi gibi.
- Ağ ekipmanları, güvenlik duvarı, NIDS, NIPS, yönlendirici, yük dengeleyici gibi.
- Yönetim Platformları.

BT Altyapı ekipleri, Siber ve BT Güvenlik ekibi tarafından gözden geçirilen ASG'nin konfigürasyon temellerini belirleme ve yayınlama sorumluluğuna sahiptir. Temeller, aşağıdaki kaynaklar dahil olmak üzere, endüstri tarafından kabul edilen sistem ölçütlerine dayanarak geliştirilmelidir:

- İnternet Güvenlik Merkezi (“CIS”)
- Ulusal Standartlar ve Teknoloji Enstitüsü (“NIST”)
- SysAdmin Ağ Güvenliği Denetim Enstitüsü (“SANS”)

BT sistemlerinin konfigürasyonları, üretim ağına kurmadan veya etkinleştirmeden önce sertleştirilmelidir. Sistemin sahibi veya kontrolörü, aşağıdakilere göre konfigürasyonları değiştirmelidir:

- ASG'nin konfigürasyon temeli.
- Yukarıdakiler mevcut değilse, tedarikçi tarafından sağlanan ölçüt veya CIS, NIST veya SANS'ten ölçütler kullanılmalıdır.
- Yukarıdaki iki seçenek mevcut değilse, endüstri ölçütü veya en iyi uygulama seçilmeli ve seçilen ölçüt hakkında BT Güvenlik ekibi bilgilendirilmelidir.

Temel veya ölçütlerde önerilen ayarların, ürünün kullanılabilirliğini veya performansını olumsuz etkileyebileceği ve sahibinin gerektirdiği işlevle çelişebileceği durumlar olabilir. Bir ayar istisnasının kaçınılması gerektiğinde, istisna gerekçelendirilmelidir ve istisnanın gerekliliğini kanıtlamak için kanıt gereklidir. BT Güvenlik ekibi, herhangi bir ayar istisnasından haberdar edilmelidir.

8.10. Bilgi Silme

ASG, ilgili yasalar ve düzenlemelere uygun olarak hassas bilgilerin, özellikle Kişisel Tanımlanabilir Bilgilerin (PII), artık gerekli olmadığında silinmesini ve yetkisiz ifşayı önlemek için uygun yöntemlerin benimsenmesini sağlamalıdır. İş gereksinimleri göz önünde bulundurularak uygun silme yöntemi uygulanmalı ve silme işleminin sonucu kanıt olarak kaydedilmelidir. Detaylar için ASG Kişisel Verilerin Korunması Politikasına bakınız.

8.11. Veri Maskeleme

ASG, geçerli mevzuat, düzenlemeler ve standartlar gerektirdiğinde hassas bilgilerin, özellikle PII'nın uygun maskeleme teknikleri (maskeleme, şifreleme, tokenizasyon vb.) kullanılarak korunmasını sağlamalıdır. Detaylar için ASG Kişisel Verilerin Korunması Politikasına bakınız.

8.12. Veri Sızıntısı Önleme

Veri sızıntısı önleme önlemleri, hassas bilgileri işleyen, depolayan veya ileten sistemlere uygulanmalıdır. Mümkün olduğunda, bilgi sızıntısı kanalları iş gerekçesiyle izlenmeli ve sınırlandırılmalıdır. Hassas bilgilerin sızıntısını önlemek ve yetkisiz kullanıcılara ifşasını tespit etmek için önleyici/detektif önlemler uygulanmalıdır.

8.13. Bilgi Yedekleme

Bölüm BT fonksiyonu ve uygulanabilir yerlerde bilgi sistemi sahibi, bilginin ve bilgi sistemlerinin uygun şekilde yedeklenmesini ve yedekleme verilerini ve yedekleme ortamını korumak için gerekli kontrollerin uygulanmasını sağlama sorumluluğuna sahiptir.

- BT fonksiyonu, ilgili paydaşlarla birlikte iş fonksiyonları içindeki bilgilerin yedekleme ve geri yükleme gereksinimlerini belirlemelidir. Yedekleme prosedürü, gereken aralıklarla, ancak yılda en az bir kez gözden geçirilerek hazırlanmalıdır. Prosedür şunları içermelidir, ancak bunlarla sınırlı değildir:
    - Yedekleme alma ve geri yükleme sürecini test etme sıklığı.
    - Yedeklenecek veriler.
    - Yedekleme türü (artımlı, diferansiyel, tam).
    - Gerçek bir felaket durumunda geri yükleme talimatları.
    - Yedeklerin yasal, düzenleyici ve iş gereksinimlerine göre saklama süresi.
- Tüm uygulama ve işletim sistemi yazılımları, veriler (veritabanları dahil), sistem konfigürasyon dosyaları iş gereksinimlerine ve tedarikçi tarafından önerilen prosedürlere göre yedeklenmelidir.
- Kritik sunucular için çevrimiçi yedeklemeye ek olarak, çevrimdışı/air gap yedekleme düşünülmelidir.
- Fiziksel yedekleme ortamı açıkça tanımlanmalı, etiketlenmeli, kaydedilmeli, şifrelenmeli ve güvenli bir şekilde saklanmalıdır. Yedekleme ortamının yerinde saklanması yangına dayanıklı olmalıdır. Yedekleme ortamına erişim, "bilmesi gereken" esasına göre sınırlandırılmalıdır.

- Başarılı/başarısız yedekleme girişimleri, başarılı/başarısız geri yükleme girişimleri, yedekleme vb. izlemek için ilgili yedekleme kayıtları tutulmalıdır.

8.14. Bilgi İşleme Tesislerinin Yedekliliği

ASG, gerekli olduğu yerlerde, kritik bilgi işleme varlıklarının kullanılabilirliğini sağlamak için yedek bileşenlerin uygulanmasını sağlamalıdır. Yedek bilgi sistemleri, bir bileşenden diğerine geçişin istenildiği gibi çalıştığını doğrulamak için test edilmelidir. **İş Sürekliliği Yönetimi Politikasına** bakınız.

8.15. Günlük Tutma

Güvenlik kayıtları üretebilen tüm bilgi varlıkları, en az kritik altyapı cihazları, uygulamalar, yazılımlar ve yerel veya bulutta barındırılan SaaS uygulamaları, kayıtlarının yakalanması ve izlenmesi gerekmektedir. Tüm uygulamalar, işletim sistemleri, ağ bileşenleri ve veritabanları için denetim kayıtları etkinleştirilmelidir. Kayıtlar şu bilgileri içermelidir:

- Hangi etkinlik gerçekleştirildi?
- Etkinliği kim (kullanıcı) veya ne (hizmet vb.) gerçekleştirdi, etkinliğin nerede veya hangi sistemde gerçekleştirildiği (konu).
- Etkinlik ne zaman gerçekleştirildi?
- Etkinliği gerçekleştirmek için hangi araçlar kullanıldı?
- Etkinliğin durumu (başarı vs. başarısızlık), sonucu veya sonucu.

Diğer izlenmesi gereken eylemler, belirli risklere dayanarak belirlenmelidir. Sistem yöneticisi, sistem operatörü, yetkili kullanıcı etkinlikleri kaydedilmeli ve kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir. Kayıt bilgileri yetkisiz erişime, değişikliklere ve operasyonel sorunlara karşı korunmalıdır. Kayıtlara erişim "bilmesi gereken" esasına göre sağlanmalıdır ve kayıtlar en az 1 yıl saklanmalıdır.

8.16. İzleme Etkinlikleri

Kullanıcı etkinlikleri, istisnalar, hatalar ve bilgi güvenliği olaylarını kaydeden olay kayıtları izlenmelidir. Kayıtlar, merkezi toplama ve depolama için ilgili cihazda izlenecek şekilde yapılandırılmalı ve Güvenlik Operasyon Merkezi'ne (SOC) Güvenlik Bilgileri ve Olay Yönetimi (SIEM) analizi için gönderilmelidir.

- SOC analisti, şüpheli veya doğrulanmış güvenlik olayı fark ettiğinde rapor etmelidir.
- Kontrol 5.24'e göre olay müdahalesi başlatılmalıdır.
- Yetkili personel tarafından yanlış pozitifleri doğrulayarak izleme etkinliğinin etkinliğini kontrol etmek için yarı yıllık bir inceleme yapılmalıdır.

8.17. Saat Senkronizasyonu

Tüm ilgili bilgi işleme sistemlerinin saatleri, uygulanabilir olduğu durumlarda, merkezi bir Ağ Zaman Protokolü (NTP) ile senkronize edilmelidir. Tarih/saat formatının doğru yorumlanması sağlanmalıdır. Format, tüm sunucular ve ağ cihazları arasında aynı olmalıdır.

8.18. Ayrıcalıklı Yardımcı Programların Kullanımı

Bilgi sistemi ve uygulama kontrollerini geçersiz kılabilecek yardımcı programların kullanımı sınırlandırılmalı ve sıkı bir şekilde kontrol edilmelidir. Sorun giderme amacıyla bu yardımcı programları kullanma ihtiyacı varsa, sunucuların ve ağ cihazlarının yöneticileri, bu yardımcı programları kullanarak gerçekleştirilen etkinliklerin kaydedilip periyodik olarak gözden geçirildiğinden, yetkili bir etkinlik için etkinleştirildiğinden ve devre dışı bırakıldığından emin olmalıdır.

8.19. İşletim Sistemlerine Yazılım Yükleme

ASG, bilgi işleme sistemlerine yazılım yükleme işlemlerini sınırlandırmak için yeterli kontrollerin uygulanmasını sağlamalıdır. Yeni yazılım yükleme yetkisi yalnızca sistem yöneticisi/BT fonksiyonundan yetkili personelde bulunmalıdır. İş amaçları için gerekli olan yazılımların yüklenmesi için çalışan tarafından onay alınmalıdır.

8.20. Ağ Güvenliği

ASG, tüm ağları uygun güvenlik önlemleri ve uygun ekipmanlarla korumalıdır. Ağ adresleri, ağ konfigürasyonları ve ilgili sistem veya ağ bilgileri uygun şekilde muhafaza edilmeli ve yalnızca yetkili taraflara açıklanmalıdır.

- Ağların sahipleri veya kontrolörleri, ağ bölgelerini ve bu bölgelerdeki bilgi kaynaklarını korumak için aşağıdakiler dahil uygun güvenlik bileşenlerini konuşlandırmalıdır:
    - Güvenlik duvarı
    - Demilitarized Zone (DMZ)
    - Ağ Adresi Çevirisi (NAT)
    - Ağ Erişim Kontrolü
    - Sanal Yerel Alan Ağı (VLAN)
    - Sanal Özel Ağ (VPN)
    - Ağ Saldırı Tespit Sistemi (NIDS) ve Ağ Saldırı Önleme Sistemi (NIPS)
    - Kötü Amaçlı Yazılımdan Koruma
    - Proxy ve Ters Proxy
    - Kayıt Tutma ve Kayıt İzleme
- Güvenli ağ ve yönetilen ağlar dışındaki hassas bilgilerin iletimi şifrelenmelidir.
- Güvenilir bölgelerde sistem bileşenleri ile özel IP adresleri kullanılmalıdır. Özel IP adresleri yetkisiz taraflara açıklanmamalıdır.
- Ağ altyapısı, uygulanmadan önce ve büyük değişikliklerden sonra nitelikli güvenlik profesyonelleri tarafından incelenmeli ve onaylanmalıdır.
- Ağdaki tüm ekipmanların, güvenlik duvarları, yönlendiriciler, ana bilgisayarlar vb. dahil olmak üzere, konfigürasyonu, ASG BT fonksiyonu tarafından yayınlanan güvenlik temel konfigürasyonlarına göre sertleştirilmelidir.

- Ağın sahibi veya kontrolörü, ekipman konfigürasyonları için belirli bireyleri atamalıdır. Ekipman konfigürasyonlarını değiştirme yetkileri yalnızca yetkili bireylere verilmelidir.
- Güvenlik duvarı ve yönlendirici kural setleri, nitelikli güvenlik profesyonelleri tarafından en az 24 ayda bir veya ağ altyapısında önemli değişikliklerden sonra gözden geçirilmelidir.
- İç kablosuz erişim ağları, benzersiz kullanıcı kimlikleri aracılığıyla doğrulanmalıdır.
- Güçlü kullanıcı kimlik doğrulaması, Terminal Access Controller Access Control System (TACACS+), Remote Authentication Dial-In User Service (RADIUS) veya benzeri bir harici veri tabanına karşı doğrulama yapılmasını desteklemelidir.
- Tüm kablosuz trafiğin en az Wi-Fi Protected Access 2 (WPA2) koruması ile kullanılan Gelişmiş Şifreleme Standardı (AES) şifrelemesini kullanmasını sağlamalıdır.
- Kablosuz ağların Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) gibi kimlik doğrulama protokollerini kullanmasını sağlayarak kimlik bilgilerini koruma ve karşılıklı kimlik doğrulama sağlamalıdır.
- Kayıtlı ve izlenebilen bir donanım adresi, yani bir medya erişim kontrol adresi (MAC) bulundurulmalıdır.
- Güvenli ağ ve yönetilen ağlar dışındaki hassas bilgilerin iletimi (ASG Bilgi Sınıflandırma ve İşleme Politikasında tanımlandığı gibi sınıflandırılmış bilgiler) şifrelenmelidir.
- Organizasyon ağına bağlı tüm kablosuz erişim noktaları ve kablosuz cihazlar, belirlenen BT fonksiyonu temsilcisi tarafından kaydedilmeli ve onaylanmalıdır.
- Tüm kablosuz cihazlar, haber verilmeksizin BT fonksiyonu denetimlerine ve penetrasyon testlerine tabi tutulacaktır.
- Kritik iş fonksiyonları için tüm kablosuz bağlantılar, dış bağlantılar olarak kabul edilmeli ve iç erişim noktalarından ayrılmalıdır, sistem yöneticilerinden ayrı erişim sağlanmalıdır.
- Yalnızca ASG'ya ait kablosuz cihazların kurumsal kablosuz ağa bağlanmasına izin verilir, ASG'ya ait olmayan cihazlar veya üçüncü taraf tedarikçi cihazları yalnızca misafir ağı için kurulan SSID'lere sınırlıdır.
- Tüm kablosuz cihazlar, hizmete alınmadan önce BT fonksiyonu tarafından uygun konfigürasyon açısından kontrol edilmelidir.
- Kurumsal ağa olağanüstü erişim gerektiren ASG'ya ait olmayan cihazlar veya üçüncü taraf tedarikçi cihazları, BT fonksiyonundan ön onay almalıdır.
- Misafir kullanımı / hasta kullanımı için Wi-Fi'da kimlik doğrulama etkinleştirilmiş olmalıdır.

8.21. Ağ Hizmetlerinin Güvenliği

Tüm ağ hizmetlerinin güvenlik mekanizmaları, hizmet seviyeleri ve yönetim gereksinimleri belirlenmeli ve bu hizmetler kurum içi veya dış kaynaklı olsun, ağ hizmetleri anlaşmalarına dahil edilmelidir.

- **Kimlik Doğrulama Gereksinimleri (Kimliği doğrulama):**

- Bu politikanın kontrol 5.16 ve 5.17'sine göre Kullanıcı Kimliği ve Parola Kombinasyonu.
- Parola, kanalın kendisi şifrelenmediği ve yalnızca hedef alıcıya sınırlı olduğu sürece açık metin olarak iletilmemelidir.
- Kritik ağ varlıkları için çok faktörlü kimlik doğrulama.
- Tüm giriş modları için Radius/TACACS+ kullanarak merkezi kimlik doğrulama tercih edilmelidir; GUI, CLI, Yöneticiler vb.
- Parola kontrolüne göre başarısız kimlik doğrulama girişimleri sayısı için sınırlar uygulanmalıdır.
- Giriş arayüzüne erişimi sınırlamak için erişim kontrol politikaları uygulanmalıdır.

- Tüm ağ varlıkları SIEM ile entegre edilmelidir.
- Herhangi bir hassas veri taşıyan fiziksel veya mantıksal arayüz, güçlü kriptografik koruma ile trafiği güvence altına alacak şekilde yapılandırılmalıdır.
- Ağ hizmetlerine veya uygulamalara erişimi kısıtlamak için gerekli durumlarda ağ hizmet prosedürleri uygulanmalıdır.
- Gizli verilere kablosuz erişim, bu ve ASG'nin gizli verilere uygulanan diğer politikalarıyla tutarlı olduğu sürece izin verilir.
- Kullanıcılar, kablosuz ağı kullanmadıklarında kablosuz yeteneklerini devre dışı bırakmalıdır.
- Sinyal yayın gücünü kontrol etmek için ofis alanını kapsayacak şekilde yalnızca gerekli olan kadar azaltan teknoloji kullanılmalıdır.

a. Periyodik Ağ Testi

- Belirli aralıklarla, ASG Ağ Operasyonları ve Güvenlik ekipleri mevcut güvenlik uygulamalarını gözden geçirip, artan veya yeni keşfedilen tehditler nedeniyle değişiklikler yapmalıdır.
- ASG Güvenlik Yönetimi, Üretim Ağına giriş noktalarının güvenliğini en az yılda bir kez test ederek yetkisiz kişiler tarafından istismar edilebilecek potansiyel zayıflıkları belirleyip düzeltmelidir. Keşfedilen zayıflıklar, çözüm için ilgili personele iletilmelidir. İstismarı önlemek amacıyla, Güvenlik Yönetimi belirli test vakalarını ve detaylı sonuçları gizli tutmalıdır.
- Bu politikanın takip edildiğinden emin olmak için kablosuz ağ periyodik olarak denetlenmelidir. Spesifik denetim noktaları; erişim noktalarının konumu, sinyal gücü, SSID, SSID yayını ve güçlü şifreleme kullanımı olmalıdır.

8.22. Ağların Ayrılması

- Kontrolü basitleştirmek için, hesaplama kaynaklarının ağı konum, işlev ve işlenen bilginin sınıflandırmasına göre güvenlik bölgelerine gruplandırılması ve ayrılması gerekmektedir. Güvenlik bölgelerinin derinliği veya katman sayısı, işlenen bilginin hassasiyetine uygun olmalıdır.
- Ayrılmış bölgelerdeki hesaplama kaynaklarını korumak için Network ve Uygulama Güvenlik Duvarı, Ters Proxy, Sızma Tespit Sistemi ("IDS") gibi uygun ağ güvenlik ekipmanları kurulmalıdır.

- Sınır ötesi ağ trafiği ağ güvenlik ekipmanları aracılığıyla yönlendirilmelidir.
- Güvenilir bölgeler arasındaki tüm trafiğe varsayılan olarak izin verilmemeli; izin verilen trafiğin açıkça belgelenmiş ve gerekçelendirilmiş olması gerekmektedir.
- İnternet ve ortak ağlar da dahil olmak üzere harici ağlardaki tüm trafiğe varsayılan olarak izin verilmemeli; izin verilen trafiğin açıkça belgelenmiş ve gerekçelendirilmiş olması gerekmektedir.
- ASG'nin ağı IT fonksiyonu tarafından yönetilmektedir. Diğer ağlar ASG için harici ağlardır. İnternet ağ geçitleri ASG'nin ağını İnternet'e bağlar. Harici geçitler doğrudan ASG'nin ağını iştiraklerin ağları, yurtdışı şubelerin ağları, ortak organizasyon ağları ve üçüncü taraf hizmet sağlayıcıların ağları gibi partner ağlarına bağlar. Harici geçitlere ihtiyaç duyan ağların örnekleri özel kiralanmış hatlar, Çok Protokollü Etiket Anahtarlama ("MPLS"), Sanal Özel Ağlar ("VPN"), SDWAN gibi şeylerdir.
- ASG IT fonksiyonu, ASG ağını İnternet'e bağlayan İnternet geçitlerinin yönetiminden ve izlenmesinden sorumludur. Ayrıca, tüm ASG kullanıcılarına hizmet sağlayan harici geçitlerin yönetiminden ve izlenmesinden de sorumludur.
- ASG'nin iştirak birimleri veya içerisindeki personel, önceden ASG IT fonksiyonundan kayıt ve onay almadan geçit kullanamaz. IT fonksiyonu, iştirakler tarafından sahip olunan ve yönetilen geçitler için kayıt ve onay prosedürü oluşturmalıdır. İnternete veya harici ağlara erişim tüm kayıtlı ve onaylı geçitler aracılığıyla yönlendirilmelidir.
- Geçit sahipleri veya kontrolörleri, ASG'nin ağını güvenlik tehditlerine karşı korumak için uygun güvenlik önlemlerinin uygulandığından emin olmalıdır. Saldırıları tespit etmek ve savunmak için uygun önlemler alınmalıdır.
- ASG ağ genişliği sınırlı bir kaynaktır, bu kaynağın olağanüstü yüksek kullanımı tüm diğer kullanıcıları etkileyebilir. IT fonksiyonu ağ kullanımını izlemeli ve ASG'nin ağ genişliğinin adil kullanımını sağlamalıdır. Ağ genişliği kullanımıyla ilgili IT kılavuzları oluşturmalı ve olağanüstü yüksek ağ genişliği kullanımına sahip makineleri izlemek, bildirmek, uyarı vermek ve askıya almak için prosedürleri belirlemelidir.
- ASG'nin ağına bağlı olan ve İnternet'e ve harici ağlara erişim sağlayan tüm geçitler aşağıdaki güvenlik işlevlerini sağlamalıdır:
    - Erişim kontrolü için Güvenlik Duvarı
    - Trafik yönlendirme ve paket filtreleme için Paket-filtreleme yönlendiricileri
    - Bilgisayar virüslerine karşı koruma
- Saldırı tespiti sistemi (IDS) ve saldırı tespit izleme sistemi
- Kayıtlı olmayan geçitler yasadışı arka kapılar olarak kabul edilir. Tüm ASG iştirakleri yıllık olarak veya Grup IT fonksiyonu tarafından istendiğinde, kurulan geçitlerini, İnternet geçitlerini, harici geçitleri ve harici olarak tahsis edilen IP adresi aralıklarını Grup IT fonksiyonuna bildirmelidir. Bildirilen geçitler ve IP adresi aralıkları, yasadışı arka kapıları tespit etmek için kayıtla karşılaştırılmalıdır. Bulunan tüm yasadışı arka kapılar derhal ASG'nin ağından çıkarılmalıdır.
- Bu politika, kablosuz cihazları içeren ve destekleyen ağın bölümlerinin (kablosuz ağ) kablosuz bağlantıları desteklemeyen ağın bölümünden ayrılmasını gerektirir.

- Kablosuz cihazları veya bağlantıları destekleyen ağın bölümü, kablosuz bağlantıları desteklemeyen ağ bölümünden daha az güvenilir olarak kabul edilmelidir. Tüm dosya sunucuları ve iç alan denetim sunucuları, kablosuz ağı bir güvenlik duvarı kullanarak ayrılmalıdır.

- Kamu Wi-Fi, kurumsal ağ erişiminden fiziksel olarak ayrılmalıdır, mümkünse VLAN tarafından mantıksal olarak ayrılması önerilir.

- Ağ alanları arasında bağlantı izin verilir ancak sınırda (örneğin, güvenlik duvarı, filtre yönlendirici) yönetilmelidir. Ağın bölgelere ayrılması ve geçit erişimi gereksinimleri, her alanın güvenlik gereksinimlerinin değerlendirilmesine dayanmalıdır.

8.23. Ağ Filtreleme

- ASG IT fonksiyonu, genellikle bu tür sitelerde bulunan siber tehditlere karşı savunmak için ASG ağı içinden bu tür sitelere erişimi kısıtlayabilir. Ayrıca, aşağıdaki internet etkinlikleri veya siteler yasaktır:

- İşle ilgisi olmayan web sitelerine ve diğer internet hizmetlerine erişim, ASG IT tarafından engellenmemiş olsalar bile

- P2P veya dosya paylaşım uygulamalarının kullanımı (BitTorrent, Kazaa, Morpheus, LimeWire, Bearshare, eMule, eDonkey vb. dahil)

- Ağ performansını etkileyen hizmetlere erişim

8.24. Kriptografi kullanımı

- Şifreleme, veri dinlenme sırasında, işleme sırasında ve iletim sırasında, taşınabilir depolama cihazlarının kullanımı ve e-posta yoluyla veri iletimi için benimsenmelidir.

- ASG bilgi sistemleri dışında aktarılan tüm Kritik veya Hassas bilgiler şifrelenmelidir.

- Taşınabilir cihazlardaki verilerin güvenliği için şifreleme kullanılmalıdır.

- Dijital imzalar, inkar edilemezlik sorununu çözmek için kullanılmalıdır.

- Şifreleme anahtarlarının korunması ve kaybolma veya zarar görmesi durumunda kurtarılmasıyla ilgilenen yetkili personele sahiplik atanmalıdır.

- Tüm şifreler dinlenme sırasında şifrelenmelidir.

- Kuruluş için kriptografik standartlar uygulanırken, ilgili düzenlemeler ve kriptografik yöntemler üzerindeki kısıtlamalar dikkate alınmalıdır.

- Bilgi varlıklarında kullanılan tüm şifreleme ürünleri ve süreçleri, IT işlevinden yetkili personele onaylatılmalıdır.

a. Kriptografik Standart

Tüm amaçlar için özel şifreleme algoritmalarının kullanımı yasaktır. İşte ASG tarafından önerilen şifreleme algoritmaları ve anahtar uzunlukları:

Amaç	Algoritma	Tavsiye edilen Anahtar Uzunluğu
Şifreleme	AES (Advanced Encryption Standard)	256 bit veya daha güçlü

Anahtar Alışverişi	RSA (Rivest, Shamir & Adelman)	4096 bit
	ECDH (Elliptic Curve Diffie Helman)	256 bit, Grup 19
Dijital İmza	RSA (Rivest, Shamir & Adelman)	4096 bit
	ECDSA (Elliptic Curve Digital Signature Algorithm)	256 bit veya daha güçlü
Hashleme	SHA-2	256bit veya daha güçlü
İletişim Güvenliği	TLS 1.2 or higher (Transport Layer Security)	N/A

Anahtar uzunluk gereksinimleri yıllık olarak gözden geçirilecek ve teknoloji izin verdiği ölçüde güncellenecektir. İşte Veri Durumları ve Şifreleme Örnekleri:

Veri Durumları	Örnekler
İşlemdeki Veri	PHI/PII işleme, Hassas ticari bilgi vb.
Depolanan Veri	Dosya sunucusu depolama, masaüstü dosyaları, harici kayıt ortamları vb.
Transfer durumunda Veri	SFTP, Internet trafiği, VPN vb.

b. Kriptografik Anahtar Yönetimi

- Şifreleme anahtarları gizli veri olarak kabul edilir ve güvenli bir şekilde yönetilmelidir.
- Şifreleme anahtarları, korudukları veriden ayrı olarak saklanmalıdır.
- Anahtarlar güvenli bir şekilde oluşturulmalı ve anahtar oluşturma sürecinde kullanılan tüm materyaller kullanımdan sonra imha edilmelidir.
- Şifreleme anahtarları, bir anahtarın maruz kalması durumundaki etkiyi azaltmak için tek bir amaç için kullanılmalıdır.
- Şifreleme anahtarları güvenli bir şekilde iletilmelidir.
- Kriptografik bir anahtarı değiştirirken, yeni bir anahtar önceki anahtardan bağımsız olarak oluşturulmalıdır.
- Şifreleme anahtarları, iş gereksinimleri doğrultusunda belirlenen bir sıklıkta, en azından yılda bir kez olmak üzere, uygun şekilde döndürülmelidir.
- Tehdit altındaki anahtarlar ve tehdit altındaki anahtarlar altında şifrelenmiş veya bu anahtarlar tarafından türetilmiş tüm anahtarlar derhal iptal edilmeli, imha edilmeli ve yenilenmelidir.
- Tehdit altındaki anahtarların iptal edilmesiyle ilgili tüm ilgili taraflar bilgilendirilmelidir.

8.25. Güvenli Geliştirme Yaşam Döngüsü

ASG, içsel olarak geliştirilen uygulama ve bilgi sistemlerinin güvenli geliştirme yaşam döngüsü için belirlenen prosedürleri, standartları ve önde gelen uygulamaları izlediğinden emin olacaktır.

8.26. Uygulama Güvenliği Gereksinimleri

Uygulama sahipleri, güvenliği gereksinim aşamasından başlayarak tüm uygulama geliştirme yaşam döngüsü boyunca uygulamaya dahil edeceklerdir.

- Uygulama sahipleri, eğitimli Bilgi Güvenliği ekibiyle çalışarak kullanıcı gereksinimleriyle ilgili güvenlik gereksinimlerini tanımlamak, doğrulamak, kabul etmek ve belgelemek için çalışacaklardır.

- Hassas, değerli veya kritik iş bilgilerini işleyen tüm uygulamaların belgelenmiş güvenlik gereksinimleri olmalıdır.
- Sistem erişim kontrolü, kimlik doğrulama seviyesi, işlem yetkilendirme, veri bütünlüğü, sistem etkinlik günlüğü, denetim izi, güvenlik olayı takibi ve istisna işleme ile ilgili güvenlik gereksinimleri, sistem geliştirme veya edinme sürecinin erken aşamalarında açıkça belirtilmelidir.
- Yeni sistemler veya mevcut sistemlerin iyileştirmeleri için iş gereksinim belgeleri, güvenlik kontrolleri gereksinimlerini içermelidir.
- Uygulama tarafından yayımlanan bilgilerin yalnızca ihtiyaç duyulduğunda sağlandığından emin olunmalıdır. Mimaride bilgilerin sadece yetkili açıklamayı destekleyen güvenli bir şekilde depolandığından emin olunmalıdır.

8.27. Güvenli Sistem Mimarisi ve Mühendislik İlkeleri

- ASG, tüm yerinde ve dış kaynaklı bilgi sistemleri mühendislik faaliyetlerine uygulanacak kontrolleri içeren güvenli sistem mühendisliği üzerine gerektiğinde belgelenmiş ve onaylanmış bir prosedüre sahip olacaktır.
- ASG, iş güvenliği gereksinimleri ile bilgi güvenliği ihtiyaçlarını dengeleyerek, iş, veri, uygulama ve teknoloji katmanlarına "Güvenlik Tasarımı" prensibiyle yaklaşacaktır.
- Yeni teknoloji gereksinimleri güvenlik riskleri açısından analiz edilecek ve tasarım bilinen saldırı kalıplarına karşı gözden geçirilecektir.
- ASG, giriş ve çıkış arayüzleri olan bilgi sistemlerinin geliştirilmesinde güvenli mühendislik tekniklerini uygulayacak ve kullanıcı kimlik doğrulama teknikleri, güvenli oturum kontrolü ve veri doğrulama, temizleme ve hata ayıklama kodlarının kaldırılması konusunda rehberlik sağlayacaktır.

8.28. Güvenli Kodlama

- OWASP, NIST çerçeveleri, SANS gibi önde gelen standartlara uygun güvenli kodlama kuralları, ASG içinde uygulama ve bilgi sistem geliştirme süreçlerinde yaygın olarak kullanılacaktır. Bu sayede ortak zayıflıklara karşı koruma sağlanacaktır.
- Güvenli Kod İncelemeleri, geliştirme aşamasında bağımsız olarak (akran incelemesi / güvenlik ekibi tarafından inceleme) veya periyodik bilgi güvenliği incelemesi sırasında gerçekleştirilecektir.
- Güvenli programlama teknikleri, hem yeni geliştirmelerde hem de kod yeniden kullanım senaryolarında kullanılacaktır.

8.29. Geliştirme ve Kabul Aşamasında Güvenlik Testleri

Uygulama geliştiricilerinin, yazılımı geliştirme ortamından test ortamına taşıma yetkisi olduğu ancak yazılımı üretim ortamına taşıma yetkisinin olmadığı önerilen bir uygulamadır. Geliştiricilerin üretim ortamına yazılımın izinsiz değişikliklerini önlemek için uygun kontroller uygulanacaktır.

Bilgi sistemlerine hataları tespit etmek veya önlemek için güvenlik kontrolleri entegre edilecek ve test edilecektir:

- Uygulama sistemlerine veri girişinin doğru ve uygun olduğunu sağlamak için veri giriş validasyonu yapılacaktır.
- Kullanıcı etkinliklerinin izlenebilirliği ve kullanıcıların eylemlerinden sorumlu tutulabilirliği için denetim izi günlüğü tutulacaktır.
- İşleme hataları veya kasıtlı eylemlerden kaynaklanan veri bozulmalarını tespit etmek için sistemlere doğrulama kontrolleri entegre edilecektir.
- Uygulamaların mesaj içeriğinin bütünlüğünü korumak için mesaj doğrulama teknikleri uygulanacaktır (elektronik olarak iletilen bilgilerin, elektronik para transferi, elektronik olarak iletilen finansal teklifler gibi yetkisiz değişiklikler veya bozulmalardan korunması için).
- Geri kapılar, kullanılmayan değişkenler, açık portlar gibi güvenlik açıkları güvenli bir şekilde kaldırılacak veya kullanımdan sonra devre dışı bırakılacaktır.
- Canlıya geçmeden önce, tüm dış (internet) ile yüz yüze uygulamalar için Zayıflık Değerlendirme ve Sızma Testi, uygun olan altyapılar dahil olmak üzere Bulut bilişim ortamlarında barındırılan uygulamalar için gerçekleştirilmelidir.
- Yasal ve düzenleyici gereksinimlere uyum sağlanacaktır.
- Güvenli geliştirme uygulamaları, hem yeni geliştirmelerde hem de kod yeniden kullanım senaryolarında kullanılmalıdır.

Yeni bilgi sistemleri ve bilgi işleme tesisleri, yükseltmeler ve yeni sürümler için kabul kriterleri tanımlanacak ve geliştirme sırasında ve gerçek üretime geçmeden önce uygun testler yapılacaktır. Herhangi bir yeni bilgi sistemi, yükseltme veya yeni sürümün devreye alınmadan önce Uygulama ve Bilgi Sistem Sahibi tarafından Siber ve IT Güvenlik ekibinden güvenlik onayı alınacaktır.

a. Bakım Sırasında Güvenlik

- Tüm dış/internet ile yüz yüze uygulamalar ve web siteleri için yıllık olarak Uygulama Zayıflık Değerlendirmesi ve Sızma Testi yapılmalıdır ve/veya her Büyük Değişiklik için yapılmalıdır, bilgi sızıntısı ve güvenlik zayıflıkları potansiyel risklerini belirlemek için.
- İç yüze uygulamalar için yıllık olarak Zayıflık Değerlendirmesi yapılması önerilen bir uygulamadır.
- Uygulama geliştiricileri onaylı değişiklik talepleri üzerinde çalışacak ve yalnızca gerekli değişiklikleri yapacaklardır.
- Değişiklikler, üretim ortamına geçmeden önce sistem sahibi tarafından test edilip onaylanmalıdır.
- Uygulama yamaları, test ortamında etkisinin test edilmesinin ardından, satıcı sürümüne göre uygulanmalıdır.

b. İşletim Platformu Değişiklikleri Sonrası Uygulama Teknik İncelemesi

- İşletim sistemi ile ilgili yeni sürümler/Yamalar, üretim ortamına uygulanmadan önce test edilmeli ve iş kritik uygulamalar, işletim, uygulama kontrolleri veya güvenlik üzerinde olumsuz bir etkisi olup olmadığından emin olmak için gözden geçirilmelidir.

c. Uygulama Paketlerine Yapılan Değişikliklerin Kısıtlanması

- Satıcı tarafından sağlanan uygulama paketleri, uygulamadan önce hash doğrulama, kod imzalama vb. ile herhangi bir değişiklik veya bozulma için doğrulanmalıdır.
- Satıcı tarafından sağlanan uygulama paketleri, satıcıya danışılmadan değiştirilmemelidir.
- Bu tür uygulamalara yapılan herhangi bir değişiklik gereksinimi, Değişiklik Yönetimi Prosedürüne tabi tutulmalıdır.

8.30. Dış Kaynaklı Geliştirme

Bilgi sistemleri geliştirme süreci dış kaynaklara devredildiyse, ASG, dış taraftan ASG'nın geçerli güvenlik ve gizlilik gereksinimlerine uyduğundan ve sürekli olarak bu beklentileri karşıladığından emin olmalıdır.

8.31. Geliştirme, Test ve Üretim Ortamlarının Ayrılması

Geliştirme, Test ve Üretim ortamları (ayrı fiziksel veya sanal sunucular olarak) yetkisiz erişim veya üretim ortamında değişiklik risklerini azaltmak için ayrılmalıdır.

- Geliştirme ortamından üretim ortamına geçiş, tüm güvenlik kontrollerinin yapıldığından emin olmalıdır.
- Test sistemi eşdeğer kontroller sağlanmadıkça, hassas veriler test sistemine kopyalanmamalıdır.

8.32. Değişiklik Yönetimi

ASG, bilgi güvenliğini etkileyen örgüt, iş süreçleri, bilgi işleme tesisleri ve sistemlere yapılan değişikliklerin kontrol altında tutulmasını sağlamalıdır. Değişikliğin etkisi değerlendirilmeli, değişiklikler gözden geçirilmeli ve onaylanmalı, geri dönüş stratejileri göz önünde bulundurulmalı ve değişiklik, paydaşlara uygun iletişimle yönetilmelidir. Tüm üretim değişiklikleri için bir geri alma planı gereklidir.

- Üretim ortamında uygulamadan önce tüm üretim değişiklikleri ASG tarafından onaylanmadan önce üretim ortamında uygulanmadan önce bir bölüm spesifik Kurumsal Değişiklik Kontrol Kurulu oluşturulmalıdır.

8.33. Test Bilgileri

ASG'nın bilgi sistemlerinin geliştirme sürecinde kullanılan verileri yetkisiz erişimi ve açıklanmasını önlemek için korunmalı ve kontrol edilmelidir. Kişisel olarak tanımlanabilir bilgiler test amaçları için kullanılıyorsa, tüm hassas detaylar ve içerik, ASG Kişisel Veri Koruma Politikası'na göre kaldırma veya değiştirme ile korunmalıdır.

8.34. Denetim Testleri Sırasında Bilgi Sisteminin Korunması

ASG bilgi sistemlerinde yapılan denetim gereksinimleri ve etkinlikleri iş süreçlerinde aksaklıkları en aza indirmek için planlanmalı, belgelenmeli ve kabul edilmelidir. Denetimden kaynaklanan hasar veya aksaklıklardan korunmak için ilgili önlemler alınmalıdır.

9. REFERANSLAR

9.1. Mevzuat ve Düzenlemeler

NA

9.2. ASG Dokümanları

- ASG_002 ASG Bilgi Güvenliği Yönetişim Çerçevesi
- ASG _111 Bilgi Teknolojisi Varlık Değerleme Standardı
- ASG_009 İndirilen Veri Politikası
- ASG_112 Üçüncü Taraf BT ve Siber Güvenlik Risk Yönetimi Çerçevesi
- ASG_019 Bilgi Teknolojisi ve Siber Güvenlik Risk Yönetimi Politikası
- ASG_011 Siber Güvenlik Kriz Yönetim Planı
- ASG_020 İş Sürekliliği Yönetimi Politikası
- ASG_012 Kendi Cihazını Getir Politikası
- ASG_003 Bilgi ve BT Varlıklarının Kabul Edilebilir Kullanımı Politikası
- ASG_005 Veri Bütünlüğü Politikası
- ASG_104 Ana Bilgisayar Platformu Güvenliği
- ASG_004 ASG Bilgi Teknolojisi ve Güvenlik Riski Değerlendirme Metodolojisi
- ASG_006 ASG Kişisel Verilerin Korunması Politikası
- ASG _113 ASG Uygunsuzluk Yönetimi Kılavuzu

9.3. Tanımlar

- Ayrıcalıklı hesap: Sistem yöneticisi, Ağ yöneticisi, Uygulama yöneticisi, Kullanıcı yöneticisi gibi yöneticilerin erişimi. Yönetici olmayan, yükseltilmiş ayrıcalıklara sahip hesaplar da Ayrıcalıklı hesaplar olarak kabul edilir.
- Hizmet hesabı: Sistem hizmetlerini çalıştırmak için kullanılan kimlik / hesap (örneğin, Web Sunucusu hizmet hesabı, toplu iş hizmeti hesabı, Veritabanı hizmeti hesabı vb.) veya Uygulamalar tarafından Veritabanına bağlanmak veya diğer Hizmetlerle arayüz oluşturmak için kullanılan Uygulama hesapları
- Genel hesap: Bireysel kullanıcıya ait olmayan kimlik/hesap. Aynı şifreyi paylaşan birden fazla kişi tarafından kullanılabilir.
- Uç Nokta: ASG Kurumsal ağına bağlanan PC, dizüstü bilgisayar veya cep telefonu gibi son kullanıcı bilgi işlem cihazı.
- Siber Güvenlik, bilgisayarların, ağların, programların ve verilerin, Organize suçlular, Siber casusluk, Hacktivistler, Ulus-devlet destekli suçlular vb. gibi çeşitli Siber tehdit aktörlerinin neden olduğu kasıtsız veya yetkisiz erişim, değişiklik veya tahribata bağlı Siber riskten korunmasıdır. Siber tehdit aktörleri genellikle aşağıdakileri gerçekleştirmeyi hedefler:

    o Özel bilgileri, fikri mülkiyeti ve gizli bilgileri çalmak

    o Karaborsada değeri olan kredi kartları, tıbbi kayıtlar ve kişisel veriler dahil olmak üzere gizlilik bilgilerinin çalınması

    o Hasar bilgi sistemleri

    o Sistemlerin/bilgisayarların gizli şifrelenmesi ve şifrenin çözülmesi için fidye talebi o Web sitelerinin tahrif edilmesi

    o İş hizmetlerini kesintiye uğratmak

- BGYS: Kuruluşun veriyi/bilgiyi yönetmesini sağlayan politika/prosedür/teknoloji dizisi

9.4. Kısaltmalar

- CIA: Gizlilik, Bütünlük ve Erişilebilirlik
- COE: Mükemmeliyet Merkezi
- CSP: Bulut Hizmet Sağlayıcısı
- DLP: Veri Sızıntısını Önleme
- GRC: Yönetişim, Risk ve Uyumluluk
- İK: İnsan Kaynakları
- ICER: Tanımlama, Sınırlama, Yok Etme ve İyileştirme
- BT: Bilgi Teknolojisi
- ISO: Uluslararası Standardizasyon Örgütü
- ISO/IEC 27001:2022: ISO/IEC (Uluslararası Standardizasyon Örgütü/Uluslararası Elektroteknik Komisyonu) 27001:2022
- BGYS: Bilgi Güvenliği Yönetim Sistemi
- KPI: Temel Performans Göstergeleri
- NDA: Gizlilik Anlaşması
- NIST: Ulusal Standartlar ve Teknoloji Enstitüsü
- PII: Kişisel Olarak Tanımlanabilir Bilgiler
- RPO: Kurtarma Noktası Hedefi
- RTO: İyileşme Süresi Hedefi
- SANS: Sistem Yöneticisi Denetim Ağı Güvenliği
- SIEM: Güvenlik Bilgileri ve Olay Yönetimi
- SLA: Hizmet Düzeyi Anlaşmaları
- SoD: Görevler Ayrılığı
- SBU: Stratejik İş Birimi
- VAPT: Güvenlik Açığı Değerlendirmesi ve Sızma Testi
- VPN: Sanal Özel Ağ\

9.5. Diğerleri

- ISO/IEC 27001:2022

10. EKLER

10.1. ASG Siber ve BT Güvenlik Politikası Çerçevesi