1. **Amaç**

Bu politikanın amacı, hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere bilgi güvenliği gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetiminin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

1. **Kapsam**

Kurumumuz kullanıcılarının bilgi varlıklarının kullanım kriterlerini ve tüm güvenlik uygulamalarını kapsar.

1. **Sorumluluklar**

Bilgi Güvenliği Politikasının hazırlanması, gözden geçirilmesi ve güncellenmesinden Bilgi Güvenliği Yönetim Sistemi Yöneticisi sorumludur. Kurumumuz firmasının Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar.

1. **Politika Detayları**

**Tanımlar**

**Bilgi Güvenliği Yönetim Sistemi (BGYS)**

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

**Bilgi Güvenliği Yöneticisi**

Bilgi Güvenliği Yönetim Sistemi’nin operasyonundan ve sürekli iyileştirilmesinden sorumludur.

**Bilgi Varlığı**

Kurumumuz firmasının sahip olduğu, işlerini aksatmadan yürütebilmesi için önemli olan varlıklardır. Bu politikaya konu olan bilgi varlıkları aşağıdadır:

* Kağıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri,
* Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım,
* Bilginin transfer edilmesini sağlayan ağlar,
* Bölümler, birimler, ekipler ve çalışanlar,
* Ofis ve Özel alanlar,
* Çözüm ortakları,
* Üçüncü taraflardan sağlanan servis ve hizmetler,

**Bilgi Varlığının İş Sahibi**

Bilgi varlıklarının üretimi, geliştirilmesi, bakımı, kullanımı ve güvenliğini kontrol etmek için onaylanmış yönetim sorumluluğu bulunan kişi veya varlıkları tanımlar. ‘Sahip’ terimi, gerçekten varlık üzerinde mülkiyet hakları olan kişi anlamına gelmez.

**Bilgi Varlığının Tek Sahibi**

Bilgi varlıklarının kurum içinde kullanılması için gerekli olan teknik operasyonda sorumluluğu bulunan kişi veya ekipleri tanımlar.

1. **Liderlik ve bağlılık**

Üst yönetim bilgi güvenliği yönetim sistemi ile ilgili olarak aşağıdakileri yerine getirerek, liderlik ve bağlılık göstermektedir;

a) Bilgi güvenliği politikası ve bilgi güvenliği amaçlarının oluşturulmasını ve kurumumuzun stratejik yönü ile uyumlu olmasının temin edilmesi,

b) Bilgi güvenliği yönetim sisteminin şartlarının kurumumuzun süreçleri ile bütünleştirilmesinin temin edilmesi,

c) Bilgi güvenliği yönetim sistemi için gerekli olan kaynakların erişilebilirliğinin temin edilmesi,

ç) Etkin bilgi güvenliği yönetiminin ve bilgi güvenliği yönetim sisteminin şartlarına uyum sağlamanın öneminin duyurulması,

d) Bilgi güvenliği yönetim sisteminin hedeflenen çıktılarının başarılmasının temin edilmesi,

e) Bilgi güvenliği yönetim sisteminin etkinliğine katkı sağlamaları için kişilerin yönlendirilmesi ve desteklenmesi,

f) Sürekli iyileştirmenin desteklenmesi ve

g) Kendi sorumluluk alanlarında liderliklerini sergileyebilmeleri için diğer ilgili yönetim rollerinin desteklenmesi.

**5.2 Politika**

 Bilgi kaynakları, ofis ve cihazlar gibi Kurumumuz firması açısından büyük önem taşıyan varlıklardır. Bilgi varlıklarını ve kaynaklarını kullanan veya bilgi sağlayan herhangi bir kişi, bilgi varlıklarını korumakla yükümlüdür.

 Ortak bilgi varlıklarını kullanan tüm çalışanların, gereken duyarlılığı göstermesi ve diğer meslektaşlarını, kurum çalışanlarını ve kurumsal değerleri gözeterek hareket etmesi beklenir.

 Kurumsal değerlerin gereği olarak gizliliğe önem verilir, her türlü kişisel bilgi en yüksek güvenlik standartlarına sahip sistemlerle korunur. Bilginin sahibi istemedikçe, yetki verilmedikçe veya yasal gereklilikler oluşmadıkça bilgi paylaşılmaz.

 Kurumumuz firması için tüm bu bilgi varlıkları ve kaynakları içerisinde en kritik olanı, özenle korunması, gizliliğinin sağlanması, ihtiyaç duyulduğu anda erişilmesi gereken bilgi varlıkları, sunucu sistemi üzerinde ve ofistedir.

 Bilgi varlıkları ve kaynakları farklı konumlarda veya ortamlarda bulunabilir. Hangi konumda veya ortamda olursa olsun müşteri iletişim gereksinimleri ve kurumsal değerler bu varlıkların ve kaynakların kullanımını belirler.

 Bilgi güvenliği, sadece bilginin gizliliğinin değil, bütünlüğünün ve kullanılabilirliğinin de sağlanması ile mümkündür. Bilginin gizlilik gerekliliği, sadece yetkilendirme dâhilinde gereken bilgi varlıklarına erişim verilmesi anlamına gelir. Bilginin bütünlüğü, tüm bilgi varlıklarının tamlığını ve doğruluğunu sağlamayı gerektirir.

Bilginin kullanılabilirliği, bilgi varlıklarının ihtiyaç duyulduğu anda ulaşılabilir ve kullanılabilir olması anlamına gelir.

Bilginin kullanımı, yerleşimi ve korunması ile ilgili ihtiyaçların karmaşıklığı ve çokluğu, kapsamlı ve geniş bilgi güvenliği süreçlerinin ve politikalarının tanımlanmasını zorunlu kılmaktadır. Bu nedenle belirlenen süreçler doğrultusunda bilgi güvenliği riskleri, bilgi varlığından sorumlu olan kişiler tarafından değerlendirilir, risklerin önceliği belirlenir ve gereken önlemler alınır.

Özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel dernekler ile uygun iletişime geçilir. Üst yönetim ve teknik çalışanlar özellikle güvenlik alaninda gelen bildirimler takip edilmektedir.

Sistem odası ve sunucularıngüvenliğinin sağlanması öncelikli olarak ele alınır. Varlık envanterinin ve bu envanterin olası risklerinin önceden belirlenerek müşterilerin güven içinde ve kesintisiz hizmet almaları için çalışılır.

Karar ve eylemlerde, güvenilir nesnel bilgiler ile teknolojinin tüm olanaklarının kullanılmasına önem ve öncelik verilir.

Bunu sağlamak için bilgi dünyadaki en ileri kaynaklardan transfer edilir, benimsenir ve mesleki uygulamalar bu doğrultuda yapılır. Kaynaklar verimli kullanılarak teknolojiye yatırım yapılır, gelişim bu doğrultuda sürdürülür.

Bu nedenle bilgi güvenliği yönetim sisteminin planlama, uygulama, izleme ve iyileştirme adımları ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi standardına ve bu standardı destekleyen standartlara uygun olarak yürütülür.

**5.3 Kurumsal Roller, Sorumluluklar ve Yetkiler**

Üst yönetim, bilgi güvenliği ile ilgili olan roller için sorumluluk ve yetkilerin atanmasını ve duyurulmasını temin etmektedir. Bünyesindeki tüm birimlerin bilgi güvenliği ile ilişkili konularını tartışan ve çözen merkezi bir birim olarak görev alır. Kurum bünyesinde bilgi güvenliği yönetim sisteminin ve bunun paralelinde ilgili politika ve prosedürlerinin uygulanmasından sorumludur. Bilgi güvenliği ile ilişkili konuları tartışan ve genel bilgi güvenliği stratejisinin, tehdit istihbaratını kurum bazında koordineli ilerlemesinden de yükümlüdür.

Kurul en az yılda bir kere ve gerekli hallerde toplanır. Tüm toplantıların tutanağı dokümante edilir ve ilgili kurul üyelerine ulaştırılır.

*Üst yönetim aşağıdakiler için sorumluluk ve yetki ataması yapmaktadır:*

a) Bilgi güvenliği yönetim sisteminin bu standardın şartlarına uyum sağlamasını temin etmek ve

b)  Üst yönetime bilgi güvenliği yönetim sisteminin performansı hakkında raporlama.

1. **Planlama**

**6.1 .1 Risk ve Fırsatları Ele Alan Faaliyetler**

Bilgi güvenliği yönetim sistemi planlaması yaparken, kurumumuz atıf yapılan hususları ve atıf yapılan şartları göz önünde bulundurmaktadır. Aşağıdaki maddelerin gerçekleştirilmesi için gerekli olan riskleri ve fırsatları belirlemektedir:

a)  Bilgi güvenliği yönetim sisteminin amaçlanan çıktıları sağlanabilmesinin temin edilmesi,

b) İstenmeyen etkilerin önlenmesi veya azaltılması ve

c) Sürekli iyileştirmenin başarılması,

Kurumumuz aşağıdakileri planlamaktadır:

 d) Bu risk ve fırsatların ele alınması için faaliyetler ve

 e) Aşağıdakilerin nasıl gerçekleştirileceği,

1) Faaliyetleri, bilgi güvenliği yönetim sistemi süreçleri ile bütünleştirme ve uygulama,

2) Faaliyetlerin etkinliğinin değerlendirilmesi.

**Risk Tanımlama ve Analiz**

Risk değerlendirmesinde, aşağıdaki puanlama formülüne göre risk değerlendirmesi yapılır.

|  |
| --- |
| Risk=(Olasılık \* Gizlilik)+(Olasılık \* Bütünlük)+(Olasılık \* Erişebilirlik) |

Riskin gerçekleşme olasılığı değerlendirilirken yardımcı olması için aşağıdaki sorular faydalı olabilir:

1. Daha önce bu kurumda/bölümde/süreçte böyle bir risk gerçekleşti mi?
2. Konuyla ilgili istatistiki bilgi var mı?
3. Bu risk unsurunun gerçekleşmesinin kolaylık derecesi nedir?

Olasılık değerlendirmesi için aşağıdaki tablo esas alınır.

|  |  |
| --- | --- |
| **Tehdit Olasılığı Değeri** | **Tehdit Olasılığı Tanımı** |
| 1 | Olası değil / Daha önce karşılaşılmamış. Mevcut kontrol ya da kontroller tehdidin her ortaya çıkışında etkin bir şekilde çalışmakta ve tehdidin oluşmasını/etkisini önlemektedir. |
| 2 | Son 3 yılda yaşanmış / Üç yılda bir ortaya çıkması muhtemel. Mevcut kontrol ya da kontroller kısmen etkin ve tehdidin her ortaya çıkışında çoğunlukla doğru işlemektedir ve önleyici etki göstermektedir. |
| 3 | Son bir sene içerisinde yaşanmış / sene içerisinde tekrarlaması muhtemel. Mevcut kontrol ya da kontroller tehdidin her ortaya çıkışında başarısız olabilmektedir veya bu tehdidi bertaraf edecek bir kontrol bulunmamaktadır. |
| 4 | Son bir sene içerisinde iki kere yaşanmış / sene içerisinde altı ayda bir tekrarlaması muhtemel. Mevcut kontrol ya da kontroller tehdidin her ortaya çıkışında başarısız olabilmektedir veya bu tehdidi bertaraf edecek bir kontrol bulunmamaktadır. |
| 5 | Son bir sene içerisinde dört kere yaşanmış / sene içerisinde üç ayda bir tekrarlaması muhtemel. Mevcut kontrol ya da kontroller tehdidin her ortaya çıkışında başarısız olmaktadır veya bu tehdidi bertaraf edecek bir kontrol bulunmamaktadır. |

Riskin etki değeri varlığa bir zarar gelmesi durumunda ve yasal düzenlemeler sonucu ortaya çıkan değişikliklerde bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik kaybına göre aşağıdaki tabloda belirtildiği metodoloji de değerlendirilir.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Etki Değeri** | **Etki Değeri Tanımı** | **GİZLİLİĞİN KAYBI** | **BÜTÜNLÜĞÜN KAYBI** | **ERİŞİLEBİLİRLİĞİN KAYBI** |
| 1 | ÇOK DÜŞÜK | - Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritiklik seviyesi altındaki bilgi, kurumu hiç etkilemez veya etkisi göz ardı edilebilir. | - Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritiklik seviyesi altındaki bilgi, kurumu hiç etkilemez veya etkisi göz ardı edilebilir. | - Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritiklik seviyesi altındaki bilgi, kurumu hiç etkilemez veya etkisi göz ardı edilebilir. |
| - Bilgi'nin kaybı veya gerçekleşen olay sadece yönetim tarafından bilinir. | - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %1'i şikayetçi olur veya hiç şikayet yaşanmaz. | - Kurumun operasyonlarında kesinti yaşanmaz veya yaşanan kesinti en fazla yarım saatliktir. |
| - Sözleşme şartlarında veya kanuni düzenlemelerde, kolay giderilebilecek bir problem veya uyumsuzluk oluşur. | - Kanuni düzenlemelere uyumluluk konusunda kolay giderilebilecek problemler ortaya çıkar.  |  |
| 2 | DÜŞÜK | - Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritiklik seviyesi altındaki bilgi, kurumu çok az etkiler.  | - Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu çok az etkiler.  | - Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritiklik seviyesi altındaki bilgi, kurumu çok az etkiler.  |
| - Bilgi'nin kaybı veya gerçekleşen olaylar kurum bünyesinde ve doğrudan ilişkili taraflarca (bankalar, il meclisi, düzenleyici kuruluşlar vb) bilinir. | - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %5'i şikayetçi olur. | - Kurumun operasyonlarında yaşanan kesinti yarım saatin üzerindedir ancak 8 saati geçmez ve etkileri çok yüksek değildir. |
| - Sözleşme şartlarında veya kanuni düzenlemelerde, bir problem veya uyumsuzluk oluşur. | - Kanuni düzenlemelere uyumluluk konusunda oluşan problemler sebebi ile kurum uyarı cezası alır. |  |
| 3 | ORTA | - Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritiklik seviyesi altındaki bilgi, kurumu etkiler. Etki orta vadede telafi edilebilir.  | - Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.  | - Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritiklik seviyesi altındaki bilgi, kurumu etkiler. Etki orta vadede telafi edilebilir.  |
| - Bilgi'nin kaybı veya gerçekleşen olaylar düzenleyici kuruluş tarafından incelemeye alınır. | - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %10'u şikayetçi olur. | - Kurumun operasyonlarında yaşanan kesinti 8 saat ile 12 saat arasında olur. Kısa vadede itibar kaybı olsa da, kurumun operasyonları devam eder. |
| - Sözleşme şartlarında veya kanuni düzenlemelerde oluşan problem sebebi kriz çıkabilir. Kriz sebebi ile cezai hükümler uygulanmasa bile, kurum nezdinde itibar kaybı yaşanır. | - Kanuni düzenlemelere uyumluluk konusunda oluşan problemler sebebi ile ilgili konuda düzenleyici kuruluş tarafından bir inceleme başlatılır. |  |
| 4 | YÜKSEK | - Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi, kurumu etkiler. Etki orta vadede telafi edilebilir.  | - Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.  | - Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi, kurumu etkiler. Etki orta vadede telafi edilebilir.  |
| - Bilgi'nin kaybı veya gerçekleşen olaylar medyada (yerel, ulusal basın vb.) olumsuz olarak bahsedilir.  | - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %20'si şikayetçi olur. | - Kurumun operasyonlarında yaşanan kesinti 12 saat ile 1 gün arasında olur. Kurumun operasyonlarının durmasından dolayı, itibarı negatif etkilenir ve uzun vadede kapatılması zor problem oluşur. |
| - Kurumda uygunsuzluk sebebi ile ciddi itibar kaybı yaşanır. | - Kanuni düzenlemelere uyumsuzluk yüzünden kurumun idari kadrosuna soruşturma açılır veya idari işlem başlatılır. |  |
| 5 | ÇOK YÜKSEK | - Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi, kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.  | - Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.  | - Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi, kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.  |
| - Bilgi'nin kaybı veya gerçekleşen olaylar medyada sürekli olarak gündeme getirilir ve vatandaşlar üzerinde kalıcı bir itibar kaybı oluşturur. | - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %20'den fazlası şikayetçi olur. | - Kurum operasyonları ilgili varlığa ulaşılamadığı için gerçekleştirilemez veya 1 günden uzun bir süre sekteye uğrar. |
| - Kurum sözleşmelerinde yer alan gizlilik şartlarını yerine getiremediği için, üst yönetim kadrosunda görevden almalar başlar. | - Kanuni düzenlemelere uyumsuzluk yüzünden yönetim değişikliği yapılır. |  |

**6.1.2 Bilgi Güvenliği Risk Değerlendirmesi**

Kurumumuz aşağıda belirtilen şartları yerine getiren bir bilgi güvenliği risk değerlendirmesi sürecini tanımlamakta ve uygulamaktadır.

Aşağıdakileri içeren bilgi güvenliği risk kriterlerinin oluşturulması ve sürdürülmesi:

a) Risk kabul kriterleri ve

b) Bilgi güvenliği risk değerlendirmesi yapılması için kriterler,

c) Tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesinin temin edilmesi,

d) Bilgi güvenliği risklerinin tespit edilmes,:

e) Bilgi güvenliği yönetim sistemi kapsamı dâhilindeki bilginin gizlilik, bütünlük ve erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi için bilgi güvenliği risk değerlendirme prosesinin uygulanması ve risk sahiplerinin belirlenmesi,

f) Bilgi güvenliği risklerinin analiz edilmesi:

g) Belirlenen riskler gerçekleştiği takdirde muhtemel sonuçların değerlendirilmesi,

h) Belirlenen risklerin gerçekleşmesi ihtimalinin gerçekçi bir şekilde değerlendirilmesi ve

 ı) Risk seviyelerinin belirlenmesi,

i)  Bilgi güvenliği risklerinin değerlendirilmesi,

k) Risk analizi sonuçlarının oluşturulan risk kriterleri ile karşılaştırılması ve analiz edilen risklerin risk işleme için önceliklendirilmesi.

Risk puanına göre aşağıdaki tabloya uygun olarak risk derecesi belirlenir.

|  |
| --- |
| **Eylem Matrisi** |
| **Risk Aralığı** | **Risk Derecesi** | **Eylem** |
| 45 | 75 | Kabul Edilemez Risk | Bu risklerle ilgili hemen çalışma yapılmalı. |
| 24 | 44 | Dikkate Değer Risk | Risklere mümkün olduğunca çabuk müdahale edilmeli. |
| 3 | 23 | Kabul Edilebilir Risk | Acil tedbir gerekmeyebilir. |
|  |  |  |  |
|  |  |  |  |
| Risk=(Olasılık \* Gizlilik)+(Olasılık \* Bütünlük)+(Olasılık \* Erişebilirlik) |
| Artık Risk |
| Yönetilen risklerden kalan risk puanları artık risk olarak tanımlanmaktadır. |

Risk değerlemenin amacı, risk analiz sonuçlarına bağlı olarak, risklerin azaltılmasına ve iyileştirmenin gerçekleştirilmesinin önceliğine karar vermede yardımcı olmaktır. Risklere karşı aşağıdaki yöntemlerle cevap verilebilir;

\*1- Riski kabul etme (Riskle yaşamaya devam etme)

 2- Riskten kaçınma (Riskli olduğu için geri adım atma)

 3- Riski azaltma ve kontrol etme (Risk seviyesini azaltmak için önlem alma)

 4- Riskin transferi başka bir kurumun yönetiminde

\*Kabul edilecek risklere ilgili birimin yöneticisi ile Bilgi Teknolojileri biriminin birlikte gözden geçirmeleri sonucu karar verilir. Kabul edilen bu riskler yıllık YGG toplantılarında gözden geçirilir. Söz konusu riskin kabulü, diğer birimlere herhangi bir tehdit oluşturmaması dikkate alınarak gerçekleştirilir. Kabul edilen risklerle ilgili onay e-mailleri ve ilgili kayıtlar mutlaka tutulmalıdır.

Risklerin durumu ‘’Açık‘’ veya ‘’Kapalı’’ olarak değerlendirilir ve açık riskler ‘’Açık Risk Yönetimi’’ sekmesinden takip edilir.

**6.1.3 Bilgi Güvenliği Risk İşleme**

Kurumumuz aşağıdakileri gerçekleştirmek için bir bilgi güvenliği risk işleme süreci tanımlamakta ve uygulanmaktadır:

a) Risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği risk işleme seçeneklerinin seçilmesi,

b) Seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan tüm kontrollerin belirlenmesi,

c) Belirlenen kontroller ile Ek A daki kontrollerin karşılaştırılması ve gerekli hiçbir kontrolün gözden kaçırılmadığının doğrulanması Uygulanabilirlik Beyanı dokümanında belirtilmiştir.,

d) Bir bilgi güvenliği risk işleme planının formüle edilmesi ve

e) Bilgi güvenliği risk işleme planına dair risk sahiplerinin onayının alınması ve artık bilgi güvenliği risklerinin kabulü

**6.2 Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama**

Kurumumuz, uygun işlevler ve seviyelerde bilgi güvenliği amaçlarını tesis etmektedir.

Bilgi güvenliği amaçları aşağıdakileri sağlamaktadır:

Bilgi güvenliği politikası ile tutarlı,

Ölçülebilir, Uygulanabilir bilgi güvenliği şartlarını ve risk değerlendirme ve risk işlemenin sonuçlarını dikkate alınarak,

İzlenmekte, Duyurmakta ve uygun şekilde güncellenmektedir.

Dokümante bilgi olarak mevcut olmalıdır.

**6.3 Değişikliklerin Planlanması**

Kurumumuz, bilgi güvenliği yönetim sisteminde değişiklik ihtiyacını belirlediğinde, değişiklikler planlı bir şekilde gerçekleştirilmektedir.

Bilgi sistemlerinde değişiklik yapmaya yetkili personel, bilgi teknolojileri departmanındaki sistem yönetileri ve uygulama yöneticisidir.

Yazılım ve donanım envanteri oluşturularak yazılım sürümleri kontrol edilmektedir.

Herhangi bir değişiklik yapılmadan önce, bu değişiklikten etkilenecek tüm sistemler ve uygulamalar belirlenmekte ve dokümante edilmektedir.

Değişiklik gerçekleştirilmeden önce bilgi teknolojileri müdüründen ve ilgili yöneticilerden onay alınmaktadır.

Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma oluşturulmakta ve bilgi teknolojileri direktöründen onay alınmaktadır.

Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmektedir.

Sistemler üzerinde yapılan değişikliklerden sonra loglar incelenerek kontrol edilmektedir.

Tüm bu değişim yönetimi işleri, bilgi teknolojileri müdürlüğünce kullanılan service desk plus adlı yazılımdan yürütülmektedir.

*BGYS de değişiklik planlarken kurumumuz bunları dikkate alır:*

Değişikliklerin amacı ve olası sonuçları.

BGYS nin bütünlüğü.

Kaynakların kullanılabilirliği.

Sorumlulukların ve yetkilerin tahsisi veya yeniden tahsisi.

1. **Kaynaklar**

Kurumumuz bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli olan kaynakları belirlemekte ve düzenli olarak sağlamaktadır.

Uygun beceri ve yetkinliklere sahip insan kaynakları.

Bilgi Güvenliği geliştirme ve yönetişim için gerekli teknolojik kaynaklar.

Bilgi Güvenliği girişimlerini ve uyumluluk faaliyetlerini destekleyici mali kaynaklar.

**7.2 Yeterlilik**

Kurumumuz Bilgi Güvenliği Yönetimi Sistemi performansını etkileyen tüm çalışanlarına aşağıdakileri sağlamaktadır.

a)  Bilgi güvenliği performansını etkileyen kendi kontrolü altında çalışan kişilerin gerekli yeterliliklerinin belirlenerek seçilmesi,

b)  Uygun öğretim, eğitim veya tecrübe temelinde bu kişilerin yeterliliklerinin temin edilmesi,

c)  Uygun olduğu durumlarda, gerekli yeterliliğin sağlanması için girişimde bulunulması ve bu girişimlerin etkinliğinin değerlendirilmesi birlikte ilgili çalışma ve eğitim imkanlarını sağlamaktadır.

**7.3 Farkındalık**

Kurumumuz Bilgi Güvenliği Yönetim Sistemi kontrolü dâhilinde görev yapan kişiler için farkındalık imkanlarını sağlamaktadır. Mevcut Bilgi güvenliği politikası, iyileştirilmiş bilgi güvenliği performansının faydaları da dâhil bilgi güvenliği yönetim sisteminin etkinliğine yaptıkları katkı ve Bilgi Güvenliği Yönetim Sistemi şartlarına uyum sağlamama’nın sonuçlarını BGYS farkındalığını yaratmak adına bildirimler yaparak, ilgili birim tarafından bilgilendirme mesajları uygulama üzerinden sağlanmaktadır. Ofis içerisinde bilgilendirme yazıları bulunmaktadır. Düzenli eğitimler sağlamakta ve kayıtları tutulmaktadır.

**7.4 İletişim**

Kurumumuz aşağıdakileri içeren bilgi güvenliği yönetim sistemi ile ilgili dâhili ve harici iletişim ihtiyaçlarını belirlemektedir:

a) İletişimin konusu,

b) Ne zaman iletişim kurulacağı,

c) Kiminle iletişim kurulacağı,

d) Kimin iletişim kuracağı ve

e) İletişimin hangi süreçten etkileneceği ve alternatif iletişim kaynaklarını belirlemekte ve paylaşmaktadır.

**7.5 Yazılı Bilgiler**

Kurumumuz bilgi güvenliği yönetim sistemi yazılı bilgileri aşağıdakileri içermektedir:

a)  Bu standardın gerektirdiği yazılı bilgiler ve

b)  kurumumuz tarafından bilgi güvenliği yönetim sisteminin etkinliği için gerekli olduğu belirlenen yazılı bilgiler.

Kurumumuz uygulaması ile dokümanların yönetimine ilişkin tanımlamaları içeren bir dokümanlar tanımlanarak ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi gerekliliklerini karşılayacak şekilde tanımlanmıştır.

**Oluşturma ve güncelleme**

Kurumumuz, yazılı bilgileri oluştururken ve güncellerken, aşağıdakileri uygun bir şekilde temin etmektedir:

a)  Tanımlama ve tarif etme (örneğin,  bir başlık, tarih, yazar veya referans numarası),

b)  Biçim (örneğin;  dil, yazılım sürümü, grafikler) ve ortam (örneğin,  kâğıt, elektronik) ve

c)  Uygunluğun ve doğruluğun gözden geçirilmesi ve onaylanması.

**Yazılı bilgilerin kontrolü**

Bilgi güvenliği yönetim sistemi ve bu standardın gerektirdiği yazılı bilgiler aşağıdakileri temin etmek için kontrol edilmektedir:

a) Gereken yerde ve zamanda kullanım için erişilebilir ve uygun olması ve

b)  Doğru bir şekilde korunması (örneğin, gizlilik kaybından, uygun olmayan kullanımdan veya bütünlük kaybından).

Yazılı bilgilerin kontrolü için, kurumumuz uygunluğuna göre aşağıdaki faaliyetleri ele almalıdır:

c)  Dağıtım, erişim, getirme ve kullanım,

d)  Okunaklılığın korunması da dâhil olmak üzere saklama ve koruma,

e)  Değişikliklerin kontrolü (örneğin sürüm kontrolü) ve

f) Muhafaza etme ve yok etme.

Kurumumuz, tarafından bilgi güvenliği yönetim sisteminin planlaması ve işletimi için gerekli olduğu belirlenen dış kaynaklı yazılı bilgiler dokümanında, uygun şekilde tespit edilerek kontrol edilmektedir.

1. **İşletim**

**8.1 İşletimsel planlama ve kontrol**

Kurumumuz, gereksinimleri karşılamak ve belirlenen eylemleri uygulamak için ihtiyaç duyulan süreçleri aşağıdakileri yaparak planlamakta, uygulamakta ve kontrol etmektedir.

 - Süreçler için kriterlerin belirlenmesi,

 - Süreçlerin kontrolünün kriterlere uygun olarak uygulanması,

Süreçlerin planlandığı gibi yürütüldüğünden emin olmak için gerekli olduğu ölçüde dokümante edilmiş bilgi mevcut ve güncel olarak tutulmaktadır.

Kurumumuz, planlanan değişiklikleri kontrol etmeli ve istenmeyen değişikliklerin sonuçlarını gözden geçirerek, gerektiğinde olumsuz etkileri azaltmak için harekete geçmektedir. Bilgi güvenliği yönetim sistemi ile ilgili dışarıdan sağlanan süreçlerin, ürünlerin veya hizmetlerin kontrol edilmesini sağlamaktadır.

**8.2 Bilgi Güvenliği Risk Değerlendirme**

Kurumumuz, belirtilen kriterleri de dikkate alarak, bilgi güvenliği risk değerlendirmelerini planlanan aralıklarda veya önemli değişiklikler önerildiğinde veya meydana geldiğinde gerçekleştirmektedir. Ayrıca, bilgi güvenliği risk değerlendirmesinin sonuçlarına dair yazılı bilgileri risk analizi dokümanında değerlendirmektedir.

**8.3 Bilgi Güvenliği Risk İşleme**

Kurumumuz,bilgi güvenliği risk işleme planını uygulamaktadır.Ayrıca, bilgi güvenliği risk işlemesinin sonuçlarına dair yazılı bilgileri risk analizi dokümanında işlemektedir.

1. **Performans Değerlendirme**

**9.1 İzleme, Ölçme, Analiz ve Değerlendirme**

Kurumumuz, bilgi güvenliği performansı ve bilgi güvenliği yönetim sisteminin etkinliğini değerlendirmektedir.

Kurumumuz aşağıdakileri belirlemektedir:

a)  Bilgi güvenliği süreçleri ve kontrolleri,

b)  İzleme ve ölçmenin ne zaman yapılacağı,

c)  İzlemeyi ve ölçmeyi kimin yapacağı,

d)  İzleme ve ölçme sonuçlarının ne zaman analiz edileceği ve değerlendirileceği ve

e)  Bu Sonuçları kimin analiz edeceği ve değerlendireceği gibi çalışmalar yapılmaktadır.

**9.2 İç Tetkik**

Kurumumuz, bilgi güvenliği yönetim sisteminin, aşağıdaki hususları yerine getirip getirmediği konusunda bilgi elde etmek için planlanan aralık olarak yılda 1 kez iç tetkikler gerçekleştirmektedir.

İç tetkiklerde uyumlu olup olmadığı, bilgi güvenliği yönetim sistemi ile ilgili olarak kurumumuzun kendi şartları ve bu standardın şartları, etkin bir şekilde uygulanması ve sürdürülmesi.

Ayrıca kurumumuz uygulanan iç tetkiklerde,

a) Sıklık, yöntemler, sorumluluklar, gereksinimleri planlama ve raporlama da dâhil olmak üzere bir tetkik programının/programlarının planlanması, oluşturulması, uygulanması ve sürdürülmesi. Tetkik programı/programları ilgili süreçlerin önemini ve önceki tetkiklerin sonuçlarını dikkate almaktadır.

b) Her bir tetkik için tetkik kriterlerinin ve kapsamın tanımlanması,

c) Tetkik sürecinin tarafsızlığı ve objektifliğini temin edecek şekilde tetkikçilerin seçimi ve tetkiklerin yürütülmesi,

d) Tetkik sonuçlarının uygun yönetim kademesine raporlanmasının temin edilmesi ve

e) Tetkik programı/programları ve tetkik sonuçlarının delil teşkil eden yazılı bilgilerinin muhafaza edilmesini sağlamaktadır.

**9.3 Yönetimin Gözden Geçirmesi**

Üst yönetim bilgi güvenliği yönetim sisteminin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek için planlı aralıklarla (Yılda 1 kez) gözden geçirilmektedir.

Yönetimin gözden geçirmesi aşağıdakileri ele almaktadır.

a)  Önceki yönetimin gözden geçirmelerinden gelen görevlerin durumu,

b)  Bilgi güvenliği yönetim sistemini ilgilendiren dış ve iç konulardaki değişiklikler,

c)  Gelişmeler dâhil bilgi güvenliği performansına dair geri bildirim,

d) Uygunsuzluklar ve düzeltici faaliyetler,

e) İzleme ve ölçme sonuçları,

f) Tetkik sonuçları ve Bilgi güvenliği amaçlarının yerine getirilmesi,

g)  İlgili taraflardan geri bildirimler,

h)  Risk değerlendirme sonuçları ve risk işleme planının durumu ve

ı)   Sürekli iyileştirme için fırsatlar.

Yönetimin gözden geçirmesi çıktıları, sürekli iyileştirme fırsatlarına ve bilgi güvenliği yönetim sisteminde gerekli olan değişiklikler için tüm ihtiyaçlara dair kararları içermektedir.

Üst yönetim, sürekli uygunluğunu, yeterliliğini ve etkinliğini sağlamak için kurumumuzun bilgi güvenliği yönetim sistemini planlanan aralıklarla gözden geçirmektedir.

**9.3.2 Yönetimin gözden geçirmesi girdileri;**

Önceki yönetimin gözden geçirmelerinden gelen görevlerin durumu;

Bilgi güvenliği yönetim sistemi ile ilgili iç ve dış konulardaki değişiklikler,

Bilgi güvenliği yönetim sistemi ile ilgili ilgili tarafların ihtiyaç ve değişiklikler,

Aşağıdaki trendler dahil olmak üzere bilgi güvenliği performansı hakkında geri bildirim,

Uygunsuzluklar ve düzeltici faaliyetler,

İzleme ve ölçme sonuçları,

Tetkik sonuçları,

Bilgi güvenliği amaçlarının yerine getirilmesi,

İlgili taraflardan geri bildirimler,

Risk değerlendirmesinin sonuçları ve risk işleme planının durumu,

Sürekli iyileştirme için fırsatlar.

**9.3.3 Yönetim Gözden Geçirme Sonuçları;**

Yönetim, Bilgi Güvenliği Yönetim Sisteminin sürekli uygunluğunu, yeterliliğini ve etkinliğini sağlamak için BGYS'yi planlı aralıklarla gözden geçirir. Sonuçlar Yönetimin Gözden Geçirme Tutanaklarında belgelenir. İncelemede denetim sonuçları, paydaş geri bildirimleri, performans ölçümleri ve BGYS'yi etkileyen değişiklikler dikkate alınır. Sistemi iyileştirmek ve sorunları çözmek için kararlar ve eylemler ele alınır. Yönetimin gözden geçirmesinin sonuçları, sürekli iyileştirme fırsatlarıyla ilgili kararları ve bilgi güvenliği yönetim sistemindeki tüm değişiklik ihtiyaçlarını içermektedir.

1. **Sürekli İyileştirme**

Kurumumuz, Bilgi Güvenliği Yönetim Sisteminin sürekli iyileştirilmesine kendini adamıştır. İyileştirme faaliyetleri, düzeltici eylemler ve iyileştirme fırsatlarının bir kaydında belgelenir. Kurumumuz süreçleri ve kontrolleri geliştirmeye yönelik eylemleri uygulayarak denetimler, izleme ve geri bildirim yoluyla fırsatları belirler.

Kurumumuz, bilgi güvenliği yönetim sisteminin uygunluğunu, doğruluğunu ve etkinliğini sürekli olarak iyileştirmektedir.

**10.2 Uygunsuzluk ve Düzeltici Faaliyet**

Uygunsuzluklar oluştuğunda uygunsuzluk raporları ve düzeltici faaliyet kayıtları kullanılarak giderilir. Süreç, uygunsuzluğa tepki verilmesini, eylem ihtiyacının değerlendirilmesini, düzeltici eylemlerin uygulanmasını ve bunların etkinliğinin gözden geçirilmesini içerir. Şeffaflık ve hesap verebilirliğin sağlanması amacıyla kayıtlar tutulur.

Bir uygunsuzluk oluştuğunda, kurumumuz aşağıdakileri yerine getirmektedir.

a)  Uygunsuzluğa tepki verilmesi ve mümkün olması durumunda;

1) Kontrol edilmesi, düzeltmek için eyleme geçilmesi ve sonuçları ile ilgilenilmesi,

b)  Aşağıdakilerin yerine getirilmesi yoluyla, uygunsuzluğun başka bir yerde tekrar etmemesi veya oluşmaması için nedenlerinin giderilmesi amacıyla eyleme geçme ihtiyacının değerlendirilmesi;

1)  Uygunsuzluğu gözden geçirerek,

2)  Uygunsuzluğun nedenleri belirlenerek ve

3)  Benzer uygunsuzlukların var olup olmadığını veya olasılıkla gerçekleşip gerçekleşmeyeceğini belirleyerek,

c)  Gerekli tüm faaliyetlerin uygulanması,

d)  Tüm düzeltici faaliyetlerin etkinliğinin gözden geçirilmesi ve

e)  Gerekli olan durumlarda yapay zeka yönetim sisteminde değişikliklerin yapılması.

f )  Uygunsuzlukların doğası ve gerçekleştirilen müteakip eylemler ve herhangi bir düzeltici faaliyetin sonuçları.

Düzeltici faaliyetler, karşılaşılan uygunsuzlukların etkilerine uygun yapılarak muhafaza edilmektedir.

**Bu kısımdan sonraki madde numaralarının başına “EK-A Kontrol” getirilerek ifade edilecektir.**

**5.1 Bilgi güvenliği politikaları**

Bilgi güvenliği politikaları tanımlanarak, yönetim tarafından onaylı haliyle yayınlanmakta ilgili personele ve ilgili taraflara iletilmektedir. İgili taraflarca kabul edilerek ve planlı aralıklarla ve önemli değişikliklerde gözden geçirilmektedir.

1. Yönetim yönünün sürekli uygunluğunu, yeterliliğini, etkinliğini ve bilgi güvenliği desteğini ticari, yasal, kanuni, düzenleyici ve sözleşme gerekliliklerine uygun olarak hazırlanmaktadır.
2. Bilgi güvenliği politikası, iş stratejisi, düzenlemeler, mevzuat ve sözleşmeler, mevcut ve öngörülen bilgi güvenliği riskleri ve tehditleri gereksinimleri dikkate almaktadır.
3. Bilgi güvenliği politikasında bilgi güvenliğinin tanımı, bilgi güvenliği hedefleri veya bilgi güvenliği hedefleri belirlemek için çerçeve ilgili ifadeleri içermektedir.
4. Yönetim yönünün sürekli uygunluğunu, yeterliliğini, etkinliğini ve bilgi güvenliği desteğini ticari, yasal, kanuni, düzenleyici ve sözleşme gerekliliklerine uygun olarak hazırlanmaktadır..
5. Bilgi güvenliği politikası, iş stratejisi, düzenlemeler, mevzuat ve sözleşmeler, mevcut ve öngörülen bilgi güvenliği riskleri ve tehditleri gereksinimleri dikkate almaktadır.
6. Bilgi güvenliği politikasında bilgi güvenliğinin tanımı, bilgi güvenliği hedefleri veya bilgi güvenliği hedefleri belirlemek için çerçeve ilgili ifadeleri içermektedir.
7. Bilgi Güvenliği Politikasının gözden geçirilmesi
8. Risk Yönetim Metodolojisinin onaylanması
9. Güncel risk raporunun değerlendirilmesi
10. Kabul edilebilir risk seviyesinin Genel Müdür tarafından onaylanması
11. Kabul edilebilir risklerin Genel Müdür tarafından onaylanması
12. Risk işleme planının Genel Müdür tarafından onaylanması
13. Güvenlik ihlal olaylarının değerlendirilmesi
14. İş süreklilik stratejisinin gözden geçirilmesi
15. İş sürekliliği tatbikat sonuçlarının değerlendirilmesi
16. Bilgi güvenliği bilinçlendirme çalışmalarının gözden geçirilmesi
17. İç denetim raporlarının değerlendirilmesi
18. Kurumu etkileyebilecek önemli değişiklikler.

**5.2 Rol ve Sorumluluklar**

Bilgi varlıklarının teknik sahipleri bilginin gizlilik bütünlük ve kullanılabilirliğini sağlamak için;

1. Bilgi varlıklarına yetkisiz olarak erişilmesini; bilgi varlıklarının yetkisiz olarak değiştirilmesini veya tahribatını önlemek suretiyle, bilgi varlıklarını korurlar.
2. Operasyonun mümkün olan en kısa hizmet kesintisi ile devam etmesini sağlamak için gerekli süreçlerin tanımlanmasını ve uygulanmasını sağlarlar.
3. Bilgi güvenliği gerekliliklerini gözetirken, ihtiyaç duyulduğunda bilgiye hızla erişilebilmesi için karmaşıklığı ortadan kaldıracak dengeyi kurarlar.
4. Çalışanlarını ve birlikte çalıştıkları üçüncü taraf çalışanlarını bilgi güvenliği gereklilikleri, rolleri ve sorumlulukları konusunda bilgilendirirler ve bilinçlendirirler.

Bütün bu faaliyetlerin kurumsal ISO/IEC 27001 standardı ile uyumlu bir çerçevede ele alınması için, tüm kurumumuzun süreç ve hizmetlerini kapsayan bir Bilgi Güvenliği Yönetim Sistemi kurulmuş, Bilgi Güvenliği Yöneticisi atanmış ve Bilgi Güvenliği Komitesi kurulmuştur.

**Bilgi Güvenliği Komitesi**

Bilgi Güvenliği Komitesi (BGK) aşağıdaki kişilerden oluşur;

Bilgi Güvenliği Yöneticisi, Bilgi Güvenliği Sorumlusu, Bilgi Güvenliği Komite diğer üyeleri

BGK, yılda bir, Bilgi Güvenliği Yöneticisinin oluşturduğu gündem çerçevesinde toplanır. Bu toplantılar aynı zamanda yönetim gözden geçirme toplantılarıdır.

Toplantılarda görüşülen konular aşağıda belirtilen maddeleri içerir, ancak bunlarla sınırlı kalmayabilir;

1. Bilgi Güvenliği Politikasının gözden geçirilmesi
2. Risk Yönetim Metodolojisinin onaylanması
3. Güncel risk raporunun değerlendirilmesi
4. Kabul edilebilir risk seviyesinin Genel Müdür tarafından onaylanması
5. Kabul edilebilir risklerin Genel Müdür tarafından onaylanması
6. Risk işleme planının Genel Müdür tarafından onaylanması
7. Güvenlik ihlal olaylarının değerlendirilmesi
8. İş süreklilik stratejisinin gözden geçirilmesi
9. İş sürekliliği tatbikat sonuçlarının değerlendirilmesi
10. Bilgi güvenliği bilinçlendirme çalışmalarının gözden geçirilmesi
11. İç denetim raporlarının değerlendirilmesi
12. Kurumu etkileyebilecek önemli değişiklikler.

**5.3. Görevlerin ayrılığı**

Görevlerin ve sorumluluk alanlarının ayrılığı, bir kişinin potansiyel olarak çelişkili görevleri kendi başına yürütmesini önlemek için farklı kişiler arasında çelişen görevleri ayırmayı amaçlama ilkesine göre oluşturularak uygulanmaktadır.

Hangi görev ve sorumluluk alanlarının ayrılması gerektiğini aşağıda, ayrım gerektirebilecek faaliyetlere örnekler ile verilmiştir:

a) bir değişikliği başlatmak, onaylamak ve uygulamak;

b) erişim haklarını talep etmek, onaylamak ve uygulamak;

c) kodun tasarlanması, uygulanması ve gözden geçirilmesi;

d) yazılım geliştirmek ve üretim sistemlerini yönetmek;

e) uygulamaları kullanma ve yönetme;

f) uygulamaları kullanma ve veritabanlarını yönetme;

g) bilgi güvenliği kontrollerinin tasarlanması, denetlenmesi ve sağlanması.

**5.4 Yönetim sorumlulukları**

Yönetim, bilgi güvenliği politikasını, konuya özel politikaları, prosedürleri ve bilgi güvenliği kontrollerini desteklediğini yapılan toplantı ve komite toplantıları ile sürdürmektedir.

Yönetim sorumlulukları, personelin aşağıdakileri sağlamasını içermektedir.

a) kuruluşun bilgilerine ve diğer ilgili varlıklara erişim verilmeden önce bilgi güvenliği rolleri ve sorumlulukları hakkında uygun şekilde bilgilendirme,

b) kuruluş içindeki rollerine ilişkin bilgi güvenliği beklentilerini belirten yönergeler ile sağlanması,

c) kuruluşun bilgi güvenliği politikasını ve konuya özel politikalarını yerine getirmesi,

d) kuruluş içindeki rolleri ve sorumlulukları ile ilgili bir bilgi güvenliği farkındalığı düzeyine ulaşmaları için yürütülen faaliyetler,

e) kuruluşun bilgi güvenliği politikası ve uygun çalışma yöntemleri dahil olmak üzere istihdam, sözleşme veya sözleşmenin hüküm ve koşullarına uygunluk,

f) sürekli mesleki eğitim yoluyla uygun bilgi güvenliği becerilerine ve niteliklerine sahip olmayı sürdürmek,

g) mümkün olduğu durumlarda, bilgi güvenliği politikası, konuya özgü politikalar veya bilgi güvenliği prosedürleri (“ihbar”) ihlallerini bildirmek için uygulama kanallarının oluşturulması, bu bildirime izin verebilir veya bildirimde bulunanın kimliğine ilişkin bilginin yalnızca bu tür bildirimlerle ilgilenmesi gereken kişiler tarafından bilinmesini sağlayacak hükümlere sahip altyapının sağlanması,

h) kuruluşun güvenlikle ilgili süreçlerini ve kontrollerini uygulamak için yeterli kaynaklar ve proje planlama sürelerinin sağlanması

**5.5 Yetkililerle ve Otoritelerle İletişim**

Kurumumuz, ilgili otoritelerle iletişim kurmakta ve sürdürmektedir.

Kurumumuz, yetkililerle (örn. kolluk kuvvetleri, düzenleyici kurumlar, denetim makamları) ne zaman ve kimler tarafından temasa geçilmesi gerektiğini ve tespit edilen bilgi güvenliği olaylarının nasıl zamanında raporlanması gerektiğini “İletişim Listesinde” belirtmektedir.

**5.6 Özel ilgi Gruplarıyla İletişim**

Kurumumuz, özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel derneklerle iletişim kurmakta ve sürdürmektedir.

Özel ilgi gruplarına veya forumlara üyelik, aşağıdakiler için bir araç olarak düşünülmektedir.

a) en iyi uygulamalar hakkındaki bilgileri geliştirmek ve ilgili güvenlik bilgileriyle güncel kalmak,

b) bilgi güvenliği ortamı anlayışının güncel olmasını sağlamak,

c) saldırılar ve güvenlik açıklarıyla ilgili uyarılar, tavsiyeler ve yamalar hakkında erken uyarılar alın,

d) uzman bilgi güvenliği tavsiyesine erişim elde edin,

e) yeni teknolojiler, ürünler, hizmetler, tehditler veya güvenlik açıkları hakkında bilgi paylaşmak ve değiş tokuş etmek,

f) bilgi güvenliği olaylarıyla uğraşırken uygun irtibat noktaları sağlanmaktadır.

Kurumumuz, özel ilgi gruplarıyla iletişim (örn. güvenlik forumları, teknolojik dernekler vb.) ne zaman ve kimler tarafından temasa geçilmesi gerektiğini ve tespit edilen bilgi güvenliği olaylarının nasıl zamanında raporlanması gerektiğini “İletişim Listesinde” belirtmektedir.

**5.7 Tehdit İstihbaratı**

Bilgi güvenliği tehditleri ile ilgili bilgiler toplanmalı ve tehdit istihbaratı oluşturmak için analiz edilmektedir.

Tehdit istihbaratı faaliyetleri şunları içermektedir.

a) tehdit istihbaratı üretimi için hedefler belirlemek,

b) tehdit istihbaratı üretimi için gerekli bilgileri sağlamak için gerekli ve uygun olan iç ve dış bilgi kaynaklarının belirlenmesi, incelenmesi ve seçilmesi,

c) dahili ve harici olabilen seçilmiş kaynaklardan bilgi toplamak,

d) toplanan bilgileri analize hazırlamak için işleme (örneğin bilgileri çevirerek, biçimlendirerek veya doğrulayarak),

e) kurumumuzla nasıl ilişkili ve anlamlı olduğunu anlamak için bilgileri analiz etmek;

f) anlaşılabilir bir formatta ilgili kişilere iletilmesi ve paylaşılması.

Tehdit istihbaratı analiz edilmekte ve daha sonra kullanılmak üzere ders çıkarılmaktadır.

a) tehdit istihbaratı kaynaklarından toplanan bilgileri kurumumuzun bilgi güvenliği risk yönetimi süreçlerine dahil etmek için süreçler uygulayarak,

b) güvenlik duvarları, izinsiz giriş tespit sistemi veya kötü amaçlı yazılım önleme çözümleri gibi teknik önleyici ve tespit edici kontroller ek girdi olarak,

c) bilgi güvenliği testi süreçlerine ve tekniklerine girdi olarak.

Kurumumuz, genel tehdit istihbaratını iyileştirmek için tehdit istihbaratını diğer kurumumuzlarla karşılıklı olarak paylaşmaktadır.

 **Tehdit ve Zafiyet Tanımlama**

Şirket içi ve dışında meydana gelebilecek potansiyel tehditler düzenli olarak değerlendirilir.

Sistemlerdeki zaafiyetler düzenli olarak taranır ve belirlenir.

**Tehdit ve Zafiyet Önleme ve Korunma**

 Güvenlik önlemleri, siber tehditlere karşı etkin bir şekilde koruma sağlar.

* Zafiyetlerin giderilmesi için düzeltici önlemler alınır ve güvenlik açıkları kapatılır.
* Firewall yönetimleri bilgili kişilerce yapılır ve kurallar sınırlandırılır.

**Olay Müdahalesi ve Yanıt**

* Olası bir siber saldırı durumunda, hızlı yanıt ve müdahale planları uygulanır.
* Olaylar kaydedilir, incelenir ve raporlanır.

**Sürekli İyileştirme**

* Tehdit ve zaafiyetlerle ilgili sürekli olarak değerlendirme yapılır ve politika ve prosedürler güncellenir.
* Çalışanlar, güvenlik eğitimlerine düzenli olarak tabi tutulur ve farkındalık artırılır.

**Uyumluluk ve İyileştirme**

* Kurumumuz, politika ve prosedürleri, uyum sağlamak için ulusal ve uluslararası standartlarla uyumlu olmaktadır.
* Performans ve uyumluluk düzenli olarak değerlendirilir ve iyileştirme alanları belirlenir.

Bu kurallar Kurumumuz tarafından siber tehditlere karşı korunma ve güvenlik zafiyetlerinin yönetimi için kabul edilmiştir.

Kurumumuz, tehdit istihbarat ekipleriyle iletişim (örn. güvenlik ekibi, dış kaynak destek alınan kurum vb.) ne zaman ve kimler tarafından temasa geçilmesi gerektiğini ve tespit edilen bilgi güvenliği olaylarının nasıl zamanında raporlanması gerektiğini “İletişim Listesinde” belirtmektedir.

**5.8 Proje Yönetiminde Bilgi Güvenliği**

Bilgi güvenliği proje yönetimine entegre edilmektedir.

Bilgi güvenliği risklerinin proje yönetiminin bir parçası olarak ele alınmasını sağlamak için bilgi güvenliği proje yönetimine entegre edilmektedir. Bu, karmaşıklığı, boyutu, süresi, disiplini veya uygulama alanı ne olursa olsun her tür projeye uygulanabilir (örneğin, temel iş süreci, BİT, tesis yönetimi veya diğer destekleyici süreçler için bir proje).

Kullanılan proje yönetimi şunları gerektirmektedir:

a) bilgi güvenliği riskleri erken bir aşamada ve proje yaşam döngüsü boyunca proje risklerinin bir parçası olarak periyodik olarak değerlendirilir ve ele alınır,

b) bilgi güvenliği gereksinimleri [örn. uygulama güvenlik gereksinimleri, fikri mülkiyet haklarına uyum gereksinimleri ) vb.] projelerin ilk aşamalarında ele alınır,

c) İç ve dış iletişim unsurlarının güvenliği gibi projelerin yürütülmesiyle ilgili bilgi güvenliği riskleri, proje yaşam döngüsü boyunca dikkate alınır,

d) bilgi güvenliği risk tedavisindeki ilerleme gözden geçirilir ve tedavinin etkinliği değerlendirilir ve test edilir.

Bilgi güvenliği hususlarının ve faaliyetlerinin uygunluğu, proje yönlendirme komitesi gibi uygun kişiler veya yönetişim organları tarafından önceden tanımlanmış aşamalarda izlenmektedir.

**5.9.Bilgi Envanteri ve Diğer İlgili Varlıklar**

Kurum, bilgilerini ve diğer ilişkili varlıkları “Bilgi Güvenliği Varlık Envanterinde” tanımlama ve bunların bilgi güvenliği açısından önemini belirlemektedir.

Bilgi envanteri ve diğer ilgili varlıklar doğru, güncel, tutarlı ve diğer envanterlerle uyumlu halde bir bilgi envanterinin ve diğer ilişkili varlıkların doğruluğunu sağlamaya yönelik çalışmalar ile sağlanır.

Kurumumuz için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlar bilgi varlığı envanterinin kapsamındadır. Örneğin; Ağ cihazlari, Bilgi, Donanımlar, İş süreçleri ve hizmetleri, Kritik birim ve personeller, Organizasyon, Fiziksel tesis ve ortamlar, Yazilimlar gibi işletme için bir değer ifade eden tüm unsurlar bilgi varlık olarak değerlendirilmektedir. Örneklerde verilen varlıklar içerisinde en soyut olanı bilgidir. Bilgi; bir organizasyonun tüm süreçlerinde yer alabilir. Donanımlar ve yazılımlar bilgiyi işler, donanımlarda ve medyalarda (CD, USB depolama üniteleri) depolanır, dokümanlarda yazılı olarak bulunur. Ayrıca bilgi, kurum çalışanlarının zihinlerinde, konuşmalarında bulunur.

**Varlık Ana Kategorileri**

* Ağ cihazlari
* Bilgi
* Donanımlar
* İş süreçleri ve hizmetleri
* Kritik birim ve personeller
* Organizasyon
* Fiziksel tesis ve ortamlar
* Yazilimlar

**Varlık Alt Kategorisi**

* Ağ Bileşenleri
* Güvenlik Sistemleri
* Basılı Kayıtlar
* Elektronik Kayıtlar
* Bakım Ekipmanları
* Depolama Sistemleri
* İş İstasyonları
* Mobil Cihazlar
* Monitörler
* Ofis Ekipmanları
* Operatör Konsolları
* PC'ler
* Enerji Donanımları
* Sunucular
* Süreçler
* 3.Taraf Hizmetler
* Birimler
* Personeller
* İç Konular
* Dış Konular
* Otoriteler
* Fiziksel Tesisler
* Fiziksel Ortamlar
* Yazılımlar
* Lisanslar

varlık adı gibi tanımlanır.

**Varlık Adı**

Varlığın açık adı yazılır.

**Varlık Açıklaması**

* Switch, router (kenar, omurga vb), modem, vb.
* Ağ güvenliği ve fiziksel güvenliğe ait sistemler (Örn: Firewall, vb.)
* Arşiv dokümanları, Scada dokümanları (sistem konfigürasyonu), felaket kurtarma dokümaları, zimmet formları, müşteri abonelik sözleşmeleri, faturalar, vb.
* Bordro, sözleşme, otomasyon çizimleri, mutabakat formları, müşteri abonelik sözleşmeleri, faturalar, zimmet formları, vb.
* Sistem bakım ekipmanları
* SAN, Data Domain, Teyp, vb.
* Scada iş istasyonları, vb.
* Tablet, Scada tablet, cep telefonu, telsiz, taşınabilir hard disk, vb.
* Kullanıcı monitörleri, iş istasyonu monitörleri, vb.
* Faks, yazıcı, monitor, projektör, vb.
* Operatör konsolu, vb.
* Dizüstü bilgisayarlar
* UPS, Jeneratör, kamera, vb.
* Test, uygulama, geliştirme, veritabanı sunucuları, web sunucuları, vb.
* Kurumdaki ele geçirilmemesi, değiştirilmemesi gerekli bilgiler içeren süreçler veya sürekliliği organizasyonun iş hedefleri ve itibarı için önemli olan süreçler (örn: insan kaynakları süreci, muhasebe süreci, satın alma süreci, vs.).
* IT ve OT’nin sunduğu hizmetler. Örneğin; arıza bakımları, jeneratör, UPS), helpdesk hizmeti, network hizmeti vb. (Bu varlık kategorisindeki varlıklar için RPO ve RTO değerleri belirlenmelidir.)
* Kritik birimler (Ör. İnsan kaynakları departmanı, vb.)
* Ünvan bazında kritik karar vericiler, kullanıcılar, işletim/yönetim çalışanları, geliştiriciler, vb. kurum personelleri ile tedarikçiler (Ör. BT çalışanları, yöneticiler, vb.)
* Departmanlar, kurumda belirlenmiş rol ve sorumluluklar, sözleşmesel düzenlemeler, hizmet seviyesi anlaşmaları (SLA), yasal ve mevzuata dayalı yaptırımlar
* Politik değişimler, ekonomik değişimler, sektörel değişimler, belgelendirme sürecindeki değişimler, müşteri sayısı, tedarikçi yetkinliği, vb.
* Düzenleyici kurumlar, devlet kurumları, vs. (SGK, belediye, vs.)
* Merkez bina, sistem odası, ups odası, ofisler, arşiv, ek bina, vb.
* UPS, Jeneratör, kamera odası vb.
* Kurumda kullanılan tüm yazılımlar (IPS, IDS, Firewall, kamera sistemi, şifreleme yazılımları, Scada yazılımları, vb.) (Bu varlık kategorisindeki varlıklar için RPO ve RTO değerleri belirlenmelidir.)
* Microsoft Office lisansları, SAP lisansları, antivirüs yazılımı lisanları, vb. tüm lisans gerektiren uygulamaların lisansları

**Varlık Statüsü** (Aktif (Kullanımda) mı?)

Varlığın durumu yazılır.

**Aktif:** Varlık yaşam döngüsü devam ediyorsa, varlık kullanımdaysa.

**Pasif:** Varlık kullanımdan kalktıysa

**Varlık Tanımı**

Varlıkla ilgili kısa bir tanım yazılır.

**Varlık Sahibi Ünvanı**

Varlık sahibi kişinin ünvanı yazılır.

**Varlık Sahibi Departman**

Varlığın sahibi olan departman yazılır.

**Varlığın Bulunduğu Lokasyon**

Varlığın bulunduğu yer yazılır.

**Kritiklik Değerleri**

**Gizlilik**

Bilginin sadece erişmesine izin verilen kişi veya kitleler için erişilebilir halde olmasıdır. Hedeflenen kişi ve kitleler dışında bilginin başkaları tarafından okunabilir ve/veya yazılabilir, değiştirilebilir, kısaca erişilebilir olması durumunda bilginin gizliliği bozulmuş olur.

**Bütünlük**

Bilginin kaynağında olduğu şekliyle, bozulmadan, değiştirilmeden, tutarlı bir şekilde hedeflenen kişi ve kitleler için erişilebilir olmasıdır. Bir bilginin kısmen bozulmuş veya kısmen değiştirilmiş olması bütünlüğün bozulması anlamına gelmektedir.

**Erişebilirlik**

Bilginin ihtiyaç duyulduğunda erişilebilir halde olmasıdır. Gizlilikten farkı, kimlerin bilgiye erişebildiğinden çok, bilginin erişilebilir olup olmaması ile ifade edilmesidir.

Envanter içerisindeki “Kritiklik Değerleri” sayfasında yer alan dereceler ve tanımları referans alınır ve tanımlanan 5 kritiklik seviyesinden biri seçilir.

**Varlık Değeri**

Belirlenen gizlilik, bütünlük ve erişilebilirlik değerlerinin çarpımı ile oluşturulur, varlık değeri 64 puan üstü Risk analizinde değerlendirmeye alınır.



**Varlık Gizlilik Sınıfı ve Etiketlenmesi**

Bilgi, koruma seviyesinin gerektirdiği şekilde sınıflandırılır. Bu sınıflandırmada üzerinde durulması gereken nokta; bilgilerin yetkisi olmayan kişiler tarafından okunması veya elde edilmesi durumunda ortaya çıkacak sonuçların potansiyel etkileridir. Sınıflandırma işlemi basitçe, bu bilgilerin oluşturulmasını sağlayan ve bilgi ile ilgili süreçleri düzenlemesine izin verilen kişiler tarafından tanımlanır. Belgeler sınıflandırılırken, içerdiği en önemli veri baz alınır ve bir belge sadece bir sınıfa ait olabilir.Tipik bir sınıflandırma şemasında; koruma gerektiren, koruma gerektirmeyen yada herkes tarafından serbestçe kullanılabilen gibi üç veya daha fazla sınıflandırma olabilir.

Bilgi sınıflandırma sisteminde ilk olarak, kuruma ait bilgilerin, özelliklerine göre sınıflandırılması gerekmektedir. Sınıflandırılmayan bilgi ve belgeler, kurum için potansiyel veri kaybı riski taşımaktadır. Sınıflandırılmayan tüm bilgi ve belgelere öncelikle bir sahip belirlenmeli ve tanımlanmamış bilgi sahiplerinin bu bilgileri ele alarak sınıflandırmasının yapılması istenmelidir. Bilgi sahibi belirlenirlenmesinde bilginin genel özellikleri baz alınır. (Kalite ile ilgili bir döküman gibi) Böylece bilgi sınıflandırma bir süreç olarak başlatılmalı, sürecin en kısa sürede tamamlanması için birim yöneticileri ve üst yönetimin desteği alınmalıdır. Bir kez sınıflandırılan belgeler sınıflandırma şemasında yerini alarak zaten oturmuş olan bilgi sınıflandırması yapısına göre işlem görecektir ve daha fazla kurum için risk taşımayacaktır.

Etiketleme,

Kurumumuz varlık envanterinde tanımlandığı şekilde kullanılır.

A- Ağ cihazları

B- Bilgi varlıkları

D- Donanım

İ-  İş Süreçleri

K- Kritik Personel

O- Organizasyonel Bilgi

F- Fiziksel tesis ve ORtamlar

Y- Yazılımlar

Varlık Sınıfları ve renk kodları aşağıdaki şekilde tanımlanmıştır.

1000 - Kırmızı Hassas

2000 Turuncu Kişisel

3000 Sarı Gizli

4000 Mavi Kurum İçi

5000 Yeşil Genel



**RTO Kurtarma Zamanı**

Varlığın kesinti sonrasında sistemlerin ve uygulamaların ne kadar sürede tekrar çevrimiçi olması gerektiğini tanımlayan bir değeri ifade eder.

**RPO Kurtarma Noktası**

Verinin ne kadar zaman önceki haline dönebildiğinizi ifade eder

**Saklama Süresi**

Varlık verisinin sistemlerde ne kadar süre ile tutulacağını ifader eder.

**Versiyon**

Varlığın sistemlerde kullanılan sürüm bilgisini ifade eder.

**Notlar**

Varlık ile ilgili herhangi bir ek ya da açıklayıcı bilgi yazılabilir.

**Varlık Envanteri Yönetimi**

Varlıklar süreçler üzerinden tanımlancaktır. Varlık envanteri birden fazla tabloda tutulabileceği gibi tek bir tabloda da tutulabilir. Varlık sayısı çok yüksek mertebelerde ise varlıkların; yazılım, donanım, bilgi, süreç gibi ayrı ayrı envanterlerde tutulmasında fayda vardır.Tek bir envanter halinde tutulmak istenirse, varlıkları envantere mantıksal gruplar halinde işlemek tüm varlıkların kapsandığından emin olunmasını sağlayacaktır. Dosya doldurulurken combobox olan menüler combobox tan seçilerek doldurulacak , formül olan hücrelerin formülü değiştirilmeyecektir.

**5.10 Bilgi Varlıkları ve Kaynaklarının Kabul Edilebilir Kullanımı**

 Yürütülen işlerin sürekliliğinin ve gelişiminin sağlanması nedeniyle, bilginin gizliliğinin korunması öte yandan bilginin ve fikirlerin paylaşılması ve yaygınlaştırılması gerekir. Bilginin hassasiyeti ve güvenliği ile ilgili ihtiyaçlar gözetilirken, aynı zamanda bilgiye ihtiyaç anında hızla ulaşılması büyük önem taşımaktadır. O nedenle, bilgi kaynaklarının değerinin iyi tespit edilmesi, bilginin korunmasını sağlayacak çaba ve maliyetin bilginin hassasiyeti ile orantılı olması gerekir.

 Kurumumuz firmasının bilgi kaynaklarını kullanarak etik dışı veya yasalara karşı faaliyetlerde bulunmak, hiç kimse için kabul edilemez.

 Bu politikanın asgari gereği olarak,

1. Verinin kasıtlı olarak değiştirilmesi,
2. Kasıtlı olarak veride hataların oluşmasına veya veri kaybına neden olunması,
3. Bilgi kaynaklarının yasaları ihlal eden bir faaliyet için kullanılması,
4. Bilgi güvenliğinin ihlal edilmesi veya suiistimal edilmesi;
5. Cihazların, yazılımların veya herhangi diğer bir bilgi kaynağının çalınması, tahrip edilmesi,
6. Bilgi kaynaklarının bilişim sistemlerinin performans kaybına sebep olacak şekilde kullanılması,
7. Tesislerin, fiziksel cihazların, ağların tahrip edilmesi kabul edilemez.

 Bu ve benzeri faaliyetler ve teşebbüsler disiplin suçu olarak ele alınır, gereken disiplin süreçleri ve yasal süreçler uygulanır.

Belirtilen tarzda bilgi güvenliği ihlallerinin, ihlal teşebbüslerinin veya bu tür ihlaller ile sonuçlanabilecek zafiyetlerin, tespit edildiği anda zaman kaybetmeden Bilgi Güvenliği Yöneticisine bildirilmesi gerekir.

**Varlık:** Bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır.İnsan, bilgi, yazılım, donanım, bina, iş araç ve gereçleri gibi işletme için bir değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir. Örneklerde verilen varlıklar içerisinde en soyut olanı bilgidir. Bilgi bir organizasyonda her yerde bulunabilir. Donanımlar ve yazılımlar bilgiyi işler, donanımlarda ve medyalarda (CD, USB depolama üniteleri) depolanır, dokümanlarda yazılı olarak bulunur. Şirket çalışanlarının zihinlerinde, konuşmalarında bulunur.

**Varlık kavramı için örnekler:**

a) Bilgi varlıkları: Kurumumuz .’nin tüm bilgi sistemlerinde, çalışanlarında, dosya kütüphanelerinde tutulan ve şirket iş süreçlerinde değişik formlarda işlenen veridir;

b) Yazılım varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları;

c) Fiziksel varlıklar: Bilgisayar bileşenleri (işlemciler, ekranlar, diz üstü bilgisayarlar, modemler), manyetik ortamlar (kayıt cihazları ve diskler), diğer teknik araçlar (güç kaynakları, havalandırma üniteleri), mobilya, yerleşim düzeni;

d) Servisler (Hizmetler): Bilgi işleme ve haberleşme servisleri (web servisi, e-ticaret servisi, ftp servisi), genel faydalar; örneğin ısınma, ışıklandırma, elektrik, havalandırma.

e) İnsan: Şirket çalışanları da şirket varlığı olarak düşünülmelidir.

**Gizlilik:** Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Örn: Şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir)

**Bütünlük:** Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Örn: Veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması, dijital imza)

**Erişilebilirlik/Kullanılabilirlik:** Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Diğer bir ifade ile, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır. (Örn: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şasilerinde yedekli güç kaynağı kullanımı). Bu dokümanda “Erişilebilirlik” olarak kullanılacaktır.

Varlık Sahibi: Varlığın gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanmasından birinci derecede sorumlu kişi veya kişilerdir. Sahip kelimesi Türkçe de mülkiyet anlamını içinde barındırmaktadır. Bilgi Güvenliği Yönetim Sistemi Varlık yönetimindeki sahip kavramı daha çok sorumluluk anlamında kullanılmaktadır. Varlık değerinin belirlenmesi, varlığa yönelik risk tanımlamalarının yapılması varlık sahibinin görevleri arasındadır. (Örn: Şirket finansal bilgilerinin sahibi şirketin finans bölüm müdürüdür)

Varlık Yedek Sahibi: Varlığın sahibi olmamasına rağmen, varlığın sağlıklı bir şekilde

sürekliliğinin idamesini sağlayan rolündeki kişi veya kişilerdir. Birçok durumda varlık

sahibi ile farklı kişi olabilir. (Örn: Şirket finansal bilgilerinin sahibi finans bölümü müdürü iken emanetçisi ilgili veri tabanı yöneticisidir.)

**Genel Kurallar**

Kurumumuz, bilgi ve haberleşme sistemleri ve donanımları (İnternet, e-posta, bilgisayarlar, Bulut sistemleri) kurum işlerinin yürütülmesi için kullanılmalıdır. Bu sistemlerin yasa dışı, rahatsız edici, kurumun diğer politika, standart ve rehberlerine aykırı veya kuruma zarar verecek herhangi bir şekilde kullanımı bu politikanın ihlal edildiği anlamına gelir.

Kurumumuz bu sistemleri ve bu sistemlerle gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak denetleme hakkını saklı tutar.

Aşağıdaki kurallar uyulması gereken kuralların kapsamlı bir listesi olarak düşünülmemelidir. Gerçekleştirilen aktiviteler buradaki kurallarla tutarlı olmaktadır.

**Kabul Edilebilir Kurumsal Kullanım**

* Kurum internet kaynakları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
* Kurum çıkarlarıyla çakışmadığı sürece internet kaynaklarının kişisel kullanımına kısıtlı olarak izin verilmektedir.
* Kurum internet kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulmaktadır.
* Kullanıcılar kendi kullanıcı hesaplarıyla internet üzerinde gerçekleştirilen tüm işlemlerden sorumludur. Bunun için kullanıcılar kimlik bilgilerini uygun şekilde saklamalı ve başkaları ile paylaşmamaktadır.

**Uygunsuz Kullanım**

* Kurum internet kaynakları hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişemez ve kurumun normal operasyon ve iş aktivitelerini engelleyemez.
* Kurum kaynakları uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz
* Odanın resmi işlerinin yürütülmesi dışında kurumsal mail adresi ile sohbet gruplarına, forumlara, elektronik haber gruplarına katılmak yasaktır.
* Kullanıcıların sistemi kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır.
* Yazılı olarak izin verilmedikçe port taraması veya güvenlik taraması yapılamaz.
* Yazılı olarak izin verilmedikçe ağın izlenmesi ve kullanıcın kendisi için olmayan veriyi almaya çalışması yasaktır.
* Kurumun kritik bilgisinin ortaya çıkmasını veya kurum servislerinin ulaşılamaz hale gelmesini sağlayacak tüm aktiviteler yasaktır.

**İndirilen Yazılım**

* İndirilen tüm yazılımlar kullanılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilmektedir.

**İzleme**

* Kurum, internet sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.
* Kurum, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.

**Kabul Edilebilir E-posta Kullanım Kuralları**

**Kurumsal Kullanım**

* Kurumumuz, e-posta kaynakları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
* Kurumumuz, çıkarlarıyla çatışmadığı sürece e-posta kaynaklarının kişisel kullanımına kısıtlı olarak izin verilmektedir.
* Kurumumuz e-posta kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.
* Kullanıcılar kendi kullanıcı hesaplarıyla gerçekleştirilen tüm e-posta işlemlerinden sorumludur.

**Uygunsuz Kullanım**

* Kurumumuz, e-posta kaynakları hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişemez ve kurumun normal operasyon ve iş aktivitelerini engelleyemez.
* Kurumumuz, e-posta kaynakları uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz.
* Kullanıcıların e-posta sistemini kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır.
* Kurumumuz, e-posta kaynakları; “zincir e-postalar”, reklam, aldatma, karalama gibi istenmeyen mesajlar (SPAM) göndermek için kullanılamaz.
* E-posta sisteminin izinsiz kullanımı ve mesaj içeriğinde veya başlığında sahtecilik yapılması yasaktır.
* Kurumumuz, e-posta sistemi, ücretsiz veya ticari hiçbir yazılımın alınması, gönderilmesi veya saklanması için kullanılamaz.
* Tüm e-posta içerikleri ve eklentileri açılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilmelidir.

**E-posta Yazılımı**

* Kullanıcılar sadece kurumun yetkili birimlerince onaylanmış e-posta yazılımlarını ve konfigürasyonlarını kullanabilirler.
* E-posta yazılımının mevcut güvenlik ayarlarını gevşetecek ayarlamalar yapılamaz.
* Kullanıcılar e-posta yazılımının gönderenin kimliğini gizleyecek özelliklerini kullanamazlar.

**İzleme**

* Kurumumuz, e-posta sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.
* Kurumumuz, kullanıcının e-posta sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.

**Uygulama ve Ceza**

* Kabul Edilebilir Kullanım Prosedürüne ve burada belirtilen diğer politika ve prosedürlere uymayanlar hakkında disiplin süreci başlatılır ve yasal işlem uygulanır.

**Gözden Geçirme ve Onay**

* Kabul Edilebilir Kullanım Prosedürünü yılda (1) bir BGYS yöneticisi tarafından gözden geçirilir Genel Müdür onayından sonra yürürlüğe sokulur.

**Genel Kullanım ve Sahip Olma**

* Kullanıcılar şunun farkında olmalıdırlar; kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da kurumun bünyesinde oluşturulan tüm veriler kurumun mülkiyetindedir.
* Çalışanlar bilgi sistemlerini kendi kişisel kullanımı için makul seviyede yararlanabilirler. Her bir departman kendi bilgi sistemlerinin kişisel kullanımı için gerekli kuralları koymalıdır. Birimler böyle bir kural koymamış ise kurumun koyduğu genel güvenlik politikaları geçerlidir.
* Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmelidir.
* Güvenlik ve ağın bakımı amacı ile yetkili kişiler cihazları, sistemleri ve ağ trafiğini gözlemleyebilir.
* Kurumumuz firmasının bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
* Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı, kopyalanmamalıdır.
* Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
* Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemeler hiçbir surette değiştirilmemelidir.
* Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

**Güvenlik ve Kişiye Ait Bilgiler**

* Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları tanımlanmaktadır.
* Şifreleri güvenli bir şekilde tutun ve hesabınızı başka kimselerle paylaşmayın. Sistem seviyeli şifreler yılda 1 bir, kullanıcı seviyeli şifreler ise en az 6 ayda bir değiştirilmektedir.
* Bütün PC ve Laptoplar kullanılmadığı durumlarda otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmektedir.
* Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmaktadır. Bios ve işletim sistemi şifreleri aktif hale getirilmelidir. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmaktadır.
* Laptop bilgisayarın çalınması / kaybolması durumunda, durum fark edildiğinde en kısa zamanda yetkili kişiye haber verilmelidir.
* Bütün cep telefonu ve PDA cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmaktadır. Kullanılmadığı durumlarda kablosuz erişim özellikleri aktif halde olmamaktadır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmaktadır.
* Geçici personel kullanıcı hesapları açılırken sezon sonunda otomatik olarak süresi dolacak şekilde oluşturulur.
* Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar.
* Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler.
* Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olun ve gerekirse dosyaları sıkıştırılmalıdır.
* Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek kuruma veya kişiye yönelik saldırılardan sistemin sahibi sorumludur.

**Güvenlik ve Kişiye Ait Bilgiler**

Genel olarak aşağıdaki eylemler yasaklanmıştır. Sistem yöneticileri bu kapsamın dışında olabilir. Herhangi bir kullanıcı kurumun kaynaklarını kullanarak hiçbir şart altında herhangi bir yasadışı aktivitede bulunamaz.

**Sistem ve Ağ Aktiviteleri**

Aşağıdaki aktiviteler hiçbir istisna olmadan kesinlikle yasaklanmıştır.

* Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer şirket bilgileri, yazılım lisansları vs. haklarını çiğnemek.
* Zararlı programların ağa veya sunuculara bulaştırılması.
* Kendi hesabınızın şifresini başkalarına vermek veya kendi hesabınızı kullandırmak.
* Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmak.
* Ağ güvenliğini etkilemek, ağ haberleşmesini bozmak.
* Kullanıcı kimlik tanıma yöntemlerinden kaçmak.
* Kurum bilgilerini kurum dışından üçüncü şahıslara iletmek.
* Kullanıcıların kişisel bilgisayarları üzerine bilgi işlem bölümünün onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapması.
* Cihaz, yazılım ve verinin izinsiz olarak kurum dışına çıkarılması.
* Kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programları kurmak ve kullanmak yasaktır.

**E-Mail ve Haberleşme Aktiviteleri**

* Kurum dışından web posta sistemini güvenliğinden emin olunmayan bir bilgisayardan kullanmak
* İstenmeyen e-posta mesajlarının iletilmesi. Bunlar karşı tarafın özellikle istemediği reklam mesajlarını içeren mailler olabilir.
* E-posta veya telefon vasıtası ile taciz etmek
* E-posta başlık bilgilerini yetkisiz kullanmak veya değiştirmek
* Zincir e-postaları oluşturmak veya iletmek
* İş ile alakalı olmayan mesajları birçok haber gruplarına iletmek.

**5.11 Varlıkların İadesi**

Personel ve diğer ilgili taraflar, istihdamlarının, sözleşmelerinin veya anlaşmalarının değiştirilmesi veya feshedilmesi üzerine kurumumuzun sahip oldukları tüm varlıkları uygun şekilde iade etmektedir.

Kurumumuz, aşağıdakileri içerebilecek tüm bilgileri ve iade edilecek diğer ilgili varlıkları açıkça tanımlamakta ve belgelemektedir.

a) kullanıcı uç nokta cihazları,

b) taşınabilir depolama cihazları,

c) uzman ekipman,

d) bilgi sistemleri, siteler ve fiziksel arşivler için kimlik doğrulama donanımı (örn. mekanik anahtarlar, fiziksel belirteçler ve akıllı kartlar)

e) bilgilerin fiziksel kopyaları.

**5.12 Bilgilerin Sınıflandırılması**

Kurumumuz’da bilgi aşağıdaki tabloda verildiği şekilde sınıflandırılmıştır.

|  |  |  |
| --- | --- | --- |
|  **Bilgi Sınıfı**  |  **Tanımlama**  | **Örnekler**  |
|  **Genel**  |  Kullanılması ve paylaşılması bilgi güvenliği açısından önemli olmayan herkese açık verilerdir. Veri bütünlüğü önemli değildir. İstenmeyen saldırılar sonucunda, veri kaybı kabul edilebilir.  |  Standartlar, yaygın dağıtımı olan genel bilgiler Resmi kurumlar tarafından istenen finansal raporlar Bilgilendirme için gönderilen bültenler Şirket web sayfaları   |
| **Kurum İçi**  | Şirket dahilinde üretilen, şirket dışına çıkarılması için onay alınması gereken bilgi varlıklarıdır. Şirket içinde kullanımında, kopyalanmasında sakınca yoktur. Yetkisiz erişim, şirketin operasyonel verimliliğini etkileyebilir, rakiplere avantaj sağlayabilir veya müşteri güvenini zedeleyebilir. Veri bütünlüğü önemlidir.  | Standartlar, prosedürler, politikalar Şifreler ve şirketin güvenlik politikaları ile ilgili bilgiler Teknik bilgi (know-how) Şirketin yazdığı her türlü program kaynak kodu   |
| **Gizli**  | Şirketin faaliyetini devam ettirebilmesi için kritik olan ve yetkisiz kişilerin eline geçmesi durumunda, sorunların yaşanacağı bilgi varlıklarıdır. Gerekli izin alınmadan açıklandığında şirketin güvenliğini, güvenilirliğini, saygınlığını ve çıkarlarını ciddi suretle zedeleyebilecek, rakiplere geniş yararlar sağlayabilecek bilgi varlıklarıdır. En yüksek seviyede bütünlük ve gizlilik gerektirir, sınırlı erişim zorunludur.  | Arge bilgileri Şirket bilgi birikimi İhale Dokümanları Stratejik planlar Yatırım Kararlar Organizasyonel Planları Müşteriye ait veriler Müşterilerle olan her türlü yazışma Sözleşmeler   |
| **Kişisel Bilgi**  | Kaybı yada yetkisiz kişilerin eline geçmesi durumunda çok ciddi sorunların yaşanacağı bilgi varlıklarıdır. İzinsiz olarak açıklandığı takdirde şirketin güvenliğini, çıkarlarını ve diğer kurumlarla ilişkilerini olumsuz yönde etkileyebilecek, şirketin maddimanevi büyük zararına neden olabilecek nitelikte olağanüstü önem taşıyan bilgi varlıklarıdır. Şirket içinde bu veriye erişim çok sınırlıdır. Yüksek seviyede bütünlük ve gizlilik gerektirir. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder.  | Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir.  |
| **Hassas Bilgi**  | Özel nitelikli (hassas kişisel veriler) başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olmasına, ayrımcılığa maruz kalmasına ya da şeref ve onurunun zedelenmesine neden olabilecek nitelikteki verilerdir.  | Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli hassas kişisel veriler olarak belirlenmiştir.  |

**5.13 Etiketleme,**

Kurumumuzda varlık envanterinde tanımlandığı şekilde kullanılır.

A- Ağ cihazları

B- Bilgi varlıkları

D- Donanım

İ- İş Süreçleri

K- Kritik Personel

O- Organizasyonel Bilgi

F- Fiziksel tesis ve Ortamlar

Y- Yazılımlar

Varlık Sınıfları ve renk kodları aşağıdaki şekilde tanımlanmıştır.

1000 Kırmızı Hassas

2000 Turuncu Kişisel

3000 Sarı Gizli

4000 Mavi Kurum İçi

5000 Yeşil Genel

**5.14 Bilginin Transferi**

Yapılan toplantılarda kuruma ait bilgiler hakkında konuşulması, kurum içinde evraklar ile yapılan işlemler, bilgi sistemleri üzerinde yapılan sorgulama, hesaplama, raporlama, vb. işlemler “bilgi varlıklarının işlenmesi” kapsamında değerlendirilen örnek durumlardır.

Bilginin, yazılı, sözlü, görsel ortamlarda işlenmesi söz konusu olduğunda, bilginin kullanıldığı ortamın ve altyapının, Bilgi İşlem bilgi güvenliği politika ve prosedürlerine uygunluğu sağlanmalı; bilgiyi kullanan tüm tarafların da bu politika ve prosedürlerin gereklerinden haberdar olduğundan ve bunlara uyduğundan emin olunmalıdır.

Hassas, kişisel ve gizlilik dereceli bilgiler kamuya açık alanlarda kullanılmaz (okunmaz, tartışılmaz, vb.).

Hassas, kişisel ve gizlilik dereceli bilgiler üzerinde çalışma yapılırken, bu bilgilere erişim yetkisi olduğundan emin olunmayan bir başka kişinin çalışma ortamına gelmesi durumunda, fiziksel veya elektronik ortamdaki bu bilgiler, gelen kişinin erişimini veya görüşünü engelleyecek şekilde korunur.

Hassas, kişisel ve gizlilik dereceli bilgiler ile ilgili çalışmalar ortak alanlarda yapıldığında (örn. toplantı salonları) bu ortam terk edilirken, geride hiçbir bilgi ve belge kalmayacak şekilde kontrol ve temizlik yapılır.

Çalışmanın yürütülmesinden sorumlu birim yöneticisinin izni olmadıkça, hassas, kişisel ve gizlilik dereceli belge ve bilgilerin kullanıldığı çalışmaların yürütüldüğü ortamda herhangi bir kayıt işlemi (ses kaydı, görüntü kaydı, vb.) yapılamaz.

**Güvenli Bilgi Aktarımı**

Hassas, Kişisel veya Gizlilik dereceli bilgilerin aktarımından önce, bilgiyi talep edenin bu bilgiye erişim yetkisi bulunduğundan emin olunur. Erişim yetkisinin bulunduğunu belgelendirme sorumluluğu bilgiyi talep eden tarafındır. Şifahi olarak gizlilik dereceli bilgilerin Bilgi İşlem Birimi içinde ve dışında aktarımı söz konusu olamaz.

**Her türlü bilgi aktarımı için kurallar;**

Aktarılan bilgileri ele geçirme, yetkisiz erişim, kopyalama, değiştirme, yanlış yönlendirme, imha ve hizmet reddine karşı korumak için tasarlanmış kontroller, dahil olan bilgilerin sınıflandırılmasıyla orantılı erişim kontrolü seviyeleri ve hassas bilgileri korumak için gerekli olan herhangi bir özel kontrol, örneğin; kriptografik tekniklerin kullanımı gibi gelişmiş teknolojik çözümler kullanılır.

Hassas, Kişisel veya Gizlilik dereceli bilgilerin aktarım sırasında bilgi için bir gözetim zincirinin sürdürülmesi de dahil olmak üzere izlenebilirliği ve reddedilemezliği sağlamaya yönelik kontroller uygulanır. Transfer hizmetinin güvenilirliği ve kullanılabilirliği düzenli olarak izlenebilmektedir.

Hassas, Kişisel veya Gizlilik dereceli bilgilerin aktarım uygun olduğu şekilde, bilgi sahipleri, risk sahipleri, güvenlik görevlileri ve bilgi sorumluları dahil olmak üzere aktarımla ilgili uygun kişilerin tanımlanması sonucuna göre transferler yapılır.

Hassas, Kişisel veya Gizlilik dereceli bilgilerin kurum içinde veya kurum dışına elektronik posta olarak aktarılması söz konusu olduğunda, bilgiler sıkıştırılıp şifrelenmiş olarak e-postanın ekindeki bir dosyada yer alır. Şifre sms ile iletilir.

Hassas, Kişisel veya Gizlilik dereceli elektronik bilgilerin taşınabilir depolama ortamları ile (usb bellek vb.) aktarımı söz konusu ise, işlem tamamlanıp gizli bilgiler uygun şekilde bu taşınabilir ortamdan silinmedikçe, bu taşınabilir depolama cihazları başka bir amaç için kullanılamaz ve başka bilgisayarlara bağlanamaz.

Hassas, Kişisel veya Gizlilik dereceli bilgiler için, etiketlerin anlamının hemen anlaşılmasını ve bilgilerin uygun şekilde korunmasını sağlayan, üzerinde anlaşmaya varılmış bir etiketleme sisteminin kullanılması sağlanmıştır.

Sistemlere yönetim amaçlı yapılan uzaktan erişimler Güvenli Özel Ağ (Virtual Private Network VPN) gibi güvenli metodlar ile yapılır.

**Fiziksel Ortamda Bilgi Aktarımı**

Bilgi varlığı, zarf içine sığabilecek boyutlarda ise (Compact Disk, Kağıt gibi), zarfa konularak yapıştırılmak suretiyle kapatılır. Gönderen kişi, zarf kapağını imzalayarak kuryeye teslim eder.

Gönderen taraf, aktarılan varlığın alıcının eline geçip geçmediğini kontrol eder (örneğin telefon ile teyit alınır).

Hassas, Kişisel veya Gizlilik dereceli bilgilerin fiziksel gönderimi sırasında iki ayrı ambalaj kullanılacak, dış ambalajda özel bir işaretleme yapılmayacak, iç ambalaj ise ambalaj içeriğini belli etmeyecek şekilde koruyucu olacak, gönderinin alıcısı dışında kişilerce açılmasını engelleyecek şekilde işaretlenecektir (örn. gizlilik derecesini belirtir kaşe basılması).

Bilgi varlığı, disk, bilgisayar gibi, zarf içine sığmayacak boyutlarda ise, uygun şekilde paketlenir. Paketler, gönderilen varlığa zarar gelmesini önleyecek nitelikte ve sağlamlıkta olmalıdır. Paketlerin yolda açılmadığından emin olmak için kapak bölümü imzalanır.

Alıcı taraf, aktarım esnasında gönderilen paketin açılmadığından emin olmalıdır.

Aktarımların dolaylı yollarla, elden ele teslimat şeklinde değil, bir seferde gönderenden alıcıya ulaşacak şekilde gerçekleşmesi esastır.

Fiziksel depolama ortamının veya verilerin kaybı gibi bilgi güvenliği olayları durumunda sorumluluklar ve yükümlülükler sözleşmelerde bulunmaktadır.

**Sözlü ve Görsel Olarak Bilgi Aktarımı**

Elektronik ve fiziksel ortamlarda bilginin aktarımı konusunda olduğu gibi, sözlü iletişimde de bilgi güvenliğinin korunması sağlanır. Kurumumuzun özel konular hakkında, kamuya açık alanlarda yüksek sesle konuşulmaz.

Telefon görüşmelerinde, toplantılarda, vb. sözlü iletişimin sağlandığı ortamlarda karşı tarafın (telefonla görüşülen kişi, toplantı katılımcıları gibi) gizlilik dereceli bilgiye erişim yetkisi yoksa veya erişim yetkisinden emin olunamıyorsa, gizlilik dereceli bilgiler paylaşılmaz.

Çalışanlar “sosyal mühendislik” yöntemi konusunda bilgilendirilir ve yetkisiz kişilere bilgi vermez. Kurumun kamu oyundaki imajını oluşturan, reklam, web sitesi, afiş, tanıtım videosu gibi tanıtım materyalleri bir bilgi güvenliği ihlali olup olmadığı (gizlilik dereceli bilgilerin dahil edilmiş olması, teknik altyapıya ilişkin detaylı bilgilerin bulunması vb.) kontrol edilerek kamuoyuna sunulur.

Güvenlik kamerası ile işlenen görüntüler hukuki sebepler doğrultusunda belirtilen evraklara istinaden kolluk kuvvetleri ile paylaşılır.

**YAPTIRIM**

Bu uygulamanın ihlal edilmesi durumunda Bilgi Güvenliği Yönetim Sistemi (BGYS) yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Temsilcisi tarafından e-posta üzerinden yazılı olarak uyarılır. Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller Disiplin Prosesi” gereğince kişiler hakkında işlem yapılır. Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, birim amirinin bilgisi dahilinde BGYS Ekibi’ne en kısa sürede bildirme sorumluluğundadır. Mesajlar da dahil olmak üzere tüm ticari kayıtlar için saklama ve imha yönergeleri belirlenerek, iş kayıtlarının saklanması ve imhasına ilişkin yerel mevzuat ve düzenlemeler mevcutta kullanılabilir yada diğer ilgili yasal, kanuni, düzenleyici ve sözleşmeden doğan gerekliliklerin dikkate alınması sağlanacaktır. (örn. elektronik imza gereklilikleri).

**E-posta Kullanım Kuralları**

**Kurumsal Kullanım**

* Kurumumuz, e-posta kaynakları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
* Kurumumuz, çıkarlarıyla çatışmadığı sürece e-posta kaynaklarının kişisel kullanımına kısıtlı olarak izin verilmektedir.
* Kurumumuz, e-posta kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.
* Kullanıcılar kendi kullanıcı hesaplarıyla gerçekleştirilen tüm e-posta işlemlerinden sorumludur.

**Uygunsuz Kullanım**

* Kurumumuz, e-posta kaynakları hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişemez ve kurumun normal operasyon ve iş aktivitelerini engelleyemez.
* Kurumumuz, e-posta kaynakları uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz.
* Kullanıcıların e-posta sistemini kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır.
* Kurumumuz, e-posta kaynakları; “zincir e-postalar”, reklam, aldatma, karalama gibi istenmeyen mesajlar (SPAM) göndermek için kullanılamaz.
* E-posta sisteminin izinsiz kullanımı ve mesaj içeriğinde veya başlığında sahtecilik yapılması yasaktır.
* Kurumun e-posta sistemi, ücretsiz veya ticari hiçbir yazılımın alınması, gönderilmesi veya saklanması için kullanılamaz.
* Tüm e-posta içerikleri ve eklentileri açılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilmektedir.

**E-posta Yazılımı**

* Kullanıcılar sadece kurumun yetkili birimlerince onaylanmış e-posta yazılımlarını ve konfigürasyonlarını kullanabilirler.
* E-posta yazılımının mevcut güvenlik ayarlarını gevşetecek ayarlamalar yapılamaz.
* Kullanıcılar e-posta yazılımının gönderenin kimliğini gizleyecek özelliklerini kullanamazlar.

**İzleme**

* Kurumumuz, e-posta sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.
* Kurumumuz, kullanıcının e-posta sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.

**5.15 Erişim Kontrolü**

**İnternet Erişimi:**

İnternet Hizmetleri’nin güvenli internet erişimi için sahip olması gereken standartları belirlemektir. İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır.

**Uygulama**

Bütün kullanıcılar ve Sistem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkmamalıdır.

* Kurumumuz, bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkmaktadır.
* Ağ güvenlik duvarı kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
* Ağın dışından ağın içine erişimin denetimi burada yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmektedir.

Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmaktadır. İstenmeyen siteler (kumar, şiddet vs.) yasak olabilmektedir.

* Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme sistemleri kullanılmaktadır.
* Antivirüs gateway sistemleri kullanılmaktadır. İnternete giden veya gelen bütün trafik virüslere karşı taranmaktadır.
* Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.
* Üçüncü şahısların kurum internetini kullanmaları bilgi işlem sorumlularının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.

**Kablosuz Erişim**

**Uygulama**

**Onaylanmış Teknoloji**

Bütün kablosuz erişim cihazları yetkili birim tarafından onaylanmıştır. Belirlenen güvenlik ayarlarını kullanılmaktadır.

**Güvenlik Ayarları**

* Erişim cihazlarındaki yazılımlar düzenli olarak güncellenmektedir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.
* Erişim cihazlarını kolayca erişilebilir bir yerdedir. Çünkü cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.
* Cihaza erişim için güçlü bir şifre kullanılmaktadır. Erişim şifreleri varsayılan ayarda bırakılmamaktadır.
* Varsayılan SSID isimlerini kullanılmamaktadır. SSID bilgisi içerisinde kurumla ilgili bilgi yoktur. Mesela kurum ismi, ilgili bölüm çalışanın ismi vs.
* Erişim cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dahil edilmektedir.
* Kurum dışından, kritik yerlerde kullanıcılar SSL VPN ile kurum ağına erişmektedir.
* Hem kullanıcılar hem de erişim cihazları statik ip adresleri kullanmaktadır. Aynı zamanda donanım adresleme kullanılmaktadır.
* Sistemde hackerler tarafından konulmuş casus bir erişim cihazı olabilir veya mevcut erişim cihazı resetlenmiş olup kurumun güvenlik politikalarına aykırı bir şekilde ayar yapılmış olabilir. Bu sebeple, erişim cihazlarını bir yönetim yazılımı ile devamlı olarak gözlemlenmektedir.

**Uzaktan Erişim**

Kurumumuza, bağlı bütün uzak erişim bağlantılarını kapsamaktadır ve bunun içerisine e-posta okuma veya gönderme ve intranet web kaynaklarını gözlemleme dâhildir. Modemden port yönlendirmesi (RDP) , VPN ile sınırlıdır.

Uzaktan çalışma 4857 sayılı İş Kanununda çalışanların, işveren tarafından oluşturulan iş organizasyonu kapsamında, iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iş ilişkisi olarak tanımlanmıştır. Uzaktan çalışma; yükleniciler, tedarikçiler, iş ortakları çalışanları gibi kurum ile geçici olarak iş ilişkisi olan kişiler tarafından yapılır.

* Kurumumuz firması bünyesinde uzaktan erişim sadece çalışanlara açıktır.
* Çift tünel sistemine izin verilmemektedir, sadece tek ağ bağlantısı ile bağlantı yapılmaktadır.
* Uzak bağlantı yapan bilgisayarlar özel yetkilendirilmiş kişiler tarafından kullanılan uygulamalar ile şifrelenmiş durumdadır.
* Bilgisayar başından kalkarken personelin oturumunu kapatma veya ancak parola ile açılabilen ekran koruyucu vb. önlemleri devreye girmektedir.

Ancak,

Doğal afet, salgın hastalık gibi olağanüstü hallerde yetkili makamlar tarafından uygun görüldüğü durumlarda,

Verilen bir görevin acil olarak yerine getirilmesi veya işletilmekte olan sunucu ve sistemlere 7\*24 esasına göre uzaktan destek verilmesi gereken durumlarda,

İl dışı görevlendirme vb. nedenlerle kurum dışında çalışılması gereken durumlarda kurum personeli tarafından da “uzaktan çalışma” yapabilir.

İnternet üzerinden kurumumuzun herhangi bir yerindeki bilgisayar ağına VPN veya başka bir bağlantı sağlanmaktadır. Problem durumlarında bağlantı sadece izinli bilgisayarlara ve gizlilik sözleşmesi bulunan anlaşmalı kuruma ait IP adreslerine izin verilecek şekilde ve şifreli olarak yapılmaktadır.

kurumumuz çalışanları hiçbir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.

Çalışanlar kurumumuz ile ilgili çalışmalarında kurumumuzun dışındaki e-posta hesaplarını kullanamazlar.

kurumumuz ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler birim in özel izni ile geçici olarak izin verilebilirler.

İşten ayrılan kullanıcı hesapları ilişiği kesildikten hemen sonra kaldırılır.

Kurumumuz, bilgilerine ulaşabilen tüm kurumumuzlar ile Tedarikçi Gizlilik Sözleşmesi imzalanmıştır.

İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmaktadırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlanmaktadır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermektedir.

Uzaktan erişim güvenliği sıkı şekilde denetlenmektedir. Kontrol tek yönlü şifreleme (one-time password authentication, örnek; Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmektedir.

Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmasına dikkat edilir.

Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmakta, yetkiler ve hesap özellikleri buna göre güncellenmektedir.

Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olarak kullanımı sağlanmaktadır.

Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmektedir.

Uzaktan çalışma işlemi, yapısı itibariyle güvensiz olarak kabul edilir ve bilgi güvenliğinin sağlanması için ek önlemler alınır.

Kurumumuz çalışanları, uzaktan çalışma için kurumumuz tarafından verilen bilgisayarları kullanmak zorundadır. Ancak “iş sürekliliğinin sağlanması, işletilmekte olan sunucu ve sistemlere uzaktan destek verilmesi” gibi çok acil hallerde, başka bir imkân olmadığı için şahsi bilgisayarların kullanılması durumunda, kurumsal verilerin söz konusu bilgisayara indirilmemesi ve işlenmemesi için gerekli özen gösterilir. Yapılan müdahalenin doğası gereği bilgisayara indirilen verilerin güvenli olarak silinmesi, işlemi gerçekleştiren kişilerin sorumluluğundadır.

Uzaktan çalışma yapacak kişiler, Kurumumuz ile sözleşme/protokol imzalayan üçüncü taraf personeli ise ve bu kişilere kuruma ait bilgisayar verilemiyorsa; uzaktan çalışma esnasında kullanılacak cihazlarda gerekli güvenlik tedbirlerinin alınması, Personel Gizlilik Sözleşmesi ve Kurumsal Gizlilik Taahhütnamesi uyarınca ilgili kişilerin ve çalışanı oldukları firma/kurumun tüzel kişiliğinin sorumluluğundadır. Bu kapsamda kurumumuza ait gizlilik dereceli bilgilerin söz konusu bilgisayarlarda Parola Yönetim Politikası yöntemleri ile şifreli olarak saklanması, kullanımına ihtiyaç olmayan verilerin güvenli silme araçları ile kalıcı olarak silinmesi gerekmektedir.

Kurum web tabanlı e-posta sistemi, kurumsal portal gibi doğrudan uygulama erişimleri de dâhil olmak üzere uzaktan çalışmanın hiçbir çeşidinde, sahibi bilinmeyen/herkes tarafından erişilebilen internet kafe, otel bilgisayarları, kiosk vb. ortamlar kullanılamaz. Kullanıcıların bu tip terminaller üzerinden kurumumuz sistemlerine bağlantı yaptıklarının tespit edilmesi halinde Disiplin Prosedüründe belirtilen yaptırımlar uygulanır.

*Uzak çalışma için kullanılacak cihaz ve ortamlarda asgari olarak aşağıda belirtilen güvenlik tedbirlerinin alınmıştır.*

Cihazlara kişisel güvenlik duvarı kurulur ve aktif hale getirilir.

İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanır.

Virüs, fidye yazılımları, truva atları ve benzeri zararlı yazılımlardan korunmak için uygun bir koruma yazılımı tedarik edilir. Yazılımın kendisi ve imza dosyaları güncel halde tutulur.

Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.

Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.

Cihazlar fiziki güvenliği olmayan ortamlarda kullanılacak ise “dizüstü bilgisayar kilidi ve güvenlik kablosu” kullanılmak suretiyle çalınmaya karşı cihaz emniyete alınır.

Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (Wi-Fi, Bluetooth vb.) pasif hale getirilir.

Disk şifreleme vb. araçlarla bilgisayarlarda tutulan verilerin şifreli olarak saklanması sağlanır. Disk şifreleme işlemleri için şifreleme metotlarından yararlanılmaktadır.

Uzaktan çalışma için kullanılan bilgisayarların yerel disklerinde yer alan kurumsal verilerin yedeklenmesi için gerekli tedbirler alınır. Alınacak bu yedekler sadece şifreli ortamlarda ve/veya şifreli yedeklenmiş olarak tutulabilir.

Uzaktan çalışma ve uzaktan erişim için kullanılacak cihazlara çok faktörlü kimlik doğrulama yapılarak giriş yapılması tercih edilir.

Hassas işlemlerde kullanılan üçüncü taraf bilgisayarlarındaki kurumsal verilerin kalıcı olarak silinmesi için gerekli teknik ve idari tedbirler alınır.

Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.

Kullanılan uygulamaların varsa güvenlik ayarları yapılarak daha güvenli kullanım ortamı sağlanır.

Mobil cihaz işletim sistemi tarafından dayatılan kısıtlamalardan kurtulmak için “jailbreak” veya “rootlama” işlemi yapılmaz. Bu işlemlerin yapıldığı cihazlar, uzaktan çalışma için kullanılmaz.

Tüm mobil cihazlara (telefon/tablet) mutlaka lisanslı antivirüs yazılımı kurularak hizmet verilir.

Kullanılan her türlü mobil cihaz için üreticinin sağladığı işletim sistemi güncelleştirmeleri ve yazılım güncelleştirmeleri mutlaka periyodik olarak kontrol edilir ve uygulanır.

**Uzaktan Erişim**

Uzaktan çalışma yapacak kullanıcıların kurum tarafından işletilen ve özel koruma gerektiren bilişim kaynaklarına (sunucu ve ağ cihazlarının yönetim panelleri, VTYS yönetim ara yüzleri, kritik uygulamalar vb.) erişimi, VPN (sanal özel ağ) bağlantısı üzerinden gerçekleştirilir.

Kişilere VPN erişimi verilebilmesi için;

Firma personeli için ilgili kişilerin,

Erişim verilecek kişiler bir firma dışında bir başka kurumun çalışanı

İlgili firma/kuruma ait Bağlantı ihtiyacına ilişkin detaylı açıklamaların (ihtiyacın gerekçesi, erişilmek istenen bilişim kaynakları) resmi yazı ile kurum (Sistem Yönetimi ve Bilgi Güvenliği Ekibine) gönderilmiş olması gerekir.

VPN erişim talepleri, kurum ilgili birimleri tarafından detaylı olarak incelenir. Gerekiyorsa erişilecek bilişim kaynağının sahiplerinden doğrulama yapılır. İhtiyaç olması halinde ilave bilgi ve belge istenebilir.

VPN erişimi yapan kullanıcıların erişim yaptıkları kaynaklar üzerinde yaptıkları işlemler, “Yetkili Kullanıcı Hesap Yönetim Sistemi” tarafından video ve/veya metin (text) formatında kayıt altına alınır.

VPN erişimleri altı aylık süre sonunda otomatik olarak askıya alınacak şekilde verilir. Altı aylık sürenin sonunda ilgili kişinin kurumui ile ilişkisinin devam edip etmediği e-posta veya resmi yazı ile teyit edilir. Kişinin çalışmaya devam ettiğinin teyit edilmesi halinde, sözleşmesinde belirtilen süre dikkate alınarak erişim izni uzatılır.

Personel Gizlilik Sözleşmesinde yazan “Sözleşme Geçerlilik Tarihi”nin dolması durumunda, altı aylık sürenin dolmasını beklemeksizin erişimi askıya alınır. Kişiye yeniden erişim izni verilebilmesi için sözleşmenin yenilenmesi gerekir.

**Ağ Erişim Denetimi**

Ağ üzerinde aktif dizin kullanıcıları için ortak sürücüsü oluşturulmuştur.

* “D” sürücüsü üzerindeki birimler ve kullanıcılara göre yetkilendirilmiştir.
* personelin dosya silme yetkisi bağlı olduğu birim yöneticisi tarafından verilen izinle Bilgi Teknolojileri tarafından verilmektedir
* “D” sürücüsü üzerinde iso, iso formları, vb. ortak kullanıma açık dizinler oluşturulmuştur. Bu dizinlere erişim açıktır.
* Paylaşımlar sistem yöneticisi tarafından belirlenmektedir.
* Yazılım dizinine sadece yazılım grubuna ait üye kullanıcıların dosya oluşturma, ekleme, değiştirme yetkisi bulunmaktadır.
* İso formları dizinine tüm kullanıcılar erişebilmekte ancak sadece okuma yetkisine sahiptirler. Bilgi Güvenliği Yöneticisi dışında kullanıcıların dosya ve/veya form oluşturma, ekleme, değiştirme yetkisi bulunmamaktadır. Bu şekildeki istekleri var ise kalite birimine haber verilir.
* İso dizinine sadece Bilgi Güvenliği Yöneticisi kullanıcılarının dosya oluşturma, ekleme, değiştirme yetkisi bulunmaktadır. Silme yetkileri yoktur.
* Ağ bağlantıları için kullanıcı paroları “Kullanıcı Kimlik Yönetim Prosedürü”ne göre verilmektedir.

**İşletim Sistemi Erişim Kontrolü**

* İşletim Sistemine sadece aktif dizin kullanıcıları erişebilir. Bu kullanıcılar dışındaki kişilerin erişimi engellenmiştir.
* Bu kullanıcıların erişim yetkisi “Erişim Matrisi” tanımlanmıştır.
* Tüm kullanıcılar kendi kişisel kullanımları için benzersiz bir kimliğe sahiptirler.
* İşletim sistemlerine erişim için güvenli bir oturum açma işlemini bilgisayar kullanım talimatına göre yapmaktadır.
* Sistemin üzerine yazabilme yeteneği olabilecek yardımcı sistem programlarının kullanımı yasaklanmıştır.
* Kullanıcıların bağlantı süresinde bir kısıtlama yapılmamıştır.
* Her kullanıcı istediği bilgisayarda parolası ile sisteme bağlanabilir.
* Kurumumuz, müşterilerine erişimi ayrı bir ağ (network te) tutulan web sunucusu ile sağlanmaktadır.
* Dışarıdan bağlanan kişiler sadece bu web sunucusu (ftp://deneme.)ile bağlanabilir. Güvenliksiz bağlantı yasaklanmıştır.

**Ayrıcalıklı Destek programlarının kullanımı**

* Sistem ve uygulamanın kontrollerini geçersiz kılma kabiliyetine sahip destek programların kullanımı yasaktır.
* Şirket bünyesindeki bilgisayarlarda kurulu olan programlar periyodik olarak “Bilgi Teknolojileri İş Süreçleri Prosesine ne göre kontrol edilir.

**Program Kaynak Koduna Erişim**

* Kurumumuz, bünyesinde çalışan Yazılım Departmanı personeli hariç hiçbir personel kaynak koduna erişemez.

**5.16 Kimlik Yönetimi**

Kimlik yönetimi bağlamında kullanılan süreçler şunları sağlamaktadır.

a) kişilere atanan kimlikler için, belirli bir kimlik, yalnızca bu belirli kimlikle gerçekleştirilen işlemlerden sorumlu tutulabilmesi için tek bir kişiyle ilişkilendirilir,

b) birden çok kişiye atanan kimliklere (ör. paylaşılan kimlikler) yalnızca ticari veya operasyonel nedenlerle gerekli olduklarında ve özel onay ve belgelere tabi olduklarında izin verilir,

c) insan olmayan varlıklara atanan kimlikler, uygun şekilde ayrılmış onaya ve bağımsız sürekli gözetime tabidir,

ç) kimlikler artık gerekli değilse zamanında devre dışı bırakılır veya kaldırılır (örneğin, ilişkili varlıkların silinmesi veya artık kullanılmaması veya bir kimliğe bağlı kişinin kuruluştan ayrılması veya rolünü değiştirmesi),

d) belirli bir alanda, tek bir kimlik tek bir varlığa eşlenir, [yani birden fazla kimliğin aynı bağlam içinde aynı varlığa eşlenmesinden (yinelenen kimlikler) kaçınılır],

e) kullanıcı kimliklerinin ve kimlik doğrulama bilgilerinin kullanımı ve yönetimi ile ilgili tüm önemli olayların kayıtları tutulur.

**5.17 Kimlik Doğrulama Parola Güvenliği**

Kurumumuz, kullanıcıları bu kurallara uymakla yükümlüdürler.

Kurumumuz, içinde ve şirket kaynaklarına erişmek için kullanılacak tüm programlarda aşağıdaki standartlara uyulmalıdır.

* + Parola en az 8 karakterden oluşmalıdır.
	+ Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, \*, %" gibi özel karakterler içermelidir.
	+ Büyük ve küçük harfler bir arada kullanılmalıdır.
	+ Son kullanılan 24 şifrenin seçilmesi engellenmiştir.
	+ 30 günde bir şifreler değiştirilmelidir.
* Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.
	+ Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız, araç plakaları, telefon numaraları gibi)
	+ Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
	+ İsim, şehir, takma ad, argo tabirler, yabancı dillerdeki kelimeler vb kelimeleri yalnız başına parola olarak kullanılmamalıdır.
	+ Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.
	+ Tersten yazılan kelimeler, sık rastlanan yazım hataları ve kısaltmalar kullanmamalıdır.
* Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.

|  |  |  |
| --- | --- | --- |
| 'B' yerine 8 | 'Z' yerine 2 | Örneğin;Balıkçıl-Kazak8a11kç11-Ka2akSolaryum!501aryum! |
| 'I', 'i', 'L', 'l' yerine 1 | 'O' harfi yerine 0 |
| 'S' yerine 5'G' yerine 6 | 'g' yerine 9 |

* Basit bir cümle ya da ifade içerisindeki belirli kelimeler özel karakter veya rakamlarla değiştirilerek güçlü bir parola elde edilebilir.

|  |  |  |
| --- | --- | --- |
| 'T', 't' yerine '+' | 'Ş', 'ş' yerine '$' | "Dün Kar Yağmış" :Dün\*Yağm1$"Şeker gibi bir soru sordu" :$eker~1?Sordu"Tek eksiğim bir güldü" :1-ğim1:)dü"Yüzeysel bir soru eşittir eksi puan":%eysel1?=-Puan |
| "kar", "yıldız" yerine '\*' | "dolar" "para" yerine'$' |
| "Soru" yerine '?' | "gibi" yerine '~' |
| "gül" yerine ':)' | "eksi" yerine '-' |
| "bir", "tek" yerine 1 | "yüz", "yüzde" yerine'%' |

* Parolanızı bir parola denetleyici ile test edin . Parola denetleyici, parolanızın gücünü otomatik olarak değerlendirir. https://apps.microsoft.com/detail/9mtw05360pmw?cid=msft\_web\_chart&hl=tr-tr&gl=TR
* Kullanıcılar şifrelerinin çalındığından kuşkulandıklarında yetkili birime haber vermeli; gereken önlemlerin alınmasını sağlamalıdır.
* Her şey için aynı parolayı kullanmayın. Siber dünyanın suçluları, çok az güvenliği olan web sitelerindeki parolaları çalarlar ve ardından aynı parola ve kullanıcı adını, bankacılık web siteleri gibi daha güvenli ortamlarda kullanmaya çalışırlar.
* Tek Kayıt İle Her Şeye Erişim (single Sign On); Kullanıcı, tek bir şifre ile ağ üzerinde kendisine izin verilen uygulamalara erişebilmektedir.
* Kurumumuz çalışanı olmayan kişiler için açılan kullanıcı hesapları da güçlü parolalar ile korunmalıdır.
* Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki “parola hatırlatma” seçeneği kullanılmamalıdır.
* Başarısız parola denemeleri üst üste 3 kere ile sınırlandırılmıştır. Üçüncü denemeden sonra şifre ve bağlı olduğu kullanıcı, kullanım dışı bırakılır.
* Kullanıcı parolaları, saklandıkları ortamlarda, geri dönüşü mümkün olmayan bir şekilde bozularak korunur (örneğin Hash), bu sayede en yetkili kişilerin bile kullanıcı parolasını görmesi engellenir.
* Bilgi kaynaklarına başarılı ve başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerinin kaydı tutulur.
* Parolaların klavyeden girilmesi sırasında dikkatli olunmalı ve çevredeki kişilerin görmesine izin vermeyecek şekilde girilmelidir.
* Yeni parola ve parola değişim talepleri sistemden “yeni talep” açılarak ve departman yöneticisinin onayı ile yapılır.
* Yeni alınan donanım veya yeni kurulan yazılıma ait varsayılan bir parola var ise, şirket standardına uygun yeni bir parola ile değiştirilmelidir.
* İşten çıkış sürecinde, çalışana iç ve dış müşteriler tarafından verilmiş olan parolalar çalışanın bağlı olduğu yöneticiye teslim edilmelidir.

**5.18 Gözden Geçirme**

Erişim hakları düzenli olarak bilgi güvenliği yöneticisi tarafından yılda en az bir kez ve süreci etkileyen büyük bir değişiklik olduğunda gözden geçirilmektedir.

**5.19 Tedarikçi İlişkilerinde Bilgi Güvenliği**

Tedarikçinin ürün veya hizmetlerinin kullanımıyla ilgili bilgi güvenliği risklerini yönetmek için süreçler ve prosedürler tanımlanmakta ve uygulanmaktadır.

a) Kurumumuz bilgilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini etkileyebilecek tedarikçi türlerinin (örneğin, Bilgi İletişim Teknolojileri (BİT) hizmetleri, lojistik, kamu hizmetleri, finansal hizmetler, BİT altyapı bileşenleri) belirlenmesi ve belgelenmesi,

b) Bilgi, ürün ve hizmetlerin hassasiyetine göre tedarikçilerin nasıl değerlendirileceğinin ve seçileceğinin belirlenmesi (örneğin pazar analizi, müşteri referansları, belgelerin gözden geçirilmesi, yerinde değerlendirmeler, sertifikalar),

c) Yeterli bilgi güvenliği kontrollerine sahip tedarikçi ürün veya hizmetlerinin değerlendirilmesi ve seçilmesi ve bunların gözden geçirilmesi; özellikle, tedarikçinin bilgi ve bilgi işleme bütünlüğünü ve dolayısıyla kurumumuzun bilgi güvenliğini sağlayan tedarikçi tarafından uygulanan kontrollerin doğruluğu ve eksiksizliği,

d) tedarikçilerin erişebileceği, izleyebileceği, kontrol edebileceği veya kullanabileceği kurumumuz bilgilerinin, BİT hizmetlerinin ve fiziksel altyapının tanımlanması,

e) kurumumuzun bilgilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini etkileyebilecek tedarikçiler tarafından sağlanan BİT altyapısı bileşenlerinin ve hizmetlerinin türlerinin tanımlanması,

f) Bilgi güvenliği risklerinin değerlendirilmesi ve yönetilmesi, potansiyel kötü niyetli tedarikçi personelinden kaynaklanan riskler dahil olmak üzere tedarikçilerin kurumumuzun bilgilerini ve diğer ilgili varlıkları kullanması, tedarikçiler tarafından sağlanan ürünlerin (bu ürünlerde kullanılan yazılım bileşenleri ve alt bileşenler dahil) veya hizmetlerin arızalanması veya güvenlik açıkları,

g) Üçüncü taraf incelemesi ve ürün doğrulaması da dahil olmak üzere, her bir tedarikçi türü ve erişim türü için belirlenmiş bilgi güvenliği gerekliliklerine uygunluğun izlenmesi,

h) İster izleme yoluyla ister başka yollarla tespit edilmiş olsun, bir tedarikçinin uygunsuzluğunu hafifletmek,

i) hem organizasyonun hem de tedarikçilerin sorumlulukları dahil olmak üzere tedarikçi ürünleri ve hizmetleriyle ilgili olayları ve olasılıkları ele almak,

j) Dayanıklılık ve gerekirse, tedarikçinin bilgilerinin ve bilgi işlemenin mevcudiyetini ve dolayısıyla kurumumuzun bilgilerinin mevcudiyetini sağlamak için kurtarma ve beklenmedik durum önlemleri,

k) Tedarikçinin türüne ve tedarikçinin kurumumuzun sistemlerine ve bilgilerine erişim düzeyine bağlı olarak uygun katılım kuralları, konuya özel politikalar, süreçler ve prosesler ve davranış hakkında tedarikçi personeli ile etkileşim halinde olan kurumumuz personeli için farkındalık ve eğitim,

l) Gerekli bilgi transferini, diğer ilişkili varlıkları ve değiştirilmesi gereken diğer her şeyi yönetmek ve transfer süresi boyunca bilgi güvenliğinin sürdürülmesini sağlamak,

m) Aşağıdakiler dahil olmak üzere tedarikçi ilişkisinin güvenli bir şekilde sonlandırılmasını sağlamak için gereksinimler:

 1) erişim haklarının sağlanmasının kaldırılması;

 2) bilgi işleme;

 3) sözleşme sırasında geliştirilen fikri mülkiyetin mülkiyetinin belirlenmesi;

 4) tedarikçi değişikliği veya kaynak kullanımı durumunda bilgi taşınabilirliği;

 6) kayıt yönetimi;

 7) varlıkların iadesi;

 8) bilgilerin ve diğer ilgili varlıkların güvenli bir şekilde imha edilmesi;

 9) devam eden gizlilik gereklilikleri;

n) tedarikçinin personelinden ve tesislerinden beklenen personel güvenliği ve fiziksel güvenlik düzeyi.

**5.20 Tedarikçi Anlaşmalarında Bilgi Güvenliğinin Ele Alınması**

İlgili bilgi güvenliği gereklilikleri, tedarikçi ilişkisinin türüne göre her tedarikçi ile oluşturulmakta ve üzerinde anlaşmaya varılmaktadır.

Belirlenen bilgi güvenliği gereksinimlerinin karşılanması için aşağıdaki şartların sözleşmelere dahil edilmesine özen gösterilmektedir.

a) sağlanacak veya erişilecek bilgilerin tanımı ve bilgileri sağlama veya bilgilere erişme yöntemleri,

b) kurumumuzun sınıflandırma şemasına göre bilgilerin sınıflandırılması,

c) kurumumuzun kendi sınıflandırma şeması ile tedarikçinin sınıflandırma şeması arasında eşleme,

d) veri koruma, kişisel olarak tanımlanabilir bilgilerin (PII) işlenmesi, fikri mülkiyet hakları ve telif hakkı dahil olmak üzere yasal, kanuni, düzenleyici ve sözleşmeden doğan gereklilikler ve bunların karşılanmasının nasıl sağlanacağının açıklaması;

e) her bir sözleşme tarafının, erişim kontrolü, performans incelemesi, izleme, raporlama ve denetim dahil olmak üzere üzerinde mutabık kalınan bir dizi kontrol uygulama yükümlülüğü ve tedarikçinin kurumumuzun bilgi güvenliği gereksinimlerine uyma yükümlülükleri,

f) gerektiğinde kabul edilemez kullanım da dahil olmak üzere, bilgilerin ve diğer ilgili varlıkların kabul edilebilir kullanım kuralları,

g) tedarikçi personeli tarafından kurumumuz bilgilerinin ve diğer ilgili varlıkların kullanımına ilişkin yetkilendirme ve yetkinin kaldırılmasına ilişkin prosedürler veya koşullar (örneğin, kurumumuzun bilgilerini ve diğer ilgili varlıkları kullanma yetkisine sahip tedarikçi personelinin açık bir listesi yoluyla),

h) tedarikçinin BİT altyapısına ilişkin bilgi güvenliği gereklilikleri; özellikle, kurumumuzun iş ihtiyaçlarına ve risk kriterlerine dayalı bireysel tedarikçi anlaşmalarına temel teşkil edecek her tür bilgi ve erişim türü için asgari bilgi güvenliği gereklilikleri;

i) Yüklenicinin gereksinimleri karşılamaması durumunda tazminatlar ve düzeltmeler,

j) olay yönetimi gereklilikleri ve prosedürleri (özellikle olay iyileştirme sırasında bildirim ve işbirliği),

k) bilgi güvenliği gereklilikleri için eğitim ve farkındalık gereklilikleri (örn. olay müdahalesi, yetkilendirme prosesleri),

l) alt tedarikçilerin kullanımına ilişkin anlaşma gibi uygulanması gereken kontroller de dahil olmak üzere taşeronluk için ilgili hükümler (örneğin, bunların tedarikçinin aynı yükümlülükleri altında bulunmasının gerekliliği, alt tedarikçilerin bir listesine sahip olmanın gerekliliği ve herhangi bir değişiklikten önce bildirim),

m) bilgi güvenliği sorunları için bir irtibat kişisi dahil olmak üzere ilgili irtibat kişileri,

n) tarama tamamlanmadıysa veya sonuçlar şüphe veya endişeye neden oluyorsa, tarama ve bildirim proseslerini yürütme sorumlulukları da dahil olmak üzere, tedarikçinin personeli için yasal olarak izin verildiği durumlarda tarama gereklilikleri;

o) tedarikçi süreçleriyle ilgili bilgi güvenliği gereklilikleri için üçüncü taraf tasdiklerinin kanıt ve güvence mekanizmaları ve kontrollerin etkinliğine ilişkin bağımsız bir rapor,

p) anlaşma ile ilgili tedarikçi süreçlerini ve kontrollerini denetleme hakkı,

q) tedarikçinin, kontrollerin etkinliği hakkında periyodik olarak bir rapor sunma yükümlülüğü ve raporda ortaya çıkan ilgili konuların zamanında düzeltilmesi konusunda mutabakat,

r) kusur çözme ve çatışma çözme süreçleri,

s) (sıklık, tür ve depolama konumu açısından) kurumumuzun ihtiyaçlarına uygun yedekleme sağlamak,

t) birincil tesis ile aynı tehditlere maruz kalmayan alternatif bir tesisin (yani felaket kurtarma sahası) mevcudiyetinin ve birincil kontrollerin başarısız olması durumunda geri dönüş kontrollerinin (alternatif kontroller) dikkate alınmasının sağlanması,

u) kurumumuza önceden bildirimde bulunulmasını ve kurumumuzun değişiklikleri kabul etmeme olasılığını sağlayan bir değişiklik yönetimi sürecine sahip olmak,

v) bilgi sınıflandırmasıyla orantılı fiziksel güvenlik kontrolleri,

w) fiziksel aktarım veya mantıksal aktarım sırasında bilgileri korumak için bilgi aktarım kontrolleri

x) kayıt yönetimi, varlıkların iadesi, bilgilerin ve diğer ilgili varlıkların güvenli bir şekilde elden çıkarılması ve devam eden herhangi bir gizlilik yükümlülüğü dahil olmak üzere sözleşmenin akdedilmesi üzerine fesih hükümleri,

y) tedarikçi tarafından saklanan organizasyon bilgilerinin artık gerekli olmadığı anda güvenli bir şekilde imha edilmesi için bir yöntemin sağlanması,

z) sözleşme sonunda desteğin başka bir tedarikçiye veya kurumumuzun kendisine devredilmesini sağlamak.

**5.21 Bilgi İletişim Teknolojisi (BİT) Tedarik Zincirinde Bilgi Güvenliğini Yönetme**

BİT ürünleri ve hizmetleri tedarik zinciri ile ilişkili bilgi güvenliği risklerini yönetmek için süreçler tanımlanmakta ve uygulanmaktadır.

Tedarikçi ilişkileri için genel bilgi güvenliği gerekliliklerine ek olarak, BİT tedarik zinciri güvenliği içindeki bilgi güvenliğini ele almak için aşağıdaki konular dikkate alınmaktadır.

a) BİT ürün veya hizmet alımına uygulanacak bilgi güvenliği gereksinimlerinin tanımlanması,

b) BİT hizmet tedarikçilerinin, kurumumuza sağlanan BİT hizmetinin bazı bölümleri için taşeronluk yapmaları durumunda, kurumumuzun güvenlik gereksinimlerini tedarik zinciri boyunca yaymalarının şart koşulması,

c) bu ürünler diğer tedarikçilerden veya diğer kurumumuzlardan satın alınan veya edinilen bileşenleri içeriyorsa (örneğin, alt sözleşmeli yazılım geliştiriciler ve donanım bileşeni sağlayıcıları) BİT ürünleri tedarikçilerinin tedarik zinciri boyunca uygun güvenlik uygulamalarını yaymasını zorunlu kılmak,

d) BİT ürünleri tedarikçilerinden, ürünlerde kullanılan yazılım bileşenlerini açıklayan bilgileri sağlamalarını talep etmek,

e) BİT ürünleri tedarikçilerinden, ürünlerinin uygulanan güvenlik işlevlerini ve güvenli çalışması için gerekli yapılandırmayı açıklayan bilgileri sağlamalarını talep ederek,

f) teslim edilen BİT ürün ve hizmetlerinin belirtilen güvenlik gereksinimlerine uygun olduğunu doğrulamak için bir izleme süreci ve kabul edilebilir yöntemler uygulamak. Bu tür tedarikçi inceleme yöntemlerine örnek olarak, sızma testi ve tedarikçinin bilgi güvenliği operasyonları için üçüncü taraf tasdiklerinin kanıtlanması veya doğrulanması,

g) işlevselliği sürdürmek için kritik olan ve bu nedenle özellikle tedarikçi ürün veya hizmet bileşenlerinin bazı yönlerini diğer tedarikçilere yaptırıyorsa, kurumumuz dışında oluşturulduğunda daha fazla dikkat, inceleme ve daha fazla takip gerektiren ürün veya hizmet bileşenlerini belirlemek ve belgelemek için bir süreç uygulamak,

h) kritik bileşenlerin ve bunların kaynağının tedarik zinciri boyunca izlenebileceğine dair güvence elde etmek,

i) teslim edilen BİT ürünlerinin beklenmedik veya istenmeyen herhangi bir özellik olmaksızın beklendiği gibi çalıştığına dair güvence elde etmek,

j) tedarikçilerin bileşenlerinin orijinal olduğundan ve spesifikasyonlarından değiştirilmemiş olduğundan emin olmak için süreçlerin uygulanması. Örnek önlemler arasında (kurcalamaya karşı koruma etiketleri, kriptografik hash doğrulamaları veya dijital imzalar) yer alır. Spesifikasyon dışı performansın izlenmesi, kurcalama veya sahteciliğin bir göstergesi olabilir. Kurcalamanın önlenmesi ve tespiti, tasarım, geliştirme, entegrasyon, operasyonlar ve bakım dahil olmak üzere sistem geliştirme yaşam döngüsünün birçok aşamasında uygulanmaktadır,

k) ICT (Information and Communication Technology) ürünlerinin, örneğin resmi sertifikalandırma veya Ortak Kriter Tanıma Düzenlemesi gibi bir değerlendirme programı yoluyla gerekli güvenlik seviyelerine ulaştığına dair güvence elde etmek,

l) organizasyon ve tedarikçiler arasında tedarik zinciri ve olası sorunlar ve uzlaşmalar ile ilgili bilgi paylaşımı için kuralların tanımlanması,

m) BİT bileşenlerinin yaşam döngüsünü ve kullanılabilirliğini ve ilgili güvenlik risklerini yönetmek için özel süreçlerin uygulanması. Bu, tedarikçilerin artık faaliyet göstermemesi veya tedarikçilerin teknolojik gelişmeler nedeniyle artık bu bileşenleri sağlamaması nedeniyle artık mevcut olmayan bileşenlerin risklerinin yönetilmesini içerir. Alternatif bir tedarikçinin belirlenmesi ve alternatif tedarikçiye yazılım ve yetkinliği aktarma süreci dikkate alınmaktadır.

**5.22 Tedarikçi Hizmetlerinin İzlenmesi, Gözden Geçirilmesi ve Değişiklik Yönetimi**

Kurumumuz, tedarikçi bilgi güvenliği uygulamaları ve hizmet sunumundaki değişiklikleri düzenli olarak izlemekte, gözden geçirmekte, değerlendirmekte ve yönetmektedir.

Kurumumuz ile tedarikçi arasındaki ilişkiyi yönetmek için aşağıdakileri içeren bir süreci içermektedir.

a) anlaşmalara uygunluğu doğrulamak için hizmet performans düzeylerini izlemek,

b) Aşağıdakiler dahil tedarikçiler tarafından yapılan değişiklikleri izlemektedir,

1) sunulan mevcut hizmetlerde iyileştirmeler,

2) herhangi bir yeni uygulama ve sistemin geliştirilmesi,

3) tedarikçi sözleşmelerinde yapılan değişiklikler veya güncellemeler,

4) bilgi güvenliği olaylarını çözmek ve bilgi güvenliğini iyileştirmek için yeni veya değiştirilmiş kontroller,

c) Aşağıdakiler dahil olmak üzere tedarikçi hizmetlerindeki değişiklikleri izlemektedir,

1) ağlarda değişiklikler ve geliştirmeler,

2) yeni teknolojilerin kullanımı,

3) yeni ürünlerin veya daha yeni sürümlerin veya sürümlerin benimsenmesi,

4) yeni geliştirme araçları ve ortamları,

5) hizmet tesislerinin fiziksel konumlarındaki değişiklikler,

6) alt tedarikçilerin değiştirilmesi,

7) başka bir tedarikçiye taşeronluk yapmak,

d) tedarikçi tarafından hazırlanan hizmet raporlarını gözden geçirmek ve sözleşmelerin gerektirdiği şekilde düzenli ilerleme toplantıları düzenlemek,

e) varsa bağımsız denetçi raporlarının incelenmesi ve tespit edilen sorunların takibi ile bağlantılı olarak tedarikçilerin ve alt tedarikçilerin denetimlerini gerçekleştirmek,

f) bilgi güvenliği olayları hakkında bilgi sağlamak ve bu bilgileri anlaşmaların ve destekleyici yönergeler ve proseslerin gerektirdiği şekilde gözden geçirmek,

g) sağlanan hizmetle ilgili bilgi güvenliği olaylarının, operasyonel sorunların, arızaların, hataların ve kesintilerin izlenmesine ilişkin tedarikçi denetim izlerini ve kayıtlarını gözden geçirmek,

h) tanımlanmış herhangi bir bilgi güvenliği olayına veya olayına yanıt vermek ve bunları yönetmek,

i) bilgi güvenliği açıklarını belirlemek ve yönetmek,

j) tedarikçinin kendi tedarikçileriyle olan ilişkilerinin bilgi güvenliği yönlerini gözden geçirmek,

k) tedarikçinin, büyük hizmet başarısızlıkları veya felaketin ardından üzerinde anlaşmaya varılan hizmet süreklilik düzeylerinin sürdürülmesini sağlamak için tasarlanmış uygulanabilir planlarla birlikte yeterli hizmet kapasitesini sürdürmesini sağlayacaktır,

l) tedarikçilerin, uyumluluğu gözden geçirmek ve anlaşmaların gerekliliklerini uygulamak için sorumluluklar vermesini sağlamak,

m) tedarikçilerin yeterli bilgi güvenliği seviyelerine sahip olduklarını düzenli olarak değerlendirilmektedir.

**5.23 Bulut Hizmetlerinin Kullanımı için Bilgi Güvenliği**

Bulut hizmetlerinin edinimi, kullanımı, yönetimi ve bulut hizmetlerinden çıkış süreçleri kurumun bilgi güvenliği gereksinimlerine uygun olarak oluşturulmaktadır.

a) bulut hizmetlerinin kullanımıyla ilişkili tüm ilgili bilgi güvenliği gereksinimleri,

b) bulut hizmeti seçim kriterleri ve bulut hizmeti kullanımının kapsamı,

c) bulut hizmetlerinin kullanımı ve yönetimi ile ilgili roller ve sorumluluklar,

d) hangi bilgi güvenliği kontrollerinin bulut hizmeti sağlayıcısı tarafından yönetildiği ve hangilerinin bulut hizmeti müşterisi olarak kurumumuz tarafından yönetildiği,

e) bulut hizmeti sağlayıcısı tarafından sağlanan bilgi güvenliği yeteneklerinin nasıl elde edileceği ve kullanılacağı,

f) bulut hizmeti sağlayıcıları tarafından uygulanan bilgi güvenliği denetimlerine ilişkin güvencenin nasıl elde edileceği,

g) bir kurumumuz özellikle farklı bulut hizmeti sağlayıcılarından olmak üzere birden çok bulut hizmeti kullandığında hizmetlerdeki denetimlerin, arayüzlerin ve değişikliklerin nasıl yönetileceği,

h) bulut hizmetlerinin kullanımıyla ilgili olarak meydana gelen bilgi güvenliği olaylarının ele alınmasına yönelik prosedürler,

i) bilgi güvenliği risklerini yönetmek için bulut hizmetlerinin devam eden kullanımını izleme, inceleme ve değerlendirme yaklaşımı,

h) bulut hizmetleri için çıkış stratejileri de dahil olmak üzere bulut hizmetlerinin kullanımının nasıl değiştirileceği veya durdurulacağı.

**Bulut Servisleri Riskleri**

**Kurumsal Stratejik Riskler**

* Yönetim ve kontrol kaybı
* Bulut hizmeti sonlandırması veya arızası
* Servis sağlayıcı bağımlılığı
* Üçüncü parti tedarikçi hatası
* Bulut sağlayıcı kurumumuzun satın alınması
* Uyum sorunları
* Sağlayıcının diğer müşterileri nedeniyle itibar kaybı

**Teknik ve Güvenlik Riskleri**

* Dış Kaynaklı Saldırılar Verilerin güvensiz veya etkisiz silinmesi Nakil halindeki veriyi yakalama
* Bulut sağlayıcı tarafında kötü amaçlı giriş
* Kaynak tükenmesi
* Şifreleme
* Kaynak izolasyonu eksikliği
* Hizmet kesintisi veya bozulması
* Kötü amaçlı araştırma ve taramalara girilmesi
* Müşteri gereksinimleri ve bulut ortamı arasındaki anlaşmazlık
* Şifreleme anahtarlarının kaybı
* Hizmet motorunun hacklenmesi (Ağlara veya cihazlara yetkisiz erişim elde etme)

**Hukuksal Riskler**

Yargı değişiminden kaynaklı riskler, mahkeme celbi ve e-keşif, veri sansürü, lisans riskleri, veri koruma riskleri, genellikle tersine geçiş olarak adlandırılan buluttan çıkış stratejisi, (bir işletmenin bir bulut sağlayıcısından diğerine daha büyük bir kesinti olmadan etkili bir şekilde geçiş yapabilmesini sağlamak için bir plan) geliştirme sürecidir. Bu, buluta geçmek isteyen kurumumuz için odak noktası olmaktadır. Bulut hizmet sağlayıcısı olağanüstü çalışma süresi ve güvenilirliğe sahip hizmetler sunsada, pazar liderlerinde bile son zamanlarda önemli kesintiler olmaktadır. Aynı şekilde, işletmelerin karşılaştığı ve iş performanslarına zarar verebilecek bulut endişeleri, bütçe/maliyet kontrolleri ve yönetişim vb. gibi önceki kararları yeniden düşünmek için birçok başka neden olabilir, Bu nedenle kurumumuz bulut hizmetlerinden çıkışa stratejisine sahip olarak konuya önem vermektedir. Kurumumuz için buluttan çıkışı planlamak için etkili bir çıkış stratejisi, yeri doldurulamaz verileri güvende tutmak ve başarılı bir geçiş sağlamak için önemli bir parçadır.

Kurumumuz bulut hizmetlerinden çıkışa hazırlanırken aşağıdaki anketle testleri yaparak gerekli çıkış yöntemine ön hazırlık yapmış olur:

1. Mevcut CSP (Bulut Tabanlı Hizmet Sağlayıcısı) ile iş yüklerini çalıştırmanın zorlukları nelerdir?
2. Mevcut maliyetlendirme nasıl görünüyor?
3. Her zaman yukarı yönlü bir fiyatlandırma modeli mi?
4. Satıcı kilitlenmesi işletmenin ilerlemesini engelliyor mu?
5. Diğerlerine göre rekabet avantajı sunuyor mu?
6. Hedeflediğim duruma ulaşmak için mevcut CSP ile bir sonraki önemli şey nedir?
7. Dijital çözümler açısından ne kadar yenilikçi?
8. Mevcut CSP ile düzenleyicilerin modeli nedir?
9. Sektör kılavuzunu uyarlıyor ve güncelliyor mu? Ve hangi sıklıkta?
10. Mevcut zorlukları ele alma açısından genel yetenekleri nelerdir?
11. Örneğin, Güvenlik, Uyumluluk, Operasyonel Esneklik vb., Kurumsal yönetişim buluttan çıkışın gerçekleştirilmesine yardımcı oluyor mu?
12. Kullandığınız belirli hizmet/hizmetlerle ilgili kesintiler ne sıklıkta yaşanıyor?
13. Müşteri desteğine yönelik deneyiminiz nasıl?

Yukarıdaki aşamalar ışığında uygun adımlar izlenerek çıkış stratejisi belirlenir ve uygulamaya alınır.

**İhlal Olay Yönetimi**

**5.24 Bilgi Güvenliği İhlal Olayı Yönetimi Planlaması ve Hazırlığı**

Kurumumuz, bilgi güvenliği olay yönetimi süreçlerini, rollerini ve sorumluluklarını tanımlayarak, oluşturarak ve ileterek bilgi güvenliği olaylarını yönetmek için planlamakta ve hazırlanmaktadır.

İhlal olay planlaması hazırlıklarında aşağıdakiler dikkate alınmaktadır.

a) temas noktası da dahil olmak üzere bilgi güvenliği olaylarını raporlamak için ortak bir yöntem oluşturmak,

b) kurumumuza yönetim, dokümantasyon, tespit, öncelik belirleme, önceliklendirme, analiz, iletişim ve ilgili tarafları koordine etme dahil olmak üzere bilgi güvenliği olaylarını yönetme yeteneği sağlamak için bir olay yönetimi süreci oluşturmak,

c) kurumumuza bilgi güvenliği olaylarını değerlendirme, yanıt verme ve bunlardan öğrenme yeteneği sağlamak için bir olay yanıt süreci oluşturmak,

d) yalnızca yetkin personelin kurumumuz içindeki bilgi güvenliği olaylarıyla ilgili sorunları ele almasına izin vermek. Personellere periyodik eğitim sağlanmaktadır,

e) Olay müdahale personeli için gerekli eğitim, sertifikalandırma ve devam eden mesleki gelişimi belirlemek için bir süreç oluşturmak.

**5.25 Bilgi Güvenliği İhlal Olaylarını Değerlendirme ve Karar Verme**

Kurumumuz, bilgi güvenliği olaylarını değerlendirmekte ve bunların bilgi güvenliği olayları olarak kategorize edilip edilmeyeceğine karar vermektedir.

Bir olayın sonuçlarının ve önceliğinin tanımlanması için bilgi güvenliği olaylarının bir kategorizasyon ve önceliklendirme şeması üzerinde anlaşmaya varılmaktadır. İhlal olayları bilgi güvenliği olayları olarak kategorize etmek için kriterleri içermektedir. İrtibat noktası, mutabık kalınan planı kullanarak her bir bilgi güvenliği olayını değerlendirmektedir.

Bilgi güvenliği olaylarını koordine etmekten ve bunlara müdahale etmekten sorumlu personel, değerlendirmeyi gerçekleştirmekte ve bilgi güvenliği olaylarına ilişkin bir karar vermektedir.

Değerlendirme ve kararın sonuçları, gelecekte referans ve doğrulama amacıyla ayrıntılı olarak kaydedilmektedir.

**5.26 Bilgi Güvenliği İhlal Olaylarına Yanıt Verme**

Bilgi güvenliği olaylarına, belgelenmiş proseslere uygun olarak yanıt verilmektedir.

Bilgi güvenliği olaylarına gerekli yetkinliğe sahip atanmış bir ekip tarafından müdahale edilmektedir. Yanıt aşağıdakileri içermektedir.

a) olayın sonuçları yayılabilirse, olaydan etkilenen sistemleri içeren,

b) olaydan sonra mümkün olan en kısa sürede kanıt toplamak,

c) kriz yönetimi faaliyetleri ve muhtemelen iş sürekliliği planlarına başvurma dahil olmak üzere gerektiği şekilde yükseltme,

d) ilgili tüm müdahale faaliyetlerinin daha sonraki analizler için uygun şekilde günlüğe kaydedilmesini sağlamak,

e) bilgi güvenliği olayının varlığını veya bununla ilgili herhangi bir ayrıntıyı, bilinmesi gereklilik ilkesini izleyerek tüm ilgili dahili ve harici ilgili taraflara iletmek,

f) müdahale etkinliğini artırmak ve diğer kuruluşlar için sonuçları en aza indirmeye yardımcı olmak için yetkililer, harici çıkar grupları ve forumlar, tedarikçiler ve müşteriler gibi dahili ve harici taraflarla koordinasyon sağlamak,

g) olay başarılı bir şekilde ele alındıktan sonra, resmi olarak kapatılır ve kaydedilir,

h) gerektiği şekilde bilgi güvenliği analizi yapmak,

i) kök nedeni belirlemek için olay sonrası analiz yapmak,

j) Olaya neden olan, katkıda bulunan veya önleyemeyen kontrollerle ilgili olanlar da dahil olmak üzere bilgi güvenliği açıklarını ve zayıflıklarını belirleme ve yönetme.

**5.27 Bilgi Güvenliği İhlal Olaylarından Ders Çıkarma**

Bilgi güvenliği olaylarından elde edilen bilgiler, bilgi güvenliği kontrollerini güçlendirmek ve iyileştirmek için kullanılmaktadır.

Bilgi güvenliği olaylarının değerlendirilmesinden elde edilen bilgiler şu amaçlarla kullanılmaktadır.

a) olay senaryoları ve prosedürleri dahil olmak üzere olay yönetimi planını geliştirmek,

b) Kurumumuzun, bilgi güvenliği risk değerlendirmesini güncellemek için tekrar eden veya ciddi olayları ve bunların nedenlerini belirlemek ve gelecekteki benzer olayların olasılığını veya sonuçlarını azaltmak için gerekli ek kontrolleri belirlemek ve uygulamak. Olay türleri, hacimleri ve maliyetleri hakkında bilgilerin toplanması, miktarının belirlenmesi ve izlenmesini sağlayan mekanizmalar,

c) neler olabileceğine, bu tür olaylara nasıl müdahale edileceğine ve gelecekte bunlardan nasıl kaçınılacağına dair örnekler sağlayarak kullanıcı farkındalığını ve eğitimini planlamaktadır.

**5.28 Kanıt Toplama**

Kurumumuz, bilgi güvenliği olaylarıyla ilgili kanıtların tanımlanması, toplanması, elde edilmesi ve korunması için prosesler oluşturmakta ve uygulamaktadır.

Delillerin tipik olarak uygun ulusal mahkemelerde veya başka bir disiplin kurulunda kabul edilebilir bir şekilde toplanması amaçlanmaktadır.

a) kayıtlar eksiksiz ve hiçbir şekilde tahrif edilmemiş,

b) elektronik delillerin kopyaları orjinalleriyle aynı,

c) Kanıtın toplandığı herhangi bir bilgi sistemi, delilin kaydedildiği sırada doğru bir şekilde çalışıyordu,

Mümkün olduğu durumlarda, korunan kanıtların değerini güçlendirmek için belgelendirme veya personel ve araçların kalifikasyonu için diğer ilgili araçlar aranmaktadır.

Dijital kanıtlar, kurumsal veya yargı sınırlarını aşabilir. Bu gibi durumlarda, kurumumuz gerekli bilgileri dijital kanıt olarak toplama yeteneğine sahip olacak uygulamalar kullanmaktadır.

**İş Sürekliliği**

**5.29 Kesinti Sırasında Bilgi Güvenliği**

Kurumumuz, kesinti sırasında bilgi güvenliğini uygun bir seviyede nasıl sürdüreceğini planlamaktadır.

Kurumumuz, aşağıdakileri uygulamakta ve sürdürmektedir.

a) iş sürekliliği ve BİT sürekliliği planları dahilinde bilgi güvenliği kontrolleri, destekleyici sistemler ve araçlar,

b) kesinti sırasında mevcut bilgi güvenliği kontrollerini sürdürmek için süreçler,

c) kesinti sırasında sürdürülemeyen bilgi güvenliği kontrolleri için telafi edici kontroller.

İş sürekliliği ve BİT sürekliliği planlaması bağlamında, normal çalışma koşullarına kıyasla kesintinin türüne bağlı olarak bilgi güvenliği gereksinimlerinin uyarlanması gerekebilir. İş sürekliliği yönetimi kapsamında gerçekleştirilen iş etki analizi ve risk değerlendirmesinin bir parçası olarak, kullanılabilirliği sürdürme ihtiyacına ek olarak bilgilerin gizliliğinin ve bütünlüğünün kaybının sonuçları dikkate alınarak ve önceliklendirilmektedir.

**5.30 İş Sürekliliği için BİT Hazırlığı**

BİT hazırlığı, iş sürekliliği hedefleri ve BİT sürekliliği gereklilikleri temelinde planlanmakta, uygulanmakta, sürdürülerek test edilmektedir.

Kurumumuz şunları sağlamaktadır.

a) gerekli sorumluluk, yetki ve yetkinliğe sahip personel tarafından desteklenen bir aksamaya hazırlanmak, etkisini azaltmak ve müdahale etmek için yeterli bir organizasyon yapısının mevcut olması,

b) kurumunuzun bir BİT hizmet kesintisini nasıl yönetmeyi planladığını detaylandıran müdahale ve kurtarma prosedürleri dahil olmak üzere BİT süreklilik planları şunlardır,

1) egzersizler ve testlerle düzenli olarak değerlendirilir,

2) yönetim tarafından onaylı,

c) BİT süreklilik planları aşağıdaki BİT süreklilik bilgilerini içerir,

1) BIA'da belirtilen iş sürekliliği gereksinimlerini ve hedeflerini karşılamak için performans ve kapasite özellikleri,

2) Her bir önceliklendirilmiş BİT hizmetinin Recovery Time Object RTO'su ve bu bileşenlerin geri yüklenmesine yönelik prosesler,

3) Bilgi olarak tanımlanan öncelikli BİT kaynaklarının Recovery Point Object RPO'su ve bilgiyi geri yükleme prosesleri uygulanmaktadır.

**5.31 Yasal, Meşru, Düzenleyici ve Sözleşmeye Tabi Gereklilikler**

Bilgi güvenliği ile ilgili yasal, yasal, düzenleyici ve sözleşmeden doğan gereksinimler ve kurumumuzunun bu gereksinimleri karşılama yaklaşımı tanımlı olarak belgelenmekte ve güncel tutulmaktadır.

Aşağıdaki durumlarda yasal, kanuni, düzenleyici veya sözleşmeden doğan gereklilikler dahil olmak üzere harici gereklilikler dikkate alınmaktadır.

a) bilgi güvenliği politikaları ve prosedürleri geliştirmek,

b) bilgi güvenliği kontrollerinin tasarlanması, uygulanması veya değiştirilmesi,

c) dahili ihtiyaçlar veya tedarikçi anlaşmaları için bilgi güvenliği gereksinimlerini belirleme sürecinin bir parçası olarak bilgileri ve diğer ilişkili varlıkları sınıflandırmak,

d) bilgi güvenliği risk değerlendirmelerinin yapılması ve bilgi güvenliği risk işleme faaliyetlerinin belirlenmesi,

e) bilgi güvenliğine ilişkin ilgili rol ve sorumluluklarla birlikte süreçlerin belirlenmesi,

f) tedarikçilerin kurumumuzla ilgili sözleşme gerekliliklerini ve ürün ve hizmetlerin tedarik kapsamını belirlemek.

Mevzuat ve yönetmelikler Kuruluş:

a) kendi iş türüne göre gerekliliklerden haberdar olmak için kurumumuzun bilgi güvenliği ile ilgili tüm mevzuat ve düzenlemeleri belirlenmiştir.

b) Kurumumuz aşağıdaki durumlarda, tüm ilgili ülkelerde uyumluluğu dikkate alacaktır.

— diğer ülkelerde iş yürütür,

— yasa ve yönetmeliklerin kurumumuzunu etkileyebileceği diğer ülkelerden ürün ve hizmetler kullanır,

— yasaların ve düzenlemelerin kurumumuzu etkileyebileceği yargı sınırları ötesine bilgi aktarır,

c) değişikliklerden haberdar olmak ve yeni mevzuat belirlemek için belirlenen mevzuat ve düzenlemeleri düzenli olarak gözden geçirmek,

d) bu gereklilikleri karşılamak için belirli süreçleri ve bireysel sorumlulukları tanımlanmıştır.

**5.32 Fikri Mülkiyet Hakları**

Kurumumuz, fikri mülkiyet haklarını korumak için uygun prosesleri uygulamaktadır.

Fikri mülkiyet olarak kabul edilebilecek herhangi bir materyali korumak için aşağıdaki yönergeler dikkate alınmaktadır.

a) fikri mülkiyet haklarının korunmasına ilişkin konuya özgü bir politikanın tanımlanması ve iletilmesi,

b) yazılım ve bilgi ürünlerinin uyumlu kullanımını tanımlayan fikri mülkiyet hakları uyumluluğu için yayınlama prosesleri,

c) telif hakkının ihlal edilmediğinden emin olmak için yazılımı yalnızca bilinen ve saygın kaynaklardan edinerek,

d) uygun varlık kayıtlarının tutulması ve tüm varlıkların fikri mülkiyet haklarının korunması gereklilikleri ile tanımlanması,

e) lisansların, el kitaplarının vb. sahiplik kanıtının ve kanıtlarının saklanması,

f) lisansta izin verilen maksimum kullanıcı veya kaynak [örneğin, merkezi işlem birimleri (CPU'lar)] sayısının aşılmamasının sağlanması,

g) yalnızca yetkili yazılımların ve lisanslı ürünlerin kurulu olduğundan emin olmak için incelemeler yapmak,

h) uygun lisans koşullarını sürdürmek için prosedürler sağlamak,

i) yazılımı elden çıkarmak veya başkalarına devretmek için prosedürler sağlamak,

j) genel ağlardan ve dış kaynaklardan elde edilen yazılım ve bilgilere ilişkin hüküm ve koşullara uymak,

k) telif hakkı yasası veya geçerli lisansların izin verdiği durumlar dışında ticari kayıtlardan (video, ses) çoğaltmamak, başka bir formata dönüştürmemek veya alıntı yapmamak,

l) telif hakkı yasasının veya geçerli lisansların izin verdiği durumlar dışında, standartları (örn. ISO/IEC Uluslararası Standartları), kitapları, makaleleri, raporları veya diğer belgeleri tamamen veya kısmen kopyalamamak.

**5.33 Kayıtların Korunması**

Kayıtlar kayıp, tahrifat, tahrifat, yetkisiz erişim ve izinsiz yayına karşı korunmaktadır.

Elektronik depolama ortamlarının seçildiği durumlarda, gelecekteki teknoloji değişikliğinden kaynaklanan kayıplara karşı koruma sağlamak için saklama süresi boyunca kayıtlara (hem depolama ortamı hem de formatın okunabilirliği) erişme olanağını sağlamaya yönelik prosesler oluşturulmaktsdır. Şifreli arşivler veya dijital imzalarla ilişkili tüm ilgili kriptografik anahtarlar ve programlar da, kayıtların tutulduğu süre boyunca kayıtların şifresinin çözülmesini sağlamak için saklanmaktaıdır.

**5.34 Kişiyi Tespit Bilgisinin (PII) Gizliliği ve Korunması**

Kurumumuz, yürürlükteki yasalara ve düzenlemelere ve sözleşme gerekliliklerine göre gizliliğin korunması ve PII'nin korunmasına ilişkin gereklilikleri belirlemekte ve karşılamaktadır.

Kurumumuz, ilgili tüm taraflara PII'nin gizliliği ve korunması hakkında konuya özel bir süreçler oluşturmakta ve iletmektedir.

Kurumumuz, gizliliğin korunması ve PII'nin korunması için prosedürler geliştirmeli ve uygulamaktadır. Bu prosesler, kişisel olarak tanımlanabilir bilgilerin işlenmesinde yer alan tüm ilgili taraflara iletilmektedir.

PII'yi ele alma sorumluluğu, ilgili mevzuat ve yönetmelikler dikkate alınarak ele alınmaktadır.

PII'yi korumak için uygun teknik ve organizasyonel önlemler uygulanmaktadır.

**5.35 Bilgi Güvenliğinin Bağımsız Gözden Geçirilmesi**

Kurumumuz, bilgi güvenliğini yönetim yaklaşımı ve insanlar, süreçler ve teknolojiler dahil olmak üzere uygulanması, planlanan aralıklarla veya önemli değişiklikler meydana geldiğinde bağımsız olarak gözden geçirilmektedir.

Yönetim, periyodik bağımsız incelemeleri planlamakta ve başlatmaktadır. Gözden geçirmeler, iyileştirme fırsatlarının değerlendirilmesini ve bilgi güvenliği politikası, konuya özel politikalar ve diğer kontroller dahil olmak üzere bilgi güvenliği yaklaşımındaki değişiklik ihtiyacını içermektedir.

Bu tür gözden geçirmeler, incelenmekte olan alandan bağımsız kişiler tarafından yapılmalıdır (örneğin, iç denetim fonksiyonu, bağımsız bir yönetici veya bu tür incelemelerde uzmanlaşmış harici bir taraf kuruluş). Bu incelemeleri yürüten kişiler uygun yetkinliğe sahip olmalıdır. İncelemeleri yürüten kişi, değerlendirme yapmak için bağımsızlığa sahip olmalarını sağlayacak yetkiler doğrultusunda olmamaktadır.

Bağımsız incelemelerin sonuçları, incelemeleri başlatan yönetime ve uygunsa üst yönetime rapor edilmektedir.

**5.36 Bilgi Güvenliğine Yönelik Politikalar, Kurallar ve Standartlara Uygunluk**

Kurumumuz,bilgi güvenliği politikasına, konuya özel politikalarına, kurallarına ve standartlarına uygunluk düzenli olarak gözden geçirilmektedir.

İnceleme sonucunda herhangi bir uygunsuzluk bulunursa, yöneticiler şunları yapmaktadır.

a) uyumsuzluğun nedenlerini belirlemek,

b) uyumluluğu sağlamak için düzeltici eylemlere duyulan ihtiyacı değerlendirmek,

c) uygun düzeltici eylemleri uygulamak,

d) etkinliğini doğrulamak ve eksiklikleri veya zayıflıkları belirlemek için alınan düzeltici faaliyetleri gözden geçirin.

**5.37 Dokümante Edilmiş İşletim Prosedürleri**

Bilgi işleme tesisleri için işletim prosedürleri belgelenmeli ve bunlara ihtiyacı olan personele sunulmaktadır.

Kurumumuz, bilgi güvenliği ile ilgili operasyonel faaliyetleri için dokümante edilmiş prosedürler hazırlanmaktadır, örneğin:

a) etkinliğin birçok kişi tarafından aynı şekilde yapılması gerektiğinde,

b) aktivite nadiren yapıldığında ve bir sonraki yapıldığında prosedür unutulmuş olabilir,

c) faaliyet yeni olduğunda ve doğru yapılmadığı takdirde risk oluşturduğunda,

d) faaliyeti yeni personele devretmeden önce.

**6. Kişi Kontrolleri**

**6.1 Tarama**

Personel olacak tüm adayların geçmiş doğrulama kontrolleri, kurulu kurumumuza katılmadan önce ve sürekli olarak yürürlükteki yasalar, yönetmelikler ve etik değerler dikkate alınarak ve iş gereklilikleri, erişilecek bilgilerin sınıflandırılması ve algılanan riskler doğrultusunda yapılmaktadır.

Doğrulama, ilgili tüm gizlilik, PII koruması ve istihdama dayalı mevzuatı dikkate almalı ve izin verildiği takdirde aşağıdakileri içermektedir.

a) tatmin edici referansların mevcudiyeti (örn. ticari ve kişisel referanslar),

b) başvuranın özgeçmişinin (tamlık ve doğruluk açısından) doğrulanması,

c) iddia edilen akademik ve profesyonel niteliklerin teyidi,

d) bağımsız kimlik doğrulaması (örn. pasaport veya uygun makamlar tarafından verilen diğer kabul edilebilir belgeler),

d) aday kritik bir rol üstlenirse, kredi incelemesi veya sabıka kayıtlarının incelenmesi gibi daha ayrıntılı doğrulama,

Belirli bir bilgi güvenliği rolü için bir kişi işe alındığında, kurumumuzun adayın,

a) güvenlik rolünü yerine getirmek için gerekli yetkinliğe sahiptir,

b) özellikle rol kurumumuz için kritikse, rolü üstlenme konusunda güvenilebilir.

**6.2 İstihdam Hüküm ve Koşulları**

İş sözleşmesine dayalı sözleşmeler, personelin ve kurumumuzun bilgi güvenliğine ilişkin sorumluluklarını belirtmektedir.

Personel için sözleşmeden doğan yükümlülükler, kurumumuzun bilgi güvenliği politikasını ve ilgili konuya özgü politikaları dikkate alınmaktadır.

Ayrıca aşağıdaki hususlar;

a) gizli bilgilere erişim hakkı verilen personelin, bilgilere ve diğer ilgili varlıklara erişim verilmeden önce imzalaması gereken gizlilik veya ifşa etmeme anlaşmaları,

b) yasal sorumluluklar ve haklar [örneğin, telif hakkı yasaları veya veri koruma mevzuatı,

c) bilgilerin sınıflandırılması ve kurumumuzun bilgilerinin ve diğer ilgili varlıkların yönetimi, bilgi işleme tesisleri ve personel tarafından yürütülen bilgi, hizmetleri için sorumluluklar,

d) ilgili taraflardan alınan bilgilerin işlenmesine yönelik sorumluluklar,

e) personelin kurumumuzun güvenlik gereksinimlerini dikkate almaması durumunda alınacak önlemler.

**6.3Bilgi Güvenliği Farkındalığı, Eğitim ve Öğretim**

Kurumumuz, personeli ve ilgili taraflar, iş işlevleriyle ilgili olarak, uygun bilgi güvenliği farkındalığı, eğitim ve öğretim ve kurumumuzun bilgi güvenliği politikası, konuya özel politikalar ve prosedürler hakkında düzenli güncellemeler almaktadır.

Bilgi güvenliği farkındalığı, aşağıdakiler gibi genel hususları kapsamaktadır.

a) yönetimin kurumumuz genelinde bilgi güvenliği taahhüdü,

b) bilgi güvenliği politikası ve konuya özel politikalar, standartlar, yasalar, tüzükler, yönetmelikler, sözleşmeler ve sözleşmeler dikkate alınarak, geçerli bilgi güvenliği kuralları ve yükümlülükleri ile ilgili aşinalık ve uyum ihtiyaçları,

c) kişinin kendi eylemleri ve eylemsizlikleri için kişisel sorumluluğu ve kurumumuza ve ilgili taraflara ait bilgilerin güvenliğini sağlamaya veya korumaya yönelik genel sorumlulukları,

d) temel bilgi güvenliği prosedürleri [örn. bilgi güvenliği olay raporlaması ve temel kontroller örn. şifre güvenliği,

e) Daha fazla bilgi güvenliği farkındalık materyalleri de dahil olmak üzere bilgi güvenliği konularında ek bilgi ve tavsiye için irtibat noktaları ve kaynakları.

**6.4 Disiplin Süreci**

Bilgi güvenliği politikasını ihlal eden personele ve diğer ilgili taraflara karşı işlem yapmak için bir disiplin süreci oluşturulmuştur.

Resmi disiplin süreci, aşağıdaki gibi faktörleri dikkate alan kademeli bir yanıt sağlamaktadır.

a) ihlalin doğası (kim, ne, ne zaman, nasıl) ve ciddiyeti ve sonuçları,

b) suçun kasıtlı (kötü niyetli) veya kasıtsız (kazara) olup olmadığı,

c) bunun ilk veya tekrarlanan bir suç olup olmadığı,

d) ihlal edenin uygun şekilde eğitilip eğitilmediği.

**6.5 İstihdamın Sona Ermesinden veya Değiştirilmesinden Sonraki Sorumluluklar**

İstihdamın sona ermesinden veya değiştirilmesinden sonra geçerli olan bilgi güvenliği sorumlulukları ve görevleri tanımlanmalı, uygulanmalı ve ilgili personele ve diğer ilgili taraflara iletilmektedir.

Gerekli görüldüğü hallerde Iişten ayrılan veya rollerini değiştiren herhangi bir kişinin sahip olduğu bilgi güvenliği rolleri ve sorumlulukları tanımlanmakta ve başka bir bireye devredilmektedir.

Değişikliklerin ve işletim prosedürlerinin personele, diğer ilgili taraflara ve ilgili irtibat kişilerine (örn. müşteriler ve tedarikçilere) iletilmesi için bir süreç oluşturulmaktadır.

Personelin, kurumumuzla olan sözleşmesinin veya işinin sona ermesi veya kurumumuz içinde iş değişikliği olması durumunda, işe son verme veya değişiklik süreci dış personele (yani tedarikçilere) de uygulanmaktadır.

**6.6 Gizlilik ve İfşa Etmeme Anlaşmaları**

Kurumumuz, bilgilerin korunmasına yönelik ihtiyaçlarını yansıtan gizlilik veya ifşa etmeme anlaşmaları personel ve diğer ilgili taraflarca tanımlanmalı, belgelenmeli, düzenli olarak gözden geçirilmeli ve imzalanmaktadır.

Gizlilik veya ifşa etmeme anlaşmalarına yönelik gereklilikleri belirlemek için aşağıdaki unsurlar dikkate alınmalıdır.

a) korunacak bilginin tanımı (örn. gizli bilgi),

b) gizliliğin süresiz olarak veya bilgi kamuya açık hale gelene kadar sürdürülmesinin gerekli olabileceği durumlar da dahil olmak üzere, bir anlaşmanın beklenen süresi,

c) bir sözleşme feshedildiğinde gerekli işlemler,

d) yetkisiz bilgi ifşasını önlemek için imzalayanların sorumlulukları ve eylemleri,

e) bilgilerin, ticari sırların ve fikri mülkiyetin mülkiyeti ve bunun gizli bilgilerin korunmasıyla nasıl bir ilişkisi olduğu,

f) gizli bilgilerin izin verilen kullanımı ve imza sahibinin bilgileri kullanma hakları,

g) çok hassas durumlar için gizli bilgileri içeren faaliyetleri denetleme ve izleme hakkı,

h) yetkisiz ifşa veya gizli bilgi sızıntısının bildirilmesi ve raporlanması süreci,

i) sözleşme feshedildiğinde iade edilecek veya imha edilecek bilgilere ilişkin şartlar,

j) sözleşmeye uyulmaması durumunda alınması beklenen önlemler.

**6.7 Uzaktan Çalışma**

Personel, kurumumuz tesisleri dışında erişilen,

çalışmaya ilişkin ilgili koşulları ve kısıtlamaları tanımlayan konuya özel bir süreç yayınlamaktadır. Uygulanabilir olduğu durumlarda, aşağıdaki hususlar dikkate alınmaktadır.

a) personelin bulunduğu farklı yetki alanları da dahil olmak üzere, konumun ve yerel ortamın fiziksel güvenliğini dikkate alarak, uzak çalışma sahasının mevcut veya önerilen fiziksel güvenliği,

b) kilitlenebilir dosya dolapları, konumlar arasında güvenli ulaşım ve uzaktan erişim kuralları, açık masa, bilgilerin ve diğer ilgili varlıkların yazdırılması ve imhası ve bilgi güvenliği olay raporlaması gibi uzak fiziksel ortam için kurallar ve güvenlik mekanizmaları,

c) beklenen fiziksel uzaktan çalışma ortamları;

d) kurumumuzun sistemlerine uzaktan erişim ihtiyacı, iletişim bağlantısı üzerinden erişilecek ve aktarılacak bilgilerin hassasiyeti ile sistem ve uygulamaların hassasiyeti dikkate alınarak iletişim güvenliği gereklilikleri,

e) özel sektöre ait ekipmanlarda bilgilerin işlenmesini ve saklanmasını destekleyen sanal masaüstü erişimi gibi uzaktan erişimin kullanılması,

f) uzak çalışma sahasındaki diğer kişilerden (örn. aile ve arkadaşlar) gelen bilgilere veya kaynaklara yetkisiz erişim tehdidi,

g) halka açık yerlerde diğer kişilerden gelen bilgilere veya kaynaklara yetkisiz erişim tehdidi,

h) ev ağlarının ve genel ağların kullanımı ve kablosuz ağ hizmetlerinin yapılandırılmasına ilişkin gereksinimler veya kısıtlamalar,

i) güvenlik duvarları ve kötü amaçlı yazılımlara karşı koruma gibi güvenlik önlemlerinin kullanımı,

j) sistemleri uzaktan devreye almak ve başlatmak için güvenli mekanizmalar,

k) kurumumuzun ağına uzaktan erişime izin verilen tek faktörlü kimlik doğrulama mekanizmalarının güvenlik açığını dikkate alarak kimlik doğrulama ve erişim ayrıcalıklarının etkinleştirilmesi için güvenli mekanizmalar.

**6.8 Bilgi Güvenliği Olay Raporlaması**

Kurumumuz, personelin gözlemlenen veya şüphelenilen bilgi güvenliği olaylarını uygun kanallar aracılığıyla zamanında bildirmesi için bir mekanizma sağlamaktadır.

Bilgi güvenliği olay raporlaması için dikkate alınması gereken durumlar şunları içerir;

a) etkisiz bilgi güvenliği kontrolleri,

b) bilgi gizliliği, bütünlüğü veya erişilebilirlik beklentilerinin ihlali,

c) insan hataları,

ç) bilgi güvenliği politikasına, konuya özel politikalara veya geçerli standartlara uyulmaması,

e) fiziksel güvenlik önlemlerinin ihlali,

e) değişiklik yönetimi sürecinden geçmemiş sistem değişiklikleri,

f) yazılım veya donanımın arızaları veya diğer anormal sistem davranışları,

h) erişim ihlalleri,

ğ) güvenlik açıkları,

h) şüpheli kötü amaçlı yazılım bulaşması.

**7. Fiziksel Kontroller**

**7.1 Fiziksel Güvenlik Sınırları**

Bilgi ve diğer ilişkili varlıkları içeren alanları korumak için güvenlik çevreleri tanımlı ve kullanılmaktadır.

Fiziksel güvenlik çevreleri için aşağıdaki yönergeler dikkate alınmaktadır.

a) çevre içindeki varlıklarla ilgili bilgi güvenliği gerekliliklerine uygun olarak güvenlik çevrelerinin ve çevrelerin her birinin konumunun fiziksel şartlar dikkate alınmaktadır.

b) bilgi işleme tesisleri içeren bir bina veya site için fiziksel olarak sağlam çevre kenarlarına sahip olmak (yani çevrede veya bir zorla girmenin kolayca meydana gelebileceği alanlarda boşluklarda bulunmamaktadır).

Sahanın dış çatıları, duvarları, tavanları ve döşemeleri sağlam yapıda ve tüm dış kapılar yetkisiz erişime karşı kontrol mekanizmalarıyla (örn.parmaklıklar, alarmlar, kilitler) uygun şekilde korunmaktadır. Kapılar ve pencereler gözetimsizken kilitlenmekte ve özellikle yer seviyesindeki pencereler için harici koruma düşünülmektedir, havalandırma noktaları da dikkate alınmaktadır,

**7.2 Fiziksel Giriş**

Güvenli alanlar, uygun giriş kontrolleri ve erişim noktaları ile korunmaktadır.

Aşağıdaki yönergeler dikkate alınarak fiziksel güvenlik tedbirleri alınmaktadır.

a) sitelere ve binalara erişimi yalnızca yetkili personelle kısıtlamak.

Fiziksel alanlara erişim haklarının yönetimine ilişkin süreç, yetkilendirmelerin sağlanmasını, periyodik olarak gözden geçirilmesini, güncellenmesini ve iptal edilmesini içermektedir.

b) tüm erişimlerin fiziksel bir kayıt defterini veya elektronik denetim izini güvenli bir şekilde sürdürmek ve izlemek ve tüm günlükleri, hassas kimlik doğrulama bilgilerini korumak,

c) bilgilerin işlendiği veya saklandığı alanlara erişimin yönetimi için bir süreç ve teknik mekanizmaların oluşturulması ve uygulanması.

Kimlik doğrulama mekanizmaları, erişim kartlarının, biyometrinin veya erişim kartı kimlik doğrulamanın kullanımını içerir.

ç) sahaya veya binaya fiziksel erişimi kontrol etmek için personel veya başka yollarla izlenen bir kabul alanı oluşturmak,

d) giriş ve çıkışlarda personel ve ilgililerin şahsi eşyalarını teftiş ve muayene etmek,

NOT Kişisel eşyaların denetlenmesi olasılığına ilişkin yerel mevzuat ve düzenlemeler mevcut durumdadır.

e) tüm personelin ve ilgili tarafların bir çeşit görünür kimlik taşımasını ve refakatsiz ziyaretçilerle ve görünür kimlik taşımayan herhangi biriyle karşılaştıklarında güvenlik personelini derhal bilgilendirmesini zorunlu kılmak. Daimi çalışanları, tedarikçileri ve ziyaretçileri daha iyi tanımlamak için kolayca ayırt edilebilir rozetler vb. kullanılmaktadır.

f) tedarikçi personeline yalnızca gerektiğinde güvenli alanlara veya bilgi işleme tesislerine sınırlı erişim verilmesi. Ayrıca, erişim yetkilendirilmekte ve izlenmektedir,

g) birden çok kuruluş için varlık bulunduran binalar söz konusu olduğunda fiziksel erişim güvenliğine özel önem verilmesi,

ğ) fiziksel olay olasılığı arttığında güçlendirilebilecek şekilde fiziksel güvenlik önlemlerinin tasarlanması,

h) acil durum çıkışları gibi diğer giriş noktalarını yetkisiz erişimden korumak,

ı) fiziksel anahtarların veya kimlik doğrulama bilgilerinin (örn. kilit kodları, ofisler, odalar ve anahtar dolapları gibi tesisler için şifreli kilitler) yönetimini sağlamak ve bir kayıt defteri veya yıllık anahtar denetimi ve fiziksel anahtarlar veya kimlik doğrulama bilgileri kontrol edilir.

**7.3 Ofislerin, Odaların ve Tesislerin Emniyete Alınması**

Ofisler, odalar ve tesisler için fiziksel güvenlik tasarlanarak uygulanmaktadır.

Ofislerin, odaların ve tesislerin güvenliğini sağlamak için aşağıdaki yönergeler dikkate alınmaktadır.

a) halkın erişimini önlemek için kritik tesislerin yerleştirilmesi,

b) uygulanabilir olduğu durumlarda, binaların göze batmayan ve binanın içinde veya dışında, bilgi işleme faaliyetlerinin varlığını tanımlayan belirgin işaretler olmadan amaçlarına dair asgari düzeyde bilgi vermesini sağlamak,

c) gizli bilgilerin veya faaliyetlerin dışarıdan görünür ve işitilebilir olmasını önlemek için tesislerin yapılandırılması.

ç) rehberleri, dahili telefon rehberlerini ve gizli bilgi işleme tesislerinin yerlerini tanımlayan çevrimiçi erişilebilir haritaları herhangi bir yetkisiz kişi için hazır hale getirmemek.

**7.4 Fiziksel Güvenlik İzleme**

Tesisler yetkisiz fiziksel erişime karşı sürekli olarak izlenmektedir

Kritik sistemleri barındıran binalara erişim, yetkisiz erişimi veya şüpheli davranışı tespit etmek için aşağıdakiler tarafından sürekli olarak izlenmektedir.

a) Bina /binalar içindeki ve dışındaki hassas alanları görüntülemek ve bu alanlara erişimi kaydetmek için kapalı devre televizyon gibi video izleme sistemlerinin kurulması,

b) ilgili geçerli standartlara göre kurmak ve aşağıdakiler gibi izinsiz giriş alarmını tetiklemek için temas, ses veya hareket dedektörlerini periyodik olarak test etmek,

1) panik alarmı olarak kullanılmak üzere temasın kurulabileceği veya bozulabileceği herhangi bir yere (pencere ve kapılar ve nesnelerin altları gibi) bir temas kurulduğunda veya koptuğunda bir alarmı tetikleyen kontak dedektörlerinin kurulması,

2) görüş alanlarından bir nesne geçtiğinde bir alarmı tetikleyen kızılötesi teknolojiye dayalı hareket dedektörleri,

3) güvenlik personelini uyarmak için bir alarmı tetiklemek üzere kullanılabilecek, kırılan camın sesine duyarlı sensörlerin kurulması,

c) tüm dış kapıları ve erişilebilir pencereleri kapatmak için bu alarmları kullanmak. Boş alanlar her zaman alarma geçirilmektedir; diğer alanlar için de koruma sağlanmaktadır (örn. bilgisayar veya iletişim odaları).

**7.5 Fiziksel ve Çevresel Tehditlere Karşı Koruma**

Doğal afetler ve altyapıya yönelik diğer kasıtlı veya kasıtsız fiziksel tehditler gibi fiziksel ve çevresel tehditlere karşı koruma tasarlanarak uygulanmaktadır.

Fiziksel ve çevresel tehditlerin potansiyel sonuçlarını belirlemek için risk değerlendirmeleri, fiziksel bir tesiste kritik operasyonlara başlamadan önce ve düzenli aralıklarla yapılmaktadır. Gerekli önlemler uygulanmakta ve tehditlerdeki değişiklikler izlenmektedir.

Risk değerlendirmesi sonuçlarına dayalı olarak, ilgili fiziksel ve çevresel tehditler belirlenerek ve uygun kontroller aşağıdaki bağlamlarda örnek olarak değerlendirilmektedir.

a) yangın: depolama ortamına ve ilgili bilgi işleme sistemlerine yangın hasarını önlemek için alarm göndermek veya yangın söndürme sistemlerini tetiklemek için yangınları erken bir aşamada algılayabilen sistemlerin kullanılmaktadır. Yangın söndürme, çevredeki ortama göre en uygun madde kullanılarak yapılmaktadır (örn. kapalı alanlardaki gaz),,

b) su baskını: depolama ortamı veya bilgi işleme sistemleri içeren alanların zeminlerinin altına su baskınını erken bir aşamada tespit edebilen sistemlerin kullanılmaktdır. Taşkın meydana gelmesi durumunda su pompaları veya eşdeğer araçlar hazır bulundurulmaktadır;

c) elektrik dalgalanmaları: bu tür olayların sonuçlarını en aza indirmek için hem sunucu hem de istemci bilgi sistemlerini elektrik dalgalanmalarına veya benzer olaylara karşı koruyabilen sistemlerin benimsenmesi;

**7.6 Güvenli Alanlarda Çalışma**

Güvenli alanlarda çalışmak için güvenlik önlemleri tasarlanarak uygulanmaktadır.

Güvenli alanlarda çalışmaya yönelik güvenlik önlemleri tüm personel için geçerli olmakta ve güvenli alanda gerçekleşen tüm faaliyetleri kapsamaktadır.

Aşağıdaki yönergeler dikkate alınmaktadır.

a) personelin yalnızca ihtiyaç-bilme bazında güvenli bir alanın varlığından veya içindeki faaliyetlerden haberdar edilmesi,

b) hem güvenlik nedenleriyle hem de kötü niyetli faaliyet olasılığını azaltmak için güvenli alanlarda denetimsiz çalışmaktan kaçınmak,

c) boş güvenli alanların fiziksel olarak kilitlenmesi ve periyodik olarak denetlenmesi,

d) yetkilendirilmedikçe, kullanıcı uç nokta cihazlarında fotoğraf, video, ses veya kamera gibi diğer kayıt ekipmanlarına izin verilmemesi,

e) kullanıcı uç nokta cihazlarının güvenli alanlarda taşınması ve kullanımının uygun şekilde kontrol edilmesi,

f) bildirimleri kolayca görülebilir veya erişilebilir bir şekilde asmak.

**7.7 Temiz Masa ve Temiz Ekran**

Kağıtlar ve çıkarılabilir depolama ortamları için net masa kuralları ve bilgi işleme tesisleri için net ekran kuralları tanımlanmakta ve uygun şekilde uygulanmaktadır.

Kurumumuz, açık masa ve açık ekran üzerinde konuya özgü bir proses oluşturmakta ve ilgili tüm taraflara iletmektedir. Aşağıdaki yönergeler dikkate alınmaktadır.

a) gerekmediğinde, özellikle ofis boşken hassas veya kritik iş bilgilerini (örn. kağıt veya elektronik depolama ortamında) (ideal olarak bir kasada, dolapta veya başka bir güvenlik mobilyasında) kilitlemek,

b) kullanıcı uç nokta cihazlarının kullanılmadığı veya gözetim altında olmadığı zamanlarda anahtar kilitleri veya diğer güvenlik araçlarıyla korunması,

c) kullanıcı uç nokta cihazlarının oturumu kapatılmış veya gözetimsiz durumdayken bir kullanıcı kimlik doğrulama mekanizması tarafından kontrol edilen bir ekran ve klavye kilitleme mekanizmasıyla korunmuş halde bırakılması. Tüm bilgisayarlar ve sistemler, bir zaman aşımı veya otomatik oturum kapatma özelliği ile yapılandırılmalıdır,

d) oluşturucunun yazıcılardan veya çok işlevli cihazlardan çıktıları hemen toplamasını sağlamak. Kimlik doğrulama işlevine sahip yazıcıların kullanılması, böylece çıktılarını yalnızca oluşturucular alabilir ve yalnızca yazıcının yanında dururken,

e) hassas bilgiler içeren belgeleri ve çıkarılabilir depolama ortamını güvenli bir şekilde saklamak ve artık gerekli olmadığında bunları güvenli imha mekanizmaları kullanarak atmak,

f) ekranlardaki açılır pencerelerin yapılandırılması için kuralların ve rehberliğin oluşturulması ve iletilmesi (örneğin, sunumlar sırasında, ekran paylaşımında veya halka açık bir alanda mümkünse yeni e-posta ve mesajlaşma açılır pencerelerinin kapatılması),

g) artık gerekli olmadığında beyaz tahtalar ve diğer ekran türleri üzerindeki hassas veya kritik bilgileri temizleme.

Kurumumuz, tesislerden ayrılırken, kurumumuz varlıklarının geride bırakılmadığından emin olmak için ayrılmadan önce son bir tarama yapmak da dahil olmak üzere yürürlükte olan proseslere sahip olmaktadır (örneğin, çekmecelerin veya mobilyaların arkasına düşen belgeler)

**7.8 Ekipman Konumlandırma ve Koruma**

Ekipman güvenli bir şekilde yerleştirilmekte ve korunmaktadır.

Ekipmanı korumak için aşağıdaki yönergeler dikkate alınmaktadır.

a) çalışma alanlarına gereksiz erişimi en aza indirmek ve yetkisiz erişimi önlemek için ekipman yerleştirme,

b) kullanımları sırasında bilgilerin yetkisiz kişilerce görüntülenmesi riskini azaltmak için hassas verileri işleyen bilgi işleme tesislerinin dikkatli bir şekilde konumlandırılması,

c) potansiyel fiziksel ve çevresel tehdit riskini en aza indirmek için kontroller benimsemek [örneğin hırsızlık, yangın, patlayıcılar, duman, su (veya su kaynağı arızası), toz, titreşim, kimyasal etkiler, elektrik kaynağı paraziti, iletişim paraziti, elektromanyetik radyasyon ve vandalizm],

d) Bilgi işlemeye yakın yerlerde yemek yeme, içme ve sigara içmeye yönelik yönergeler oluşturmak,

e) bilgi işleme tesislerinin çalışmasını olumsuz etkileyebilecek koşullar için sıcaklık ve nem gibi çevresel koşulların izlenmesi,
f) tüm binalara yıldırımdan korunma uygulamak ve gelen tüm güç ve iletişim hatlarına yıldırımdan korunma filtreleri takmak,

g) endüstriyel ortamlardaki ekipmanlar için klavye membranları gibi özel koruma yöntemlerinin kullanılması dikkate alınarak,

h) elektromanyetik yayılım nedeniyle bilgi sızıntısı riskini en aza indirmek için gizli bilgileri işleyen ekipmanı korumak,

i) kurumumuz tarafından yönetilen bilgi işleme tesislerini kurumumuz tarafından yönetilmeyenlerden fiziksel olarak ayırmak.

**7.9 Kuruluş Dışındaki Varlıkların Güvenliği**

Kurumumuz dışındaki varlıklar korunmaktadır.

Kurumumuza ait cihazlar ve özel mülkiyete ait olan ve kurumumuz adına kullanılan cihazlar kendi cihazını getir (BYOD) dahil olmak üzere, bilgileri depolayan veya işleyen kurumumuzun tesisleri dışında kullanılan tüm cihazların (örneğin mobil cihaz) korunmaya ihtiyacı vardır. Bu cihazların kullanımı yönetimm tarafından yetkilendirilmektedir.

Ekipmanı kurumumuz tesislerinin dışına yerleştirirken aşağıdaki yönergeler dikkate alınmaktadır.

a) fiziksel güvenlik izleme,

b) fiziksel ve çevresel tehditlere karşı koruma,

c) fiziksel erişim ve kurcalamaya karşı koruma kontrolleri,

d) mantıksal erişim kontrolleri, güvenli, güvenli bir ortamda depolamak ve bunları çevresel tehditlere (ısı, nem, rutubet, elektronik alan veya eskime gibi) karşı üretici spesifikasyonlarına göre korumak,

d) bilgilerin gizliliği veya bütünlüğü önemli hususlarsa, çıkarılabilir depolama ortamındaki bilgileri korumak için kriptografik teknikler kullanmak,

e) depolanan bilgilere ihtiyaç duyulurken depolama ortamının bozulma riskini azaltmak, bilgileri okunamaz hale gelmeden önce yeni depolama ortamına aktarmak,

f) tesadüfi bilgi hasarı veya kaybı riskini daha da azaltmak için değerli bilgilerin birden çok kopyasını ayrı depolama ortamlarında depolamak,

g) bilgi kaybı olasılığını sınırlamak için çıkarılabilir depolama ortamının kaydedilmesinin dikkate alınması,

h) yalnızca kullanımları için kurumsal bir neden varsa çıkarılabilir depolama ortamı bağlantı noktalarının [örn. güvenli dijital (SD) kart yuvaları ve evrensel seri veri yolu (USB) bağlantı noktaları] etkinleştirilmesi,

i) Çıkarılabilir depolama ortamının kullanılması gerektiğinde, bilgilerin bu tür bir depolama ortamına aktarımının izlenmesi,

j) bilgiler, örneğin posta hizmeti veya kurye yoluyla depolama ortamını gönderirken, fiziksel taşıma sırasında yetkisiz erişime, kötüye kullanıma veya bozulmaya karşı savunma önlemleri alınmaktadır.

**7.10 Güvenli Yeniden Kullanım veya İmha**

Gizli bilgilerin yetkisiz kişilere sızması riskini en aza indirmek için depolama ortamının güvenli bir şekilde yeniden kullanılması veya atılmasıyla ilgili prosesler oluşturulmaktadır. Gizli bilgiler içeren depolama ortamının güvenli bir şekilde yeniden kullanılması veya imha edilmesiyle ilgili prosesler, bu bilgilerin hassasiyetiyle orantılı olmaktadır. Aşağıdaki öğeler dikkate alınmaktadır.

a) gizli bilgiler içeren depolama ortamının kurumumuz içinde yeniden kullanılması gerekiyorsa, verilerin güvenli bir şekilde silinmesi veya yeniden kullanılmadan önce depolama ortamının biçimlendirilmesi,

b) artık gerekmediğinde gizli bilgileri içeren depolama ortamını güvenli bir şekilde imha etmek (örn. içeriği yok ederek, parçalayarak veya güvenli bir şekilde silerek),

c) güvenli bir şekilde elden çıkarılmasını gerektirebilecek öğeleri belirlemek için yürürlükte olan proseslere sahip olmak,

d) kurumumuz, depolama ortamları için toplama ve imha hizmetleri sunar. Yeterli kontrollere ve deneyime sahip uygun bir dış taraf tedarikçinin seçilmesine özen gösterir,

e) bir denetim izini sürdürmek için hassas öğelerin elden çıkarılmasının günlüğe kaydedilmesi,

f) Saklama ortamını elden çıkarmak için biriktirirken, büyük miktarda hassas olmayan bilginin hassas hale gelmesine neden olabilecek toplama etkisini göz önünde bulundurarak.

Öğelerin onarıma gönderilmek veya atılmak yerine fiziksel olarak imha edilmesi gerekip gerekmediğini belirlemek için hassas veriler içeren hasarlı cihazlarda bir risk değerlendirmesi yapılmaktadır.

**7.11 Destekleyici Altyapı Hizmetleri**

Bilgi işleme tesisleri, destekleyici altyapı hizmetlerindeki arızalardan kaynaklanan elektrik kesintilerinden ve diğer kesintilerden korunmaktadır.

Kurumumuz, bilgi işleme tesislerini desteklemek için hizmetlere (örneğin elektrik, telekomünikasyon, su temini, gaz, kanalizasyon, havalandırma ve iklimlendirme) bağlıdır.

Bu nedenle,

a) destekleyici altyapı hizmetlerini için kullanılan ekipmanların ilgili üreticinin spesifikasyonlarına göre yapılandırılmasını, çalıştırılmasını ve bakımının yapılmasını sağlamak;

b) destekleyici altyapı hizmetlerinin ticari büyümeyi karşılama kapasiteleri ve diğer destekleyici kurumumuzlarla etkileşimleri açısından düzenli olarak değerlendirilmesini sağlamak,

c) destekleyici altyapı hizmetleri için kullanılan ekipmanın düzgün çalışmasını sağlamak için düzenli olarak denetlenmesini ve test edilmesini,

d) gerekirse, destekleyici altyapı hizmetlerin arızalarını tespit etmek için alarm izlenmekte,

e) gerekirse, destekleyici altyapı hizmetlerin farklı fiziksel yönlendirmelere sahip birden çok beslemeye hattına bağlı,

f) destekleyici altyapı hizmetleri için kullanılan ekipmanın, bilgi işleme tesislerinden ayrı bir ağ üzerinde olması,

g) destekleyici altyapı hizmetleri için kullanılan ekipmanın internete yalnızca ihtiyaç duyulduğunda ve yalnızca güvenli bir şekilde bağlanmasını sağlanmaktadır.

Acil durum aydınlatması ve haberleşme sağlanmaktadır. Gücü, suyu, gazı veya diğer hizmetleri kesmek için acil durum anahtarları ve valfleri, acil durum çıkışlarının veya ekipman odalarının yakınına yerleştirilmektedir. Acil durum iletişim bilgileri kaydedilmekte ve bir kesinti durumunda personel tarafından erişilebilir olması sağlanmıştır.

**7.12 Kablo Güvenliği**

Güç, veri veya destekleyici bilgi servislerini taşıyan kablolar, dinleme, girişim veya hasara karşı korunmaktadır.

Kablolama güvenliği için aşağıdaki yönergeler dikkate alınmaktadır.

a) güç ve telekomünikasyon hatlarını, mümkün olduğunda yer altında bulunan veya zemin kablosu koruyucusu ve elektrik direği gibi yeterli alternatif korumaya tabi olan bilgi işleme tesislerine; kablolar yer altındaysa, kazara kesilmelere karşı koruma (örn. zırhlı kanallar veya varlık sinyalleri ile);

b) paraziti önlemek için güç kablolarını iletişim kablolarından ayırmak,

c) hassas veya kritik sistemler için dikkate alınması gereken diğer kontroller şunları içerir:

1. muayene ve sonlandırma noktalarında zırhlı boru ve kilitli odalar veya kutular ve alarmların kurulumu,
2. kabloları korumak için elektromanyetik kalkan kullanımı,
3. kablolara takılan izinsiz cihazları tespit etmek için periyodik teknik taramalar ve fiziksel incelemeler,
4. patch panellere ve kablo odalarına kontrollü erişim (örn. mekanik anahtarlar veya PIN'ler ile),
5. fiber optik kabloların kullanımı;

d) kablonun fiziksel olarak tanımlanmasını ve incelenmesini sağlamak için her iki uçta da yeterli kaynak ve hedef ayrıntılarıyla kabloları etiketleme. Kablolama olaylarından veya arızalarından kaynaklanan risklerin nasıl yönetileceği konusunda uzman tavsiyesi alınmaktadır.

**7.13 Ekipman Bakımı**

Bilginin erişebilirliğini, bütünlüğünü ve gizliliğini sağlamak için ekipman bakımı doğru bir şekilde yapılmaktadır.

Ekipman bakımı için aşağıdaki yönergeler dikkate alınmaktadır.

a) ekipmanın tedarikçinin tavsiye ettiği servis sıklığına ve özelliklerine uygun olarak bakımını yapmak,

b) kurumumuz tarafından bir bakım programının uygulanması ve izlenmesi,

c) yalnızca ekipman üzerinde onarım ve bakım yapan yetkili bakım personeli,

d) tüm şüpheli veya fiili arızaların ve tüm önleyici ve düzeltici bakımın kayıtlarını tutmak,

e) ekipmanın bakımı planlandığında, bu bakımın tesisteki personel tarafından mı yoksa kurumumuz dışından mı yapıldığı dikkate alınarak uygun kontrollerin uygulanması; bakım personelini uygun bir gizlilik sözleşmesine tabi tutmak,

f) sahada bakım yapılırken bakım personelini denetlemek,

g) uzaktan bakım için erişimi yetkilendirme ve kontrol etme,

h) bilgi içeren ekipman bakım için tesis dışına çıkarıldığında tesis dışındaki varlıklar için güvenlik önlemlerinin uygulanması,

i) sigorta tarafından dayatılan tüm bakım gerekliliklerine uymak,

j) bakımdan sonra ekipmanı tekrar çalıştırmadan önce, ekipmanın kurcalanmadığından ve düzgün çalıştığından emin olmak için incelemek,

k) ekipmanın imha edileceği belirlenirse, ekipmanın güvenli bir şekilde imha edilmesi veya yeniden kullanılması için önlemler uygulamak.

Ekipman, bilgi işleme tesislerinin teknik bileşenlerini, kesintisiz güç kaynağını (UPS) ve pilleri, güç jeneratörlerini, güç alternatörlerini ve dönüştürücülerini, fiziksel izinsiz giriş tespit sistemlerini ve alarmlarını, duman dedektörlerini, yangın söndürücüleri, klimayı ve asansörleri içerir.

**7.14 Ekipmanın Güvenli Bir Şekilde Yok Edilmesi veya Tekrar Kullanılması**

Depolama ortamı içeren ekipman öğeleri, tüm hassas verilerin ve lisanslı yazılımların yok edilmeden veya tekrar kullanılmadan önce kaldırıldığından veya güvenli bir şekilde üzerine yazıldığından emin olmak için doğrulanmaktadır.

Gizli veya telif hakkıyla korunan bilgileri içeren depolama ortamı, standart silme işlevi yerine orijinal bilgileri geri alınamaz hale getiren teknikler kullanılarak fiziksel olarak imha edilmekte veya bilgiler yok edilmekte, silinmekte veya üzerine yazılmaktedır.

Kurumumuz, tanımlanan veya sınıflandırmayı, sahibini, sistemini veya ağını gösteren etiketler ve işaretler, yeniden satma veya hayır kurumlarına bağışlama da dahil olmak üzere, imha edilmeden önce çıkarılmaktadır.

Kurumumuz, kiralama süresinin sonunda veya tesis dışına taşınırken erişim kontrolleri veya gözetim ekipmanı gibi güvenlik kontrollerini kaldırmayı düşünmektedir. Bu, aşağıdaki gibi faktörlere bağlıdır:

a) tesisi orijinal durumuna döndürmek için yaptığı kira sözleşmesi,

b) hassas bilgiler içeren sistemleri bir sonraki kiracıya bırakma riskinin en aza indirilmesi (örn. kullanıcı erişim listeleri, video veya resim dosyaları),

c) kontrolleri bir sonraki tesiste yeniden kullanma yeteneği.

Depolama ortamı içeren hasarlı ekipman, öğelerin tamire gönderilmek veya atılmak yerine fiziksel olarak imha edilip edilmemesi gerektiğini belirlemek için bir risk değerlendirmesi yapılmaktadır.

**8. Teknolojik Kontroller**

**8.1 Kullanıcı Uç Nokta Cihazları**

Kullanıcı uç nokta cihazlarında depolanan, bunlar tarafından işlenen veya bunlar aracılığıyla erişilen bilgiler korunmaktadır.

Kurumumuz, kullanıcı uç nokta cihazlarının güvenli konfigürasyonu ve kullanımı hakkında konuya özel bir süreç oluşturmaktadır. Konuya özgü süreç tüm ilgili personele iletilmekte ve aşağıdakiler dikkate alınmaktadır.

a) kullanıcı uç nokta cihazlarının işleyebileceği, işleyebileceği, saklayabileceği veya destekleyebileceği bilgi türü ve sınıflandırma düzeyi,

b) kullanıcı uç nokta cihazlarının kaydı,

c) fiziksel koruma gereksinimleri,

d) yazılım kurulumunun kısıtlanması (örn. sistem yöneticileri tarafından uzaktan kontrol),

e) kullanıcı uç nokta cihazı yazılımı (yazılım sürümleri dahil) ve güncellemelerin uygulanması (örn. aktif otomatik güncelleme) için gereksinimler,

f) bilgi hizmetlerine, genel ağlara veya tesis dışındaki herhangi bir ağa bağlantı kuralları (örn. kişisel güvenlik duvarının kullanılmasını gerektiren),

g) erişim kontrolleri,

h) depolama cihazı şifrelemesi,

i) kötü amaçlı yazılımlara karşı koruma,

j) uzaktan devre dışı bırakma, silme veya kilitleme,

k) yedekler,

l) web servislerinin ve web uygulamalarının kullanımı,

m) son kullanıcı davranışı analitiği,

n) çıkarılabilir bellek aygıtları dahil olmak üzere çıkarılabilir aygıtların kullanımı ve fiziksel bağlantı noktalarını (örn. USB bağlantı noktaları) devre dışı bırakma olasılığı,

o) kullanıcı uç nokta cihazı tarafından destekleniyorsa, kurumumuzun bilgilerini ve diğer ilişkili varlıkları (örn. yazılım) cihazdaki diğer bilgilerden ve diğer ilişkili varlıklardan güvenli bir şekilde ayırabilen bölümleme yeteneklerinin kullanımı.

Belirli bilgilerin, yalnızca kullanıcı uç nokta cihazları aracılığıyla erişilebilecek, ancak bu tür cihazlarda depolanamayacak kadar hassas olup olmadığı dikkate alınmaktadır. Bu gibi durumlarda, cihaz üzerinde ek teknik güvenlik önlemleri gerekebilir. Örneğin, çevrimdışı çalışma için dosya indirmenin ve SD kart gibi yerel depolamanın devre dışı bırakılmasının sağlanması. Mümkün olduğunca, bu kontrole ilişkin tavsiyeler konfigürasyon yönetimi veya otomatikleştirilmiş araçlar aracılığıyla uygulanmaktadır.

Tüm kullanıcılar, kullanıcı uç nokta cihazlarını korumaya yönelik güvenlik gereksinimleri ve prosedürlerinin yanı sıra bu tür güvenlik önlemlerini uygulama sorumlulukları konusunda bilgilendirilmektedir. Kullanıcı uç nokta cihazlarının çalınması veya kaybolması durumlarında, kurumumuzun yasal, kanuni, düzenleyici, sözleşmeden (sigorta dahil) ve diğer güvenlik gerekliliklerini dikkate alan özel bir proses oluşturulmaktadır.

Kurumumuzun, kişisel cihazların (bazen BYOD olarak da bilinir) kullanımına izin verdiği durumlarda, bu kontrolde verilen rehberliğe ek olarak aşağıdakiler dikkate alınmaktadır.

a) özel bir cihazda iş verilerini korumak ve bu ayrımı desteklemek için yazılım kullanmak da dahil olmak üzere, cihazların kişisel ve ticari kullanımının ayrılması,
b) İş bilgilerine yalnızca kullanıcıların görevlerini (fiziksel koruma, yazılım güncelleme vb.) kabul etmelerinden sonra erişim sağlama, iş verilerinin sahipliğinden feragat etme, cihazın çalınması veya kaybolması durumunda veya artık kullanılamayacak durumdayken verilerin kurumumuz tarafından uzaktan silinmesine izin verme hizmeti kullanmaya yetkilidir. Bu gibi durumlarda, PII koruma mevzuatı dikkate alınmaktadır.

c) özel sektöre ait ekipman üzerinde geliştirilen fikri mülkiyet haklarına ilişkin ihtilafları önlemeye yönelik konuya özel politikalar ve prosedürler,
d) mevzuat tarafından engellenebilecek olan özel sektöre ait ekipmana erişim (makinenin güvenliğini doğrulamak için veya bir soruşturma sırasında),

e) kurumumuzların, personele veya dış taraf kullanıcılara ait özel olarak sahip olunan kullanıcı uç nokta cihazlarındaki istemci yazılımları için lisans vermekle yükümlü olabileceği yazılım lisans anlaşmaları.

**kablosuz bağlantılar**

Kurumumuz, aşağıdakiler için prosesler oluşturmaktadır.

a) cihazlarda kablosuz bağlantıların yapılandırılması (örn. güvenlik açığı bulunan protokollerin devre dışı bırakılması);

b) ilgili konuya özgü politikalara uygun olarak uygun bant genişliğine sahip kablosuz veya kablolu bağlantıların kullanılması (örn. yedeklemeler veya yazılım güncellemeleri gerektiğinden).

**8.2 Ayrıcalıklı Erişim Hakları**

Ayrıcalıklı erişim haklarının tahsisi ve kullanımı sınırlandırılmakta ve yönetilmektedir.

Ayrıcalıklı erişim haklarının tahsisi, erişim kontrolüne ilişkin konuya özel proses uygun olarak bir yetkilendirme süreci aracılığıyla kontrol edilmeltedir. Aşağıdakiler dikkate alınmaktadır.

a) her sistem veya işlem için ayrıcalıklı erişim haklarına ihtiyaç duyan kullanıcıların belirlenmesi (örn. işletim sistemleri, veritabanı yönetim sistemleri ve uygulamaları),

b) erişim kontrolüne ilişkin konuya özgü politikaya uygun olarak ve olay bazında kullanıcılara ayrıcalıklı erişim haklarının tahsis edilmesi, (yani, yalnızca ayrıcalıklı erişim gerektiren faaliyetleri yürütmek için gerekli yetkinliğe sahip bireylere ve fonksiyonel rolleri için asgari gereksinime göre),

c) bir yetkilendirme sürecini sürdürmek (yani, ayrıcalıklı erişim haklarını kimin onaylayabileceğini belirlemek veya yetkilendirme süreci tamamlanana kadar ayrıcalıklı erişim haklarını vermemek) ve tahsis edilen tüm ayrıcalıkların kaydını tutmak,

d) ayrıcalıklı erişim haklarının sona ermesi için gereksinimlerin tanımlanması ve uygulanması,

e) kullanıcıların ayrıcalıklı erişim haklarının farkında olmalarını ve ayrıcalıklı erişim modunda olmalarını sağlamak için önlemler almak. Muhtemel önlemler arasında belirli kullanıcı kimliklerinin, kullanıcı arabirimi ayarlarının ve hatta belirli ekipmanların kullanılması yer alır,

f) ayrıcalıklı erişim hakları için kimlik doğrulama gereksinimleri, normal erişim hakları gereksinimlerinden daha yüksek olabilir. Ayrıcalıklı erişim haklarıyla çalışmadan önce yeniden kimlik doğrulama veya kimlik doğrulama adım adım gerekli olabilir,

g) düzenli olarak ve herhangi bir organizasyonel değişiklikten sonra, görevlerinin, rollerinin, sorumluluklarının ve yetkinliklerinin onları ayrıcalıklı erişim haklarıyla çalışmaya uygun kılıp kılmadığını doğrulamak için ayrıcalıklı erişim haklarıyla çalışan kullanıcıları gözden geçirmek,

h) sistemlerin yapılandırma yeteneklerine bağlı olarak genel yönetim kullanıcı kimliklerinin (“root” gibi) kullanılmasını önlemek için özel kurallar oluşturmak. Bu tür kimliklerin kimlik doğrulama bilgilerinin yönetilmesi ve korunması,

i) ayrıcalıklı erişim haklarını kalıcı olarak vermek yerine, yalnızca onaylanmış değişiklikleri veya etkinlikleri (örneğin bakım etkinlikleri veya bazı kritik değişiklikler) uygulamak için gerekli zaman penceresi için geçici ayrıcalıklı erişim vermek. Bu genellikle cam kırma prosedürü olarak adlandırılır ve genellikle ayrıcalıklı erişim yönetimi teknolojileri tarafından otomatikleştirilir,

j) denetim amacıyla sistemlere tüm ayrıcalıklı erişimlerin günlüğe kaydedilmesi,

k) ayrıcalıklı erişim haklarına sahip kimlikleri birden çok kişiyle paylaşmamak veya birbirine bağlamamak, her kişiye ayrı bir kimlik atamak, bu da belirli ayrıcalıklı erişim haklarının atanmasına olanak tanır. Ayrıcalıklı erişim haklarının yönetimini basitleştirmek için kimlikler gruplandırılabilir (örn. bir yönetici grubu tanımlanarak),

l) günlük genel görevler için değil, yalnızca ayrıcalıklı erişim haklarına sahip kimliklerin kullanılması [ör. e-posta kontrolü, web'e erişim (kullanıcıların bu etkinlikler için ayrı bir normal ağ kimliği olmalıdır)].

**8.3 Bilgi Erişim Kısıtlaması**

Bilgilere ve diğer ilgili varlıklara erişim, erişim kontrolü konusunda oluşturulmuş konuya özgü proses ile uygun olarak kısıtlanmaktadır.

Bilgilere ve diğer ilgili varlıklara erişim, konuya özel oluşturulmuş politikalara uygun olarak kısıtlanmaktadır. Erişim kısıtlama gereksinimlerini desteklemek için aşağıdakiler dikkate alınmaktadır.

a) hassas bilgilere bilinmeyen kullanıcı kimlikleri tarafından veya anonim olarak erişime izin verilmemesi. Genel veya anonim erişim, yalnızca herhangi bir hassas bilgi içermeyen depolama konumlarına verilmelidir,

b) sistemlerdeki, uygulamalardaki ve hizmetlerdeki bilgilere erişimi kontrol etmek için yapılandırma mekanizmaları sağlamak,

c) belirli bir kullanıcı tarafından hangi verilere erişilebileceğinin kontrol edilmesi,

d) okuma, yazma, silme ve yürütme gibi hangi kimliklerin veya kimlik gruplarının hangi erişime sahip olduğunu kontrol etme,

e) hassas uygulamaların, uygulama verilerinin veya sistemlerin izolasyonu için fiziksel veya mantıksal erişim kontrolleri sağlamak.

Ayrıca, kurumumuz için yüksek değere sahip hassas bilgileri korumaya yönelik dinamik erişim yönetimi teknikleri ve süreçleri, kurumumuz aşağıdaki durumlarda dikkate alınmaktadır.

a) bu tür bilgilere kimin hangi dönemde ve ne şekilde erişebileceği konusunda ayrıntılı kontrole ihtiyaç duyar,

b) bu tür bilgileri kurumumuz dışındaki kişilerle paylaşmak ve bu bilgilere kimlerin erişebileceğini kontrol etmek istiyorsa,

c) bu tür bilgilerin kullanımını ve dağıtımını dinamik olarak, gerçek zamanlı olarak yönetmek istiyorsa,

d) bu tür bilgileri yetkisiz değişikliklere, kopyalamaya ve dağıtıma (baskı dahil) karşı korumak istiyorsa,

e) bilgilerin kullanımını izlemek istiyor,

e) gelecekte bir soruşturmanın gerekli olması durumunda bu tür bilgilerde meydana gelen değişiklikleri kaydetmek istiyor.

Dinamik erişim yönetimi teknikleri, bilgileri yaşam döngüsü boyunca korumaktadır. (örn. oluşturulması, işlenmesi, depolanması, iletilmesi ve imha edilmesi),

a) Aşağıdakileri göz önünde bulundurarak belirli kullanım durumlarına dayalı olarak dinamik erişimin yönetimine ilişkin kurallar oluşturmak,

 1) kimlik, cihaz, konum veya uygulamaya dayalı olarak erişim izinleri verilmesi;
 2) dinamik erişim yönetimi teknikleriyle hangi bilgilerin korunması gerektiğini belirlemek için sınıflandırma şemasından yararlanmak,

b) operasyonel, izleme ve raporlama süreçlerinin oluşturulması ve teknik altyapının desteklenmesi.

**8.4 Kaynak Koduna Erişim**

Kaynak koduna, geliştirme araçlarına ve yazılım kütüphanelerine okuma ve yazma erişimi uygun şekilde yönetilmektedir.

Kaynak koduna ve ilgili öğelere (tasarımlar, spesifikasyonlar, doğrulama planları ve doğrulama planları gibi) ve geliştirme araçlarına (örn. derleyiciler, oluşturucular, entegrasyon araçları, test platformları ve ortamlar) erişim sıkı bir şekilde kontrol edilmektedir.

Kaynak kodu için bu, tercihen kaynak kodu yönetim sisteminde, bu tür bir kodun merkezi depolanmasını kontrol ederek elde edilebilir.

Kaynak koduna okuma erişimi ve yazma erişimi, personelin rolüne göre farklılık gösterebilir. Örneğin, kaynak koduna okuma erişimi kurumumuz içinde geniş ölçüde sağlanabilir, ancak kaynak koduna yazma erişimi yalnızca ayrıcalıklı personele veya atanmış sahiplere sağlanır. Kod bileşenlerinin bir kurumumuz içindeki birkaç geliştirici tarafından kullanıldığı durumlarda, merkezi bir kod deposuna okuma erişimi uygulanmaktadır. Ayrıca, bir kurumumuz içinde açık kaynak kodu veya üçüncü taraf kod bileşenleri kullanılıyorsa, bu tür harici kod havuzlarına okuma erişimi geniş ölçüde sağlanabilir. Ancak, yazma erişimi yine de kısıtlanmaktadır.

Program kaynak kodunun yayınlanması amaçlanıyorsa, bütünlüğü konusunda güvence sağlamak için ek kontroller (örn. dijital imza) düşünülmektedir.

**8.5 Güvenli Kimlik Doğrulama**

Güvenli kimlik doğrulama teknolojileri ve prosesleri, bilgi erişim kısıtlamalarına ve erişim kontrolüne ilişkin konuya özgü prosese dayalı olarak uygulanmaktadır.

Bir kullanıcının, yazılımın, mesajların ve diğer varlıkların iddia edilen kimliğini doğrulamak için uygun bir kimlik doğrulama tekniği seçilmektedir.

Kimlik doğrulamanın gücü, erişilecek bilginin sınıflandırılmasına uygun olmaktadır. Güçlü kimlik doğrulama ve kimlik doğrulamanın gerekli olduğu durumlarda, dijital sertifikalar, akıllı kartlar, belirteçler veya biyometrik araçlar gibi parolalara alternatif kimlik doğrulama yöntemleri kullanılmaktadır.

Bir sistem veya uygulamada oturum açma prosesi, yetkisiz erişim riskini en aza indirecek şekilde tasarlanmaktadır. Oturum açma prosesleri ve teknolojileri aşağıdakiler dikkate alınarak uygulanmaktadır.

a) yetkisiz bir kullanıcıya gereksiz yardım sağlamaktan kaçınmak için oturum açma işlemi başarıyla tamamlanana kadar hassas sistem veya uygulama bilgilerini görüntülememek,

b) sisteme veya uygulamaya veya hizmete yalnızca yetkili kullanıcılar tarafından erişilmesi gerektiğine dair uyarı veren genel bir bildirimin görüntülenmesi,

c) oturum açma prosesesi sırasında yetkisiz bir kullanıcıya yardımcı olacak yardım mesajları vermemek (örn. bir hata durumu ortaya çıkarsa, sistem verilerin hangi kısmının doğru veya yanlış olduğunu göstermemelidir),

d) oturum açma bilgilerinin yalnızca tüm giriş verilerinin tamamlanması üzerine doğrulanması,

e) kullanıcı adları ve parolalar üzerinde kaba kuvvet oturum açma girişimlerine karşı koruma [örneğin, bilgisayarları ve insanları birbirinden ayırmak için tamamen otomatik genel Turing testi kullanma (CAPTCHA), önceden tanımlanmış sayıda başarısız denemeden sonra parolanın sıfırlanmasını gerektirme veya maksimum sayıda hatadan sonra kullanıcıyı engelleme ],

f) başarısız ve başarılı girişimlerin günlüğe kaydedilmesi,

g) oturum açma kontrollerinin olası bir şekilde ihlal edilmeye çalışıldığı veya başarılı bir şekilde ihlal edildiği tespit edilirse bir güvenlik olayının yükseltilmesi (örneğin, belirli sayıda yanlış parola girişimine ulaşıldığında kullanıcıya ve kurumumuzun sistem yöneticilerine bir uyarı gönderilmesi),

h) başarılı bir oturum açma işleminin tamamlanmasının ardından aşağıdaki bilgileri ayrı bir kanalda görüntüleme veya gönderme,

 1) önceki başarılı oturum açmanın tarih ve saati,

 2) son başarılı oturum açmadan bu yana başarısız oturum açma girişimlerinin ayrıntıları,

i) girilirken şifrenin düz metin olarak görüntülenmemesi; bazı durumlarda, kullanıcının oturum açmasını kolaylaştırmak için (örn. erişilebilirlik nedenleriyle veya tekrarlanan hatalar nedeniyle kullanıcıların engellenmesini önlemek için) bu işlevin devre dışı bırakılması gerekebilir,

j) bir ağ izleyici"sniffer" programı tarafından yakalanmamak için parolaları bir ağ üzerinden açık metin olarak iletmemek,

k) özellikle kurumumuzun güvenlik yönetimi dışındaki halka açık veya harici alanlar veya kullanıcı uç nokta cihazları gibi yüksek riskli konumlarda, etkin olmayan oturumları belirli bir etkinlik dışı kalma süresinden sonra sonlandırmak,

l) yüksek riskli uygulamalar için ek güvenlik sağlamak ve yetkisiz erişim fırsat penceresini azaltmak için bağlantı süresi sürelerini kısıtlamak.

**8.6 Kapasite Yönetimi**

Kaynakların kullanımı izlenmekte ve mevcut ve beklenen kapasite gereklilikleri doğrultusunda ayarlanmaktadır.

Bilgi işleme tesisleri, insan kaynakları, ofisler ve diğer tesisler için kapasite gereksinimleri, ilgili sistem ve süreçlerin iş açısından kritikliği dikkate alınarak belirlenmektedir.

Sistemlerin kullanılabilirliğini ve verimliliğini sağlamak ve gerektiğinde iyileştirmek için sistem ayarlama ve izleme uygulanmaktadır.

Kurumumuz, en yüksek performans gereksinimlerini karşılamak için yeterli sistem kapasitesinin mevcut olduğunu doğrulamak için sistem ve hizmetlerin stres testlerini gerçekleştirmektedir.

Sorunları zamanında belirtmek için dedektif kontrolleri devreye alınmaktadır.

Gelecekteki kapasite gereksinimlerine ilişkin projeksiyonlar, yeni iş ve sistem gereksinimleri ile kurumumuzun bilgi işleme yeteneklerindeki mevcut ve öngörülen eğilimleri dikkate almaktadır.

Uzun tedarik süreleri veya yüksek maliyetleri olan kaynaklara özel dikkat gösterilmektedir. Bu nedenle yöneticiler, hizmet veya ürün sahipleri, kilit sistem kaynaklarının kullanımını izlemektedir.

Yöneticiler, sistem güvenliğine veya hizmetlerine tehdit oluşturabilecek potansiyel kaynak sınırlamalarını ve kilit personele bağımlılığı belirlemek ve bunlardan kaçınmak ve uygun eylemi planlamak için kapasite bilgilerini kullanmaktadır.

**8.7 Kötü Amaçlı Yazılıma Karşı Koruma**

Kötü amaçlı yazılıma karşı koruma uygulanarak ve uygun kullanıcı farkındalığı ile desteklenmektedir.

Kötü amaçlı yazılıma karşı koruma, kötü amaçlı yazılım algılama ve onarım yazılımına, bilgi güvenliği farkındalığına, uygun sistem erişimine ve değişiklik yönetimi kontrollerine dayanmaktadır. Tek başına kötü amaçlı yazılım tespit ve onarım yazılımının kullanılması genellikle yeterli değildir.

Aşağıdaki kurallar dikkate alınmaktadır.

a) yetkisiz yazılımların kullanımını engelleyen veya tespit eden kurallar ve kontroller uygulamak [örneğin, izin verilen uygulamalar listesi (yani, izin verilen uygulamalar sağlayan bir liste kullanılmaktadır),

b) bilinen veya şüphelenilen kötü amaçlı web sitelerinin kullanımını önleyen veya tespit eden kontrollerin uygulanması (örn. engellenenler listesi),

c) kötü amaçlı yazılım tarafından yararlanılabilecek güvenlik açıklarının azaltılması [örneğin, teknik güvenlik açığı yönetimi aracılığıyla),

d) özellikle kritik iş süreçlerini destekleyen sistemler için yazılım ve sistemlerin veri içeriğinin düzenli olarak otomatik olarak doğrulanması; onaylanmamış dosyaların veya yetkisiz değişikliklerin varlığını araştırmak,

e) harici ağlardan veya bu ağlar aracılığıyla veya başka herhangi bir ortamdan dosya ve yazılım alınmasıyla ilişkili risklere karşı koruyucu önlemler oluşturmak,

f) bilgisayarları ve elektronik depolama ortamını taramak için kötü amaçlı yazılım algılama ve onarım yazılımı yüklemek ve düzenli olarak güncellemek.

*Aşağıdakileri içeren düzenli taramalar yapmak:*

 1) ağlar üzerinden veya herhangi bir elektronik depolama ortamı yoluyla alınan herhangi bir veriyi kullanımdan önce kötü amaçlı yazılımlara karşı taramak,

 2) kullanmadan önce e-posta ve anlık mesajlaşma eklerini ve indirmelerini kötü amaçlı yazılımlara karşı tarama. Bu taramanın farklı yerlerde (örneğin e-posta sunucularında, masaüstü bilgisayarlarda) yapılması ve kurumumuzun ağına girildiğinde,

 3) web sayfalarını erişildiğinde kötü amaçlı yazılımlara karşı taramak,

g) risk değerlendirmesi sonuçlarına dayalı olarak kötü amaçlı yazılım algılama ve onarım araçlarının yerleşimini ve yapılandırmasını belirlemek ve şunları göz önünde bulundurulmaktadır,

 1) en etkili olacakları derinlemesine savunma ilkeleri oluşturmak. Örneğin bu, bir ağ geçidinde (e-posta, dosya aktarımı ve web gibi çeşitli uygulama protokollerinde) ve ayrıca kullanıcı uç nokta cihazlarında ve sunucularında kötü amaçlı yazılım tespitine yol açabilir,

 2) saldırganların kötü amaçlı yazılım dağıtmak için kaçamak teknikleri (örneğin, şifrelenmiş dosyaların kullanımı) veya kötü amaçlı yazılımı iletmek için şifreleme protokollerinin kullanımı,

h) bakım ve acil durum prosesleri sırasında kötü amaçlı yazılımlara karşı normal kontrolleri atlayabilen kötü amaçlı yazılımların girişine karşı koruma sağlamaya özen gösterilmesi,

i) istisna onay yetkilileri, belgelenmiş gerekçe ve inceleme tarihi dahil olmak üzere, kötü amaçlı yazılıma karşı önlemlerin bazılarını veya tümünü geçici veya kalıcı olarak devre dışı bırakmak için bir süreç uygulamak.

j) kötü amaçlı yazılım saldırılarından kurtarma için uygun iş sürekliliği planlarının hazırlanması,

k) yıkıcı sonuçların ortaya çıkabileceği ortamların izole edilmesi,

l) kullanımlarına ilişkin eğitim, kötü amaçlı yazılım saldırılarını raporlama ve kurtarma dahil olmak üzere, sistemlerde kötü amaçlı yazılımlara karşı korumayla başa çıkmak için prosesler ve sorumlulukların tanımlanması,

m) tüm kullanıcılara, kötü amaçlı yazılım bulaşmış e-postaların, dosyaların veya programların [n) ve o)'da toplanan bilgilerin alınması, gönderilmesi veya yüklenmesinin nasıl tanımlanacağı ve potansiyel olarak azaltılacağı konusunda farkındalık veya eğitim sağlamak (farkındalık ve eğitim sağlamak için düzenli olarak yapılır),

n) posta listelerine abone olmak veya ilgili web sitelerini incelemek gibi yeni kötü amaçlı yazılımlar hakkında düzenli olarak bilgi toplamak için prosesler uygulamak,

o) uyarı bültenleri gibi kötü amaçlı yazılımla ilgili bilgilerin nitelikli ve saygın kaynaklardan (örneğin, güvenilir internet siteleri veya kötü amaçlı yazılım tespit yazılımı tedarikçileri) geldiğini ve doğru ve bilgilendirici olduğunu doğrulamak.

**8.8 Teknik Açıklıkların Yönetimi**

Kullanımda olan bilgi sistemlerinin teknik açıklıkları hakkında bilgi edinilmeli, kurumumuzun bu açıklara maruz kalma durumu değerlendirilmeli ve uygun önlemler alınmaktadır.

Etkin teknik güvenlik açığı yönetimi için bir ön koşul olarak doğru bir varlık envanteri kullanılmaktadır. Envanter, yazılım satıcısını, yazılım adını, sürüm numaralarını, mevcut dağıtım durumunu (örneğin, hangi yazılımların hangi sistemlere yüklendiğini) ve kurumumuz içinde yazılımdan sorumlu kişi(ler)i içermektedir.

Tüm yetkili yazılımlar için en güncel onaylı yamaların ve uygulama güncellemelerinin yüklenmesini sağlamak için bir yazılım güncelleme yönetim süreci uygulanmaktadır. Değişiklik gerekliyse, orijinal yazılım korunmalı ve değişiklikler belirlenmiş bir kopyaya uygulanmaktadır. Gerekirse gelecekteki yazılım yükseltmelerinde yeniden uygulanabilmeleri için tüm değişiklikler tam olarak test edilmekte ve belgelenmektedir. Gerekirse, değişiklikler bağımsız bir değerlendirme kuruluşu tarafından test edilmekte ve doğrulanmaktadır.

Teknik güvenlik açığı yönetiminde gerçekleştirilen tüm adımlar için bir denetim günlüğü tutulmaktadır.

Teknik zafiyet yönetimi süreci, etkinliğini ve verimliliğini sağlamak için düzenli olarak izlenmeli ve değerlendirilmektedir.

Kurumumuz, üçüncü taraf bir bulut hizmeti sağlayıcısı tarafından sağlanan bir bulut hizmeti kullandığı durumlarda, bulut hizmeti sağlayıcısı kaynaklarının teknik güvenlik açığı yönetimi, bulut hizmeti sağlayıcısı tarafından sağlanmaktadır. Bulut hizmeti sağlayıcısının teknik güvenlik açığı yönetimine ilişkin sorumlulukları, bulut hizmeti sözleşmesinin bir parçası olarak ve bu, bulut hizmeti sağlayıcısının teknik güvenlik açıklarıyla ilgili eylemlerini raporlama süreçlerini içermektedir. Bulut hizmetleri için, bulut hizmeti sağlayıcısı ve bulut hizmeti müşterisi için ilgili sorumluluklar bulunuyorsa Örneğin, bulut hizmeti müşterisi, bulut hizmetleri için kullanılan kendi varlıklarının güvenlik açığı yönetiminden sorumludur.

**8.9 Konfigürasyon (yapılandırma) Yönetimi**

Donanım, yazılım, hizmetler ve ağların güvenlik yapılandırmaları da dahil olmak üzere yapılandırmaları oluşturulmakta, doküman haline getirreek, uygulama, izleme ve gözden geçirme prosesleri uygulanmaktadır.

Tüm konfigürasyon değişikliklerinin tatmin edici kontrolünü sağlamak için roller, sorumluluklar ve prosesler mevcut olmaktadır.

Donanım, yazılım, hizmetler ve ağların güvenli yapılandırması için standart şablonlar oluştururken aşağıdakiler dikkate alınmaktadır.

a) ayrıcalıklı veya yönetici düzeyinde erişim haklarına sahip kimliklerin sayısını en aza indirmek,

b) gereksiz, kullanılmayan veya güvensiz kimlikleri devre dışı bırakmak,

c) gereksiz işlevleri ve hizmetleri devre dışı bırakmak veya kısıtlamak,

d) güçlü yardımcı programlara ve ana bilgisayar parametre ayarlarına erişimin kısıtlanması,

e) saatleri senkronize etmek,

f) kurulumdan hemen sonra varsayılan parolalar gibi satıcı varsayılan kimlik doğrulama bilgilerini değiştirmek ve varsayılan güvenlikle ilgili diğer önemli parametreleri gözden geçirmek,
g) önceden belirlenmiş bir hareketsizlik süresinden sonra bilgi işlem cihazlarının oturumunu otomatik olarak kapatan zaman aşımı olanaklarını kullanmak,

h) lisans gereksinimlerinin karşılandığının doğrulanması.

Konfigürasyonlar, kapsamlı bir sistem yönetim araçları seti (örn. bakım yardımcı programları, uzaktan destek, kurumsal yönetim araçları, yedekleme ve geri yükleme yazılımı) ile izlenerek ve konfigürasyon ayarlarını doğrulamak, parola güçlerini değerlendirmek ve gerçekleştirilen faaliyetleri değerlendirmek için düzenli olarak gözden geçirilmektedir. Gerçek konfigürasyonlar, tanımlanan hedef şablonlarla karşılaştırılabilir. Herhangi bir sapma, tanımlanan hedef konfigürasyonun otomatik olarak uygulanmasıyla veya sapmanın manuel analizi ve ardından düzeltici eylemlerle ele alınmaktadır.

**8.10 Bilgi Silme**

Bilgi sistemlerinde, cihazlarda veya diğer herhangi bir depolama ortamında saklanan bilgiler, artık gerekli olmadığında silinmektedir.

Hassas bilgiler, istenmeyen ifşa riskini azaltmak için gerekenden daha uzun süre saklanmamaktadır.

Sistemler, uygulamalar ve hizmetler hakkındaki bilgileri silerken aşağıdakiler dikkate alınmamaktadır.

a) iş gerekliliklerine uygun olarak ve ilgili yasa ve yönetmelikleri dikkate alarak bir silme yöntemi (örn. elektronik üzerine yazma veya kriptografik silme) seçmek;

b) silme sonuçlarının kanıt olarak kaydedilmesi;

c) bilgi silme hizmet sağlayıcılarını kullanırken, onlardan bilgi silme kanıtı elde etmek.

Üçüncü tarafların kurumumuzun bilgilerini kendi adına sakladığı durumlarda, kurumumuz, bu tür hizmetlerin sona ermesi sırasında ve sonrasında bunu uygulamak için üçüncü taraf anlaşmalarına bilgi silmeye ilişkin gereklilikleri dahil etmeyi düşünmektedir.

Bulut hizmetlerinin kullanıldığı durumlarda, kurumumuz, bulut hizmet sağlayıcısı tarafından sağlanan silme yönteminin kabul edilebilir olup olmadığını doğrulanarak ve böyleyse kurumumuz bunu kullanmakta veya bulut hizmet sağlayıcısından bilgileri silmesini talep etmektedir. Bu silme işlemleri, mümkün olduğunda ve uygulanabilir olduğunda, konuya özel politikalara uygun olarak otomatikleştirilmektedir. Silinen bilgilerin hassasiyetine bağlı olarak, günlükler bu silme işlemlerinin gerçekleştiğini izleyebilir veya doğrulanmaktadır.

Ekipman satıcılara geri gönderilirken hassas bilgilerin kasıtsız olarak açığa çıkmasını önlemek için, ekipman kurumumuzun tesislerinden ayrılmadan önce yardımcı depolar (örn. sabit disk sürücüleri) ve bellek kaldırılarak hassas bilgiler korunmaktadır.

Bazı cihazların (örn. akıllı telefonlar) güvenli bir şekilde silinmesinin ancak imha yoluyla veya bu cihazlara gömülü işlevlerin kullanılmasıyla (örn. “fabrika ayarlarını geri yükleme”) gerçekleştirilebileceği göz önüne alındığında, kurumumuz tarafından işlenen bilgilerin sınıflandırılmasına göre uygun yöntem seçilmektedir. bu tür cihazlar.

Depolama cihazını fiziksel olarak imha etmek ve aynı anda içerdiği bilgileri silmek için “**Ekipmanın Güvenli Bir Şekilde Yok Edilmesi veya Tekrar Kullanılmas”** maddesinde açıklanan kontrol önlemleri uygulanmaktadır. Bilgilerin silinmesine ilişkin resmi bir kayıt, olası bir bilgi sızıntısı olayının nedenini analiz ederken kullanılmaktadır.

**8.11 Veri Maskeleme**

Veri maskeleme, ilgili mevzuat dikkate alınarak, kurumumuzun konuya özgü erişim kontrolü politikası ve ilgili diğer konuya özgü politikalara ve iş gerekliliklerine uygun olarak kullanılmaktadır.

Takma ad verme veya anonimleştirme teknikleri, PII'yi gizleyebilir, PII asıllarının veya diğer hassas bilgilerin gerçek kimliğini gizleyebilir ve PII ile PII asıl kimliğinin kimliği veya diğer hassas bilgiler arasındaki bağlantıyı kesebilir.

Takma ad verme veya anonimleştirme teknikleri kullanılırken, verilerin yeterince takma ad veya anonim hale getirildiği doğrulanmaktadır. Veri anonimleştirmenin etkili olabilmesi için hassas bilgilerin tüm unsurları göz önünde bulundurulmaktadır. Örnek olarak, doğru değerlendirilmediği takdirde, bir kişiyi doğrudan tanımlayabilecek veriler anonimleştirilse bile, kişinin dolaylı olarak kimliğinin tespit edilmesini sağlayan başka verilerin varlığı ile bir kişinin kimliği belirlenebilir.

Kurumumuz, Veri maskeleme için ek teknikler şunları içerir:

a) şifreleme (yetkili kullanıcıların bir anahtara sahip olmasını gerektirir),

b) karakterleri geçersiz kılmak veya silmek (yetkisiz kullanıcıların tam mesajları görmesini engellemek),

c) değişen sayılar ve tarihler,

d) ikame (hassas verileri gizlemek için bir değeri diğeriyle değiştirmek),

e) değerleri karma değerleri ile değiştirmek.

Veri maskeleme teknikleri uygulanırken aşağıdakiler dikkate alınmaktadır.

a) tüm kullanıcılara tüm verilere erişim hakkı vermemek, dolayısıyla sorguları ve maskeleri kullanıcıya yalnızca gerekli minimum verileri gösterecek şekilde tasarlamak,

b) bir veri kümesinden bazı kayıtlar için bazı verilerin kullanıcı tarafından görülmemesi gereken durumlar vardır, bu durumda, verilerin karartılması için bir mekanizmanın tasarlanması ve uygulanması (örn. bir hasta, acil durumlarda bile hastane personelinin tüm kayıtlarını görmesini istemiyorsa, hastane personeline kısmen gizlenmiş veriler sunulur ve verilere, uygun tedavi için yararlı bilgiler içeriyorsa, yalnızca belirli rollere sahip personel tarafından erişilebilir),

c) veriler karartıldığında, PII ilkesine, verilerin gizlenip gizlenmediğini kullanıcıların görmemesini isteme olanağı verir (gizlemenin karartılması; bu, sağlık tesislerinde, örneğin hasta, personelin bu hassas bilgileri görmesini istemiyorsa kullanılır; gebelikler veya kan tahlillerinin sonuçları gizlendiği için);

d) herhangi bir yasal veya düzenleyici gereklilik (örneğin, işleme veya depolama sırasında ödeme kartı bilgilerinin maskelenmesini zorunlu kılmak).

Veri maskeleme, takma adlaştırma veya anonimleştirme kullanılırken aşağıdakiler dikkate alınmaktadır.

a) işlenen verilerin kullanımına göre veri maskeleme, takma adlaştırma veya anonimleştirmenin güç düzeyi,

b) işlenen verilere erişim kontrolleri,

c) işlenen verilerin kullanımına ilişkin anlaşmalar veya kısıtlamalar,

d) PII esasını belirlemek için işlenmiş verilerin diğer bilgilerle harmanlanmasını yasaklamak,

e) işlenen verilerin sağlanması ve alınmasının takibi.

**8.12 Veri Sızıntısı Önleme**

Hassas bilgileri işleyen, depolayan veya ileten sistemlere, ağlara ve diğer tüm cihazlara veri sızıntısı önleme önlemleri uygulanmaktadır.

Kurumumuz, veri sızıntısı riskini azaltmak için aşağıdakileri dikkate almaktadır.

a) bilgileri sızıntıya karşı korumak için tanımlama ve sınıflandırma (örn. kişisel bilgiler, fiyatlandırma modelleri ve ürün tasarımları),

b) veri sızıntısı kanallarının izlenmesi (örn. e-posta, dosya aktarımları, mobil cihazlar ve taşınabilir depolama cihazları),

c) bilgilerin sızmasını önlemek için hareket etmek (örneğin, hassas bilgiler içeren karantina e-postaları).

Veri sızıntısı önleme araçları şu amaçlarla kullanılmaktadır.

a) yetkisiz ifşa riski taşıyan hassas bilgileri (örneğin, bir kullanıcının sistemindeki yapılandırılmamış verilerde) tanımlayın ve izleyin,

b) hassas bilgilerin ifşasını tespit etmek (örneğin, bilgiler güvenilmeyen üçüncü taraf bulut hizmetlerine yüklendiğinde veya e-posta yoluyla gönderildiğinde),

c) hassas bilgileri ifşa eden kullanıcı eylemlerini veya ağ aktarımlarını bloke edin (örn. veritabanı girişlerinin bir elektronik tabloya kopyalanmasını önleme).

Kurumumuz, bir kullanıcının kurumumuz dışındaki hizmetlere, cihazlara ve depolama ortamlarına veri kopyalama ve yapıştırma ya da yükleme becerisini kısıtlamanın gerekli olup olmadığını belirlemektedir. Durum buysa kurumumuz, veri sızıntısını önleme araçları veya kullanıcıların uzaktan tutulan verileri görüntülemesine ve değiştirmesine izin veren ancak kurumumuzun kontrolü dışında kopyalama ve yapıştırmayı önleyen mevcut araçların yapılandırması gibi teknolojileri uygulamaktadır.

Verilerin dışa aktarılması gerekiyorsa, veri sahibinin dışa aktarımı onaylamasına ve kullanıcıları eylemlerinden sorumlu tutmasına izin verilmektedir. Ekranın ekran görüntülerinin veya fotoğraflarının alınması, kullanım, eğitim ve denetim hüküm ve koşulları ile ele alınmaktadır.

Verilerin yedeklendiği durumlarda, şifreleme, erişim kontrolü ve yedeği tutan depolama ortamının fiziksel olarak korunması gibi önlemler kullanılarak hassas bilgilerin korunmasını sağlamak için özen gösterilmektedir.

**8.13 Bilgi Yedekleme**

Kurumumuz da veri saklama ve bilgi güvenliği gereksinimlerini ele almak amacıyla yedekleme süreci bulunmaktadır.

Bilgilerin, yazılımların ve sistemlerin yedek kopyaları muhafaza edilmekte ve yedekleme sürecine ve yapısına uygun bir şekilde test edilmektedir.

Bir olay veya depolama ortamı arızası veya kaybının ardından temel bilgilerin ve yazılımın kurtarılabilmesini sağlamak amacıyla yeterli yedekleme olanakları sağlamaktadır.

Yedeklemeye ilişkin süreci ele almak amacıyla kurumumuzun bilgileri, yazılımları ve sistemleri nasıl yedekleme yapacağına ilişkin planlar dahilinde uygulanmaktadır.

Bireysel sistemler ve hizmetler için yedekleme önlemleri, bunların olay müdahalesi ve iş sürekliliği planlarının hedeflerini karşıladıklarından emin olmak için düzenli olarak test edilmektedir. Bu, restorasyon proseslerinin bir testi ile birleştirilmekte ve iş sürekliliği planının gerektirdiği restorasyon süresine göre kontrol edilmektedir. Kritik sistemler ve hizmetler söz konusu olduğunda, yedekleme önlemleri, bir felaket durumunda tüm sistemi kurtarmak için gerekli tüm sistem bilgilerini, uygulamaları ve verileri kapsamaktadır.

Kurumumuz, bir bulut hizmeti kullanıldığında, bulut hizmeti ortamındaki kurum bilgilerinin, uygulamalarının ve sistemlerinin yedek kopyalarını almaktadır. Kurumumuz, bulut hizmetinin bir parçası olarak sağlanan bilgi yedekleme hizmetini kullanırken yedekleme gereksinimlerinin karşılanıp karşılanmadığını ve nasıl karşılandığını belirlemektedir.

Temel iş bilgilerinin saklanma süresi, arşiv kopyalarının saklanmasına yönelik her türlü gereklilik dikkate alınarak belirlenmektedir. Kurumumuz, yedekleme için kullanılan depolama ortamlarındaki bilgilerin saklama süresi sona erdikten sonra imha etme sürecini mevzuat ve yasal düzenlemeleri dikkate alarak yapmaktadır.

**8.14 Bilgi İşleme Tesislerinin Yedek Fazlalığı**

Bilgi işleme imkanlarında, erişilebilirlik gerekliliklerini karşılamak için yeterli miktarda yedekleme sağlanmaktadır.

Kurumumuz, iş hizmetleri ve bilgi sistemlerinin mevcudiyeti için gereklilikleri tanımlamaktadır. Kurumumuz, bu gereklilikleri karşılamak için sistem mimarisini uygun fazlalıkla tasarlamakta ve uygulamaktadır.

Fazlalık, bilgi işleme tesislerinin kısmen veya tamamen kopyalanmasıyla sağlanabilir (yani yedek bileşenler veya her şeyden ikişer tane olması). kurumumuz, gereksiz bileşenlerin ve işleme tesislerinin aktivasyonu için prosedürler planlamalı ve uygulamaktadır. Prosesler, gereksiz bileşenlerin ve işleme faaliyetlerinin her zaman etkinleştirilip etkinleştirilmediğini veya acil durumlarda otomatik veya manuel olarak etkinleştirilip etkinleştirilmediğini belirlemektadir. Yedek bileşenler ve bilgi işleme tesisleri, birincil olanlarla aynı güvenlik seviyesini sağlamaktadır.

Bilgi işleme tesislerindeki herhangi bir arızaya karşı kurumumuzu uyaracak, planlanan prosedürün yürütülmesini sağlayacak ve bilgi işleme tesisleri tamir edilirken veya değiştirilirken sürekli kullanılabilirliğe izin verecek mekanizmalar yürürlükte olmaktadır.

Kurumumuz, fazlalık sistemleri uygularken aşağıdakileri dikkate almalıdır:

a) internet servis sağlayıcıları gibi ağ ve kritik bilgi işleme tesislerinin iki veya daha fazla tedarikçisiyle sözleşme yapmak,

b) yedekli ağlar kullanmak,

c) ikizlenmiş sistemlerle coğrafi olarak ayrı iki veri merkezi kullanmak,

d) fiziksel olarak yedekli güç kaynakları veya kaynakları kullanmak,

e) yazılım bileşenlerinin birden çok paralel örneğini kullanma ve aralarında otomatik yük dengeleme (aynı veri merkezindeki veya farklı veri merkezlerindeki örnekler arasında),

f) sistemlerde (örn. CPU, sabit diskler, bellekler) veya ağlarda (örn. güvenlik duvarları, yönlendiriciler, anahtarlar) yinelenen bileşenlere sahip olmak

**8.15 Kaydetme(Log tutma)**

Faaliyetleri, istisnaları, hataları ve diğer ilgili olayları kaydeden kayıtlar (loglar) üretilmekte, depolanmakta, korunmakta ve analiz edilmektedir.

Kurumumuz, günlüklerin hangi amaçla oluşturulduğunu, hangi verilerin toplanıp günlüğe kaydedildiğini ve günlük verilerinin korunması ve işlenmesi için günlüğe özgü gereksinimleri belirlemektedir. Bu, günlüğe kaydetme konusunda konuya özgü bir politikada belgelenmektedir. Olay günlükleri, uygun olduğu şekilde, her olay için şunları içermektedir.

a) kullanıcı kimlikleri,

b) sistem faaliyetleri,

c) ilgili olayların tarihleri, saatleri ve detayları (örn. oturum açma ve oturum kapatma),

d) cihaz kimliği, sistem tanımlayıcısı ve konumu,

e) ağ adresleri ve protokoller.

Günlük kaydı için aşağıdaki olaylar dikkate alınmaktadır.

a) başarılı ve reddedilen sistem erişim girişimleri,

b) başarılı ve reddedilen veriler ve diğer kaynak erişim girişimleri,

c) sistem konfigürasyonundaki değişiklikler,

d) ayrıcalıkların kullanımı,

e) yardımcı programların ve uygulamaların kullanımı,

f) önemli veri dosyalarının silinmesi dahil olmak üzere erişilen dosyalar ve erişim türü,

g) erişim kontrol sistemi tarafından verilen alarmlar,

h) anti-virüs sistemleri ve izinsiz giriş tespit sistemleri gibi güvenlik sistemlerinin etkinleştirilmesi ve devre dışı bırakılması,

i) kimliklerin oluşturulması, değiştirilmesi veya silinmesi,

j) uygulamalarda kullanıcılar tarafından gerçekleştirilen işlemler. Bazı durumlarda, uygulamalar bir üçüncü şahıs tarafından sağlanan veya yürütülen bir hizmet veya üründür.

Ayrıcalıklı erişim haklarına sahip olanlar da dahil olmak üzere kullanıcıların kendi etkinliklerine ilişkin günlükleri silme veya devre dışı bırakma izni olmamaktadır. Doğrudan kontrolleri altındaki bilgi işleme tesislerindeki günlükleri potansiyel olarak manipüle edebilirler. Bu nedenle, ayrıcalıklı kullanıcılar için hesap verebilirliği sürdürmek için günlükleri korumak ve gözden geçirmek süreçleri uygulanmaktadır.

Günlüklerin korunması için, şu teknikler kullanılmaktadır.

kriptografik karma, salt eklenen ve salt okunur bir dosyaya kayıt, genel bir şeffaflık dosyasına kayıt vb.

Bazı denetim günlüklerinin, veri saklama gereklilikleri veya kanıt toplama ve saklama gereklilikleri nedeniyle arşivlenmesi gerekliliğine göre süreç işletilmektedir.

Olay günlükleri, hassas veriler ve kişisel olarak tanımlanabilir bilgiler içeriyorsa uygun mahremiyet koruma önlemleri alınmaktadır.

Günlük analizi, uzlaşma göstergelerini temsil edebilecek olağandışı etkinliği veya anormal davranışı belirlemeye yardımcı olmak için bilgi güvenliği olaylarının analizini ve yorumlanmasını kapsamaktadır.

Olayların analizi aşağıdakiler dikkate alınarak yapılmaktadır.

a) analizi yapan uzmanlar için gerekli beceriler,

b) log analizi prosedürünün belirlenmesi,

c) güvenlikle ilgili her olayın gerekli öznitelikleri,

d) önceden belirlenmiş kuralların [örneğin, güvenlik bilgileri ve olay yönetimi (SIEM) veya güvenlik duvarı kuralları ve izinsiz giriş tespit sistemleri (IDS'ler) veya kötü amaçlı yazılım imzaları] kullanılarak tanımlanan istisnalar,

e) anormal etkinlik ve davranışa kıyasla bilinen davranış kalıpları ve standart ağ trafiği [kullanıcı ve varlık davranış analitiği,

f) trend veya örüntü analizinin sonuçları (örn. veri analitiği, büyük veri teknikleri ve özel analiz araçlarının kullanılmasının bir sonucu olarak),

g) mevcut tehdit istihbaratı.

Günlük analizi, anormal davranışı belirlemeye ve analiz etmeye yardımcı olmak için aşağıdakileri içeren belirli izleme faaliyetleriyle desteklenmektedir.

a) korunan kaynaklara [ör. alan adı sistemi (DNS) sunucuları, web portalları ve dosya paylaşımları] erişmeye yönelik başarılı ve başarısız girişimlerin gözden geçirilmesi,

b) botnet komut ve kontrol sunucuları ile ilişkili olanlar gibi kötü amaçlı sunuculara giden ağ bağlantılarını belirlemek için DNS günlüklerini kontrol etme,

c) sistemler ve ağlar içindeki olağan dışı etkinlikler için hizmet sağlayıcılardan alınan kullanım raporlarının (örneğin faturalar veya hizmet raporları) incelenmesi (örneğin, etkinlik kalıplarının gözden geçirilmesi),

d) daha doğru algılama ve olay analizi sağlamak için giriş ve çıkış gibi fiziksel izleme olay günlükleri dahil,

e) verimli ve son derece doğru analiz sağlamak için günlükleri ilişkilendirme.

Şüpheli ve gerçek bilgi güvenliği olayları belirlenmeli (örneğin, kötü amaçlı yazılım bulaşması veya güvenlik duvarlarının araştırılması) ve daha fazla araştırmaya tabi tutulmaktadır.

**UYGULAMA**

Kurum faaliyetlerinde ISO 27001 BGYS performansı ile ilgili izleme ve ölçüm faaliyetleri aşağıda yer alan temel unsurlara dayanır;

Ağlar, sistemler ve uygulamalar anomali içeren davranışlara karşı izlenmeli ve potansiyel bilgi güvenliği ihlal olaylarını değerlendirmek için uygun önlemler alınmaktadır.

İzleme kapsamı ve düzeyi, iş ve bilgi güvenliği gereksinimlerine uygun olarak ve ilgili yasa ve yönetmelikler dikkate alınarak belirlenmektedir. İzleme kayıtları, tanımlanmış saklama süreleri boyunca tutulmaktadır.

Aşağıda belirtilen faaliyetler izleme sistemine dahil edilmişdir:

a) giden ve gelen ağ, sistem ve uygulama trafiği;

b) sistemlere, sunuculara, ağ ekipmanına, izleme sistemine, kritik uygulamalara vb. erişim;

c) kritik veya yönetici düzeyinde sistem ve ağ yapılandırma dosyaları;

d) güvenlik araçlarından günlükler [örn. antivirüs, IDS, saldırı önleme sistemi (IPS), web filtreleri, güvenlik duvarları, veri sızıntısı önleme];

e) sistem ve ağ etkinliği ile ilgili olay günlükleri;

f) yürütülmekte olan kodun sistemde çalışma yetkisinin olup olmadığının ve kurcalanmadığının kontrol edilmesi (örn. ilave istenmeyen kod eklemek için yeniden derleme yoluyla);

g) kaynakların kullanımı (örn. CPU, sabit diskler, bellek, bant genişliği) ve performansları.

Kurumumuzda, normal davranış için bir temel oluşturmakta ve anormallikler için bu temele göre izleme yapmaktadır. Bu temel oluştururken, aşağıdakiler dikkate alınmalıdır:

a) sistemlerin normal ve yoğun dönemlerde kullanımının gözden geçirilmesi;

b) olağan erişim zamanı, erişim yeri, her kullanıcı veya kullanıcı grubu için erişim sıklığı.

İzleme sistemleri, aşağıdakiler gibi anormal davranışları belirlemek için belirlenen temele göre yapılandırılmaktadır:

a) süreçlerin veya uygulamaların planlanmamış sonlandırılması;

b) bilinen kötü amaçlı IP adreslerinden veya ağ etki alanlarından (örn. botnet komut ve kontrol sunucularıyla ilişkili olanlar) kaynaklanan tipik olarak kötü amaçlı yazılım veya trafikle ilişkili etkinlik;

c) bilinen saldırı özellikleri (örn. hizmet reddi ve arabellek taşmaları);
d) olağandışı sistem davranışı (örn. tuş vuruşu kaydı, işlem enjeksiyonu ve standart protokollerin kullanımındaki sapmalar);

e) darboğazlar ve aşırı yükler (örn. ağ kuyruğu, gecikme seviyeleri ve ağ titremesi);

f) sistemlere veya bilgilere yetkisiz erişim (gerçek veya denenmiş);

g) iş uygulamalarının, sistemlerinin ve ağlarının izinsiz taranması;

h) korunan kaynaklara (örn. DNS sunucuları, web portalları ve dosya sistemleri) erişmeye yönelik başarılı ve başarısız girişimler;

i) Beklenen davranışla ilişkili olağandışı kullanıcı ve sistem davranışı.

Bir izleme uygulaması aracılığıyla sürekli izleme kullanılmaktadır. İzleme, kurumsal ihtiyaç ve yeteneklere bağlı olarak gerçek zamanlı veya periyodik aralıklarla yapılmaktadır. İzleme araçları, büyük miktarda veriyi işleme, sürekli değişen tehdit ortamına uyum sağlama ve gerçek zamanlı bildirime izin verme becerisini içermektedir. Araçlar ayrıca belirli imzaları ve verileri veya ağ veya uygulama davranış modellerini tanıyabilmektedir.

Otomatik izleme yazılımı, önceden tanımlanmış eşiklere dayalı olarak uyarılar (örn. yönetim konsolları, e-posta mesajları veya anlık mesajlaşma sistemleri yoluyla) oluşturacak şekilde yapılandırılmaktadır. Yanlış pozitifleri en aza indirmek için uyarı sistemi kurumumuz temel çizgisine göre ayarlanmakta ve eğitilmektedir.

Personel, uyarılara yanıt vermek üzere görevlendirilmekte ve potansiyel olayları doğru bir şekilde yorumlamak için uygun şekilde eğitilmektedir. Uyarı bildirimlerini almak ve bunlara yanıt vermek için yedekli sistemler ve süreçler bulunmaktadır.

Ayrıca izleme, ölçme, loglama süreçleri aşağıda belirtildiği şekilde uygulanmaktadır

* ISO 27001 BGYS’ nin Uygulanması
* Belirlenen risk kontrol yöntemlerinin uygulanması ve etkinliği
* ISO 27001 BGYS uygulamalarında tespit edilen hataların, meydana gelebilecek olay ve kazaların, genel anlamda sistem eksiklerinin değerlendirilmesi, bunlardan ders çıkarılarak tekrarlanmaması.
* ISO 27001 BGYS faaliyetleri ile ilgili olarak tüm taraflarla olan bilinçlendirme, iletişim ve eğitim faaliyetleri ve bunların etkinliği
* ISO 27001 BGYS Sisteminin düzenli olarak gözden geçirilmesi ve sürekli iyileştirilmesi yönünde yapılan çalışmalar

Bu temel unsurların dikkate alınmasında aşağıdaki temel girdi bilgilerinden yararlanılır;

* Tehlike tanımlamaları, risk değerlendirme ve kontrol sonuçları
* Yasal ve diğer gereklilikler
* ISO 27001 Politika ve hedefleri
* Bilgi güvenliği ve gizliliği ihlal olayları
* Uygunsuzluk raporları
* Eğitim kayıtları
* Loglama/izleme kayıtları
* Yönetim raporları
* İç denetim sonuçları

**PERFORMANS ÖLÇME İŞLEMLERİ**

Performans ölçümü aşağıdaki şekilde yapılır.

1. İç denetimler

Kurum bünyesinde ISO 27001 BGYS performansı İç Tetkik Prosedürüne göre yapılan iç denetimler ile ölçülür. Yapılan iç tetkikler esnasında bulunan uygunsuzluklar tespit edilip ilgili kişi veya birimlere ilgili Düzeltici Faaliyet işlemleri başlatılır.

2. Dış Denetimler

Kurum ISO 27001 BGYS performansı bağımsız ve resmi dış kuruluşlar tarafından yapılan değerlendirmelerle ölçülür. Yapılan dış tetkikler esnasında bulunan uygunsuzluklar tespit edilip ilgili kişi veya birimlere ilgili Düzeltici Faaliyet işlemleri başlatılır.

3. Performans İzleme

ISO 27001 BGYS performans izleme faaliyetleri ayrıca sistem eksiklikleri, uygunsuzluklar, risk işleme faaliyetleri ve ihlal olaylarına göre de yapılır.

* ISO 9001:2015 ve ISO 27001 BGYS politikasının bilinirliği
* ISO 9001:2015 ve ISO 27001 BGYS hedeflerinin karşılanma düzeyi
* Risk değerlendirme çalışmalarının devamlılığı
* Risk kontrol ve önlemlerinin uygulanma derecesi
* Yasal gerekliliklere uygunluk derecesi somut olarak uygunluğun derecesi iç tetkiklerde yasalar listesinin kontrolü
* Personelin ISO 9001:2015 ve ISO 27001 BGYS uygulamalarına uyumu
* Bölüm yöneticilerinin ISO 9001:2015 ve ISO 27001 BGYS uygulama performansları
* ISO 9001:2015 ve ISO 27001 BGYS eğitimlerinin verilmesi ve etkinliği
* Bilgi güvenliği ihlal olaylarının sayısı
* İç tetkik başarısı (uygunsuzluk sayısı)
* Düzeltici faaliyet sayısı.

***Kullanıcı Erişim Haklarının izlenmesi, gözden geçirilmesi;***

Bilgi varlıklarına erişimler bilgi sistemleri ekibi tarafından kontorlollü ve kayıtlı olarak sağlanmakta, gözden geçirilmekte, değiştirilmekte ve kaldırılmaktadır.

Erişim haklarının sağlanması ve iptali

Bir varlığın kimliği doğrulanmış kimliğine verilen fiziksel ve mantıksal erişim haklarını atamak veya iptal etmek için sağlama süreci şunları içermektedir:

a) bilgilerin ve diğer ilgili varlıkların sahibinden, bilgilerin ve diğer ilgili varlıkların kullanımı için yetki alınması (Yönetim tarafından erişim hakları için ayrı onay da uygun olabilir)

b) iş gereksinimlerini ve kuruluşun konuya özel politikasını ve erişim kontrolü kurallarını göz önünde bulundurarak;

c) erişim haklarının onaylanması ve uygulanması rollerinin ayrılması ve çatışan rollerin ayrılması da dahil olmak üzere görevler ayrılığının dikkate alınması;

d) özellikle kuruluştan ayrılan kullanıcıların erişim haklarının zamanında kaldırılmasını sağlamak üzere, birinin bilgilere ve diğer ilgili varlıklara erişmesi gerekmediğinde erişim haklarının kaldırılmasını sağlamak;

e) özellikle geçici personel veya personelin ihtiyaç duyduğu geçici erişim için, sınırlı bir süre için geçici erişim hakları verilmesinin ve bu hakların sona erme tarihinde iptal edilmesinin değerlendirilmesi;

f) verilen erişim düzeyinin erişim kontrolüne ilişkin konuya özel politikalara uygun olduğunun ve görevler ayrılığı gibi diğer bilgi güvenliği gereklilikleriyle tutarlı olduğunun doğrulanması;

g) erişim haklarının (örneğin hizmet sağlayıcılar tarafından) ancak yetkilendirme prosedürleri başarıyla tamamlandıktan sonra etkinleştirilmesinin sağlanması;

h) bilgilere ve diğer ilişkili varlıklara erişmek için bir kullanıcı tanımlayıcısına (ID, mantıksal veya fiziksel) verilen erişim haklarının merkezi bir kaydını tutmak;

i) rol veya iş değiştiren kullanıcıların erişim haklarının değiştirilmesi;

j) anahtarların, kimlik doğrulama bilgilerinin, kimlik kartlarının veya aboneliklerin kaldırılması, iptal edilmesi veya değiştirilmesi yoluyla yapılabilecek fiziksel ve mantıksal erişim haklarının kaldırılması veya ayarlanması;

k) kullanıcıların mantıksal ve fiziksel erişim haklarındaki değişikliklerin kaydını tutmak.

***Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi;***

Kurumumuz, tedarikçi bilgi güvenliği uygulamaları ve hizmet sunumundaki değişiklikleri düzenli olarak izlemeli, gözden geçirmekte, değerlendirmekte ve yönetmektedir.

Kurumumuz ve Tedarikçi arasındaki ilişkiyi yönetmek için aşağıdakileri içeren bir süreci içermektedir.

a) anlaşmalara uygunluğu doğrulamak için hizmet performans düzeylerini izlemek;

1) sunulan mevcut hizmetlerde iyileştirmeler;

2) herhangi bir yeni uygulama ve sistemin geliştirilmesi;

3) tedarikçinin politika ve prosedürlerinde yapılan değişiklikler veya güncellemeler;

4) bilgi güvenliği olaylarını çözmek ve bilgi güvenliğini iyileştirmek için yeni veya değiştirilmiş kontroller;

5) ağlarda değişiklikler ve geliştirmeler;

6) yeni teknolojilerin kullanımı;

7) yeni ürünlerin veya daha yeni sürümlerin veya sürümlerin benimsenmesi;

8) yeni geliştirme araçları ve ortamları;

9) hizmet tesislerinin fiziksel konumlarındaki değişiklikler;

10) alt tedarikçilerin değiştirilmesi;

11) başka bir tedarikçiye taşeronluk yapmak;

b) tedarikçi tarafından hazırlanan hizmet raporlarını gözden geçirmek ve sözleşmelerin gerektirdiği şekilde düzenli ilerleme toplantıları düzenlemek;

c) varsa bağımsız denetçi raporlarının incelenmesi ve tespit edilen sorunların takibi ile bağlantılı olarak tedarikçilerin ve alt tedarikçilerin denetimlerini gerçekleştirmek;

d) bilgi güvenliği olayları hakkında bilgi sağlamak ve bu bilgileri anlaşmaların ve destekleyici yönergeler ve prosedürlerin gerektirdiği şekilde gözden geçirmek;

e) sağlanan hizmetle ilgili bilgi güvenliği olaylarının, operasyonel sorunların, arızaların, hataların ve kesintilerin izlenmesine ilişkin tedarikçi denetim izlerini ve kayıtlarını gözden geçirin;

f) tanımlanmış herhangi bir bilgi güvenliği olayına veya olayına yanıt verin ve bunları yönetin;

g) bilgi güvenliği açıklarını belirleyin ve yönetin;

h) tedarikçinin kendi tedarikçileriyle olan ilişkilerinin bilgi güvenliği yönlerini gözden geçirmek;

ı) tedarikçinin, büyük hizmet başarısızlıkları veya felaketin ardından üzerinde anlaşmaya varılan hizmet süreklilik düzeylerinin sürdürülmesini sağlamak için tasarlanmış uygulanabilir planlarla birlikte yeterli hizmet kapasitesini sürdürmesini sağlamalıdır

i) tedarikçilerin, uyumluluğu gözden geçirmek ve anlaşmaların gerekliliklerini uygulamak

k) tedarikçilerin yeterli bilgi güvenliği seviyelerine sahip olduklarını düzenli olarak değerlendirin.

***Kesinti Sıresında İş sürekliliğiinin sağlanması amacıyla izleme gözden geçirme faliyetleri;***

Kurumumuzda, kesinti sırasında bilgi güvenliğini uygun bir seviyede nasıl sürdüreceğini planlamaktadır.

aşağıdakileri uygulamakta ve sürdürmektedir:

a) iş sürekliliği ve BİT sürekliliği planları dahilinde bilgi güvenliği kontrolleri, destekleyici sistemler ve araçlar;

b) kesinti sırasında mevcut bilgi güvenliği kontrollerini sürdürmek için süreçler;

c) kesinti sırasında sürdürülemeyen bilgi güvenliği kontrolleri için telafi edici kontroller.

d) destekleyici altyapı hizmetlerinin ticari büyümeyi karşılama kapasiteleri ve diğer destekleyici kuruluşlarla etkileşimleri açısından düzenli olarak değerlendirilmesini sağlamak;

e) destekleyici altyapı hizmetleri için kullanılan ekipmanın düzgün çalışmasını sağlamak için düzenli olarak denetlenmesini ve test edilmesini sağlamaktadır.

*Kurumumuz bünyesinde kullanılan, bilgi varlıklarımızın en genel anlamda izlenmesi gözlenmesi gereken veriler aşağıdaki gibidir:*

Kaynakların kullanımı izleme ve mevcut ve beklenen kapasite gereklilikleri doğrultusunda ayarlanmaktadır.

Bilgi işleme tesisleri, insan kaynakları, ofisler ve diğer tesisler için kapasite gereksinimleri, ilgili sistem ve süreçlerin iş açısından kritikliği dikkate alınarak belirlenmektedir.

Sistemlerin kullanılabilirliğini ve verimliliğini sağlamak ve gerektiğinde iyileştirmek için sistem ayarlama ve izleme uygulanmaktadır.

Bilg varlıklarımız en yüksek performans gereksinimlerini karşılamak için yeterli sistem kapasitesinin mevcut olduğunu doğrulamak için sistem ve hizmetlerin stres testlerini gerçekleştirmektedir.

Sorunları zamanında belirtmek için dedektif kontrolleri devreye alınmaktadır.

Gelecekteki kapasite gereksinimlerine ilişkin projeksiyonlar, yeni iş ve sistem gereksinimleri ile kuruluşun bilgi işleme yeteneklerindeki mevcut ve öngörülen eğilimleri dikkate almaktadır.

Uzun tedarik süreleri veya yüksek maliyetleri olan kaynaklara özel dikkat gösterilmektedir. Bu nedenle yöneticiler, hizmet veya ürün sahipleri, kilit sistem kaynaklarının kullanımını izlemektedir.

Yöneticiler, sistem güvenliğine veya hizmetlerine tehdit oluşturabilecek potansiyel kaynak sınırlamalarını ve kilit personele bağımlılığı belirlemek ve bunlardan kaçınmak ve uygun eylemi planlamak için kapasite bilgilerini kullanmalıdır.

• CPU kullanımları

• Memory kullanımları

• Ağ trafiği

• Ağ kapasite kullanımı

• Disk kapasite kullanımı

Yapılacak işlemler;

* Kurumda sistemlerin devamlılığının sağlanabilmesi amacıyla, donanım ve yazılım kaynaklarının izlenmesi gerekmektedir. İzleme araçları kullanılarak yapılan izlemede, herhangi bir sorun durumunda sorunun giderilmesini Bilgi İşlem Birimi, kendi kontrolünde ya da dış kaynaklı hizmet tedarikçisi ile olayı takip eder.
* Yönetimi Gözden Geçirme toplantılarında iş gücü ve çalışma alanı gibi kaynaklar planlanırken kapasite ile ilgili de ileriye dönük olarak planlama da yapılır. Bilgi İşlem Birimi tarafından sunucu, yazılım ve donanım gibi teknik ihtiyaçlar, kaynak kullanım oranları tespit edilir ve sunulur.
* Bilgi İşlem Birimi Yöneticisi her hafta mevcut sunucuların kapasite kullanım oranlarını kontrol eder ve kullanım oranı %80’nin üzerine çıktığında BGYS komitesine raporlama yapılır ve YGG toplantısında bu kullanım oranları raporlanır.
* Windows Sunucu İşletim Sistemleri
* Güvenlik Donanım ve Yazılımları
* Veri tabanları Logları
* Firewall Logları
* Dosya Sunucusu Erişim Logları
* Diğer uygulama yazılımı logları

*LOGLAMA FAALİYETLERİ*

Faaliyetleri, istisnaları, hataları ve diğer ilgili olayları kaydeden kayıtlar (loglar) üretilmekte, depolanmakta, korunma ve analiz edilmektedir.

Bilgi sistemleri ekibi, günlüklerin hangi amaçla oluşturulduğunu, hangi verilerin toplanıp günlüğe kaydedildiğini ve günlük verilerinin korunması ve işlenmesi için günlüğe özgü gereksinimleri belirlemektedir. Olay günlükleri, uygun olduğu şekilde, her olay için şunları içermeketdir:

a) kullanıcı kimlikleri;

b) sistem faaliyetleri;

c) ilgili olayların tarihleri, saatleri ve detayları (örn. oturum açma ve oturum kapatma);

d) cihaz kimliği, sistem tanımlayıcısı ve konumu;

e) ağ adresleri ve protokoller.

Günlük kaydı için aşağıdaki olaylar dikkate alınmaktadır:

a) başarılı ve reddedilen sistem erişim girişimleri;

b) başarılı ve reddedilen veriler ve diğer kaynak erişim girişimleri;

c) sistem konfigürasyonundaki değişiklikler;

d) ayrıcalıkların kullanımı;

e) yardımcı programların ve uygulamaların kullanımı;

f) önemli veri dosyalarının silinmesi dahil olmak üzere erişilen dosyalar ve erişim türü;

g) erişim kontrol sistemi tarafından verilen alarmlar;

h) anti-virüs sistemleri ve izinsiz giriş tespit sistemleri gibi güvenlik sistemlerinin etkinleştirilmesi ve devre dışı bırakılması;

i) kimliklerin oluşturulması, değiştirilmesi veya silinmesi;

j) uygulamalarda kullanıcılar tarafından gerçekleştirilen işlemler. Bazı durumlarda, uygulamalar bir üçüncü şahıs tarafından sağlanan veya yürütülen bir hizmet veya üründür.

Ayrıcalıklı erişim haklarına sahip olanlar da dahil olmak üzere kullanıcıların kendi etkinliklerine ilişkin günlükleri silme veya devre dışı bırakma izni bırakılmışdır. Yetkili kullanıcılar doğrudan kontrolleri altındaki bilgi işleme tesislerindeki günlükleri potansiyel olarak manipüle edebilme davranışlarınıda izlemek amacıyla ayrıcalıklı kullanıcılar için hesap verebilirliği sürdürmek için günlükleri koruma ve gözden geçirme faliyetleri uygulanmaktadır.

Günlüklerin korunması için, şu tekniklerin kullanılması düşünülmelidir: kriptografik karma, salt eklenen ve salt okunur bir dosyaya kayıt, genel bir şeffaflık dosyasına kayıt vb.

Loglama işlerinin yürütülmesi Bilgi İşlem Birimi sorumluluğundadır.

Loglama işlerinin denetlenmesi ve takibi BGYS Komitesi sorumluluğundadır.

Loglama işlemleri aşağıdaki proseslere göre yapılır:

WINDOWS SUNUCU İŞLETİM SİSTEMLERİ LOGLARI

1. Kurumumuz dahilinde kullanılan sunucu işletim sistemleri Microsoft Windows diğer işletim sistemlerinin oluşturdukları Event logların yönetimi ve takibi Bilgi İşlem Birimi tarafından yapılır.

2. Loglama sürecinde; normal sistem olayları (login, açma, kapama, vb), bilgi güncellemeleri (dosya oluşturma, silme, güncelleme, vb), yetkisi erişimler, sistem yönetim işlemleri, yönetici hesapları işlemleri gibi olaylar kaydedilir.

ACTIVE DIRECTORY YÖNETİCİ HESAPLARIN LOGLARI

1. Active Directory üzerinde yönetici hesaplarının yapmış olduğu işlemler üçüncü parti yazılımlar ile kayıt altına alınmaktadır.

2. Loglama sürecinde; normal sistem olayları (login, açma, kapama, vb), bilgi güncellemeleri (dosya oluşturma, silme, güncelleme, vb), yetkisi erişimler, sistem yönetim işlemleri, yönetici hesapları işlemleri gibi olaylar kaydedilir.

DOSYA SUNUCU (FILE SERVER) DOSYA ERİŞİM LOGLARI

1. File Server üzerinde bulunan dosyalara erişim kayıtları üçüncü parti yazılımlar ile kayıt altına alınıp Bilgi İşlem Birimi tarafından izlenmektedir.

2. Loglama sürecinde; normal sistem olayları (login, açma, kapama, vb), bilgi güncellemeleri (dosya oluşturma, silme, güncelleme, vb), yetkisi erişimler, sistem yönetim işlemleri, yönetici hesapları işlemleri gibi olaylar kaydedilir.

SSL/VPN LOGLARI

Şirket dışından SSL/VPN ile şirket ağına giriş yapan kullanıcılara ait erişim kayıtları üçüncü parti yazılımlar ile kayıt altına alınıp Bilgi İşlem Birimi tarafından izlenmektedir.

MAIL TRAFİĞİ LOGLARI

Tüm mail trafiği üçüncü parti yazılımlar ile kayıt altına alınıp Bilgi İşlem Birimi tarafından izlenmektedir.

ANTİVİRÜS YAZILIM LOGLARI

Şirkette antivirüs yazılımı olarak Trend Micro kullanılmaktadır. Antivirüs ile ilgili eventler Bilgi İşlem Birimi tarafından izlenmektedir.

LOGLARIN SAKLANMASI VE ERİŞİM KONTROLÜ

1. Log kayıtları için farklı sunucular kullanılmaktadır. Sunucu üzerinde saklama süresi sınırsız olarak belirtilmiştir. Loglara erişim Bilgi İşlem Birimi yönetimindedir. Gerekmedikçe hizmet sağlayıcının loglara erişimi kısıtlanmıştır.
2. Firma dahilinde oluşan güvenlik logları Log Sunucuları üzerinde ilgili klasörlere kopyalanır.
3. Bilgi İşlem Birimi bu sunucunun yönetiminden sorumludur.
4. Log Sunucuları, 30 gün boyunca günlük olarak yedeklenir. Log yedekleme, “Yedekleme Politikası”ndaki uygulamalarla aynı doğrultudadır.

LOGLARIN İZLENMESİ

Bilgi İşlem Birimi tarafından düzenli olarak log kayıtlarının sorunsuz alındığı denetlenmelidir. Log detayına erişim BGYS komitesinin yetkilendirdiği kişi tarafından ulaşılabilir.

Gerekli alarmlar ve raporlama mekanizmaları kullanılan yazılımların izin verdiği ölçüde etkinleştirilir.

**8.16 İzleme Faaliyetleri**

Ağlar, sistemler ve uygulamalar anomali içeren davranışlara karşı izlenmekte ve potansiyel bilgi güvenliği ihlal olaylarını değerlendirmek için uygun önlemler alınmaktadır.

İzleme kapsamı ve düzeyi, iş ve bilgi güvenliği gereksinimlerine uygun olarak ve ilgili yasa ve yönetmelikler dikkate alınarak belirlenmektedir. İzleme kayıtları, tanımlanmış saklama süreleri boyunca tutulmaktadır.

Aşağıdakilerin izleme sistemine dahil edilmesi düşünülmektedir.

a) giden ve gelen ağ, sistem ve uygulama trafiği,

b) sistemlere, sunuculara, ağ ekipmanına, izleme sistemine, kritik uygulamalara vb. erişim,

c) kritik veya yönetici düzeyinde sistem ve ağ yapılandırma dosyaları,

d) güvenlik araçlarından günlükler [örn. antivirüs, IDS, saldırı önleme sistemi (IPS), web filtreleri, güvenlik duvarları, veri sızıntısı önleme],

e) sistem ve ağ etkinliği ile ilgili olay günlükleri,

f) yürütülmekte olan kodun sistemde çalışma yetkisinin olup olmadığının ve kurcalanmadığının kontrol edilmesi (örn. ilave istenmeyen kod eklemek için yeniden derleme yoluyla),

g) kaynakların kullanımı (örn. CPU, sabit diskler, bellek, bant genişliği) ve performansları.

Kurumumuz, normal davranış için bir temel oluşturmalı ve anormallikler için bu temele göre izleme yapmaktadır. Bir temel oluştururken, aşağıdakiler dikkate alınmaktadır.

a) sistemlerin normal ve yoğun dönemlerde kullanımının gözden geçirilmesi,

b) olağan erişim zamanı, erişim yeri, her kullanıcı veya kullanıcı grubu için erişim sıklığı.

İzleme sistemi, aşağıdakiler gibi anormal davranışları belirlemek için belirlenen temele göre yapılandırılmaktadır.

a) süreçlerin veya uygulamaların planlanmamış sonlandırılması,

b) bilinen kötü amaçlı IP adreslerinden veya ağ etki alanlarından (örn. botnet komut ve kontrol sunucularıyla ilişkili olanlar) kaynaklanan tipik olarak kötü amaçlı yazılım veya trafikle ilişkili etkinlik,

c) bilinen saldırı özellikleri (örn. hizmet reddi ve arabellek taşmaları),
d) olağandışı sistem davranışı (örn. tuş vuruşu kaydı, işlem enjeksiyonu ve standart protokollerin kullanımındaki sapmalar),

e) darboğazlar ve aşırı yükler (örn. ağ kuyruğu, gecikme seviyeleri ve ağ titremesi),

f) sistemlere veya bilgilere yetkisiz erişim (gerçek veya denenmiş),

g) iş uygulamalarının, sistemlerinin ve ağlarının izinsiz taranması,

h) korunan kaynaklara (örn. DNS sunucuları, web portalları ve dosya sistemleri) erişmeye yönelik başarılı ve başarısız girişimler,

i) Beklenen davranışla ilişkili olağandışı kullanıcı ve sistem davranışı.

Bir izleme aracı aracılığıyla sürekli izleme kullanılmaktadır. İzleme, kurumsal ihtiyaç ve yeteneklere bağlı olarak gerçek zamanlı veya periyodik aralıklarla yapılmaktadır. İzleme araçları, büyük miktarda veriyi işleme, sürekli değişen tehdit ortamına uyum sağlama ve gerçek zamanlı bildirime izin verme becerisini içermektedir. Araçlar ayrıca belirli imzaları ve verileri veya ağ veya uygulama davranış modellerini tanıyabilmektedir.

Otomatik izleme yazılımı, önceden tanımlanmış eşiklere dayalı olarak uyarılar (örn. yönetim konsolları, e-posta mesajları veya anlık mesajlaşma sistemleri yoluyla) oluşturacak şekilde yapılandırılmaktadır. Yanlış pozitifleri en aza indirmek için uyarı sistemi kurumumuzun temel çizgisine göre ayarlanmalı ve eğitilmektedir. Personel, uyarılara yanıt vermek üzere görevlendirilmekte ve potansiyel olayları doğru bir şekilde yorumlamak için uygun şekilde eğitilmektedir. Uyarı bildirimlerini almak ve bunlara yanıt vermek için yedekli sistemler ve süreçler bulunmaktadır.

**8.17 Saat Senkronizasyonu**

Kurumumuz, tarafından kullanılan bilgi işlem sistemlerinin saatleri, onaylanmış zaman kaynaklarına senkronize edilmekteir.

Ulusal bir atom saatinden veya küresel konumlandırma sisteminden (GPS) yayınlanan bir radyo zamanına bağlı bir saat, kayıt sistemleri için referans saat olarak kullanılmaktaıdır. Doğru zaman damgalarını sağlamak için tutarlı, güvenilir bir tarih ve saat kaynağı ağa bağlı tüm sistemleri bir referans saat ile senkronize halde tutmak için ağ zaman protokolü (NTP) veya hassas zaman protokolü (PTP) gibi protokoller kullanılmaktadır.

İhtiyaç halinde birden fazla bulut hizmeti kullanırken veya hem bulut hem de şirket içi hizmetleri kullanırken saat senkronizasyonu zor olması durumda, tutarsızlıklardan kaynaklanan riskleri azaltmak için her hizmetin saati izlenmekte ve fark kaydedilmektedir.

**8.18 Ayrıcalıklı Destek Programlarının Kullanımı**

Sistem ve uygulama kontrollerini geçersiz kılabilecek destek programların kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmektedir.

Sistem ve uygulama kontrollerini geçersiz kılabilen yardımcı programların kullanımına ilişkin aşağıdaki yönergeler dikkate alınmaktadır.

a) yardımcı programların kullanımının güvenilir, yetkili kullanıcıların minimum pratik sayısıyla sınırlandırılması,

b) yardımcı programı kullanan kişinin benzersiz olarak tanımlanması da dahil olmak üzere, yardımcı programlar için tanımlama, kimlik doğrulama ve yetkilendirme prosedürlerinin kullanımı,

c) yardımcı programlar için yetki düzeylerinin tanımlanması ve belgelenmesi,

d) yardımcı programların geçici kullanımı için yetkilendirme;

e) görev ayrımının gerekli olduğu sistemlerdeki uygulamalara erişimi olan kullanıcılara yardımcı programlar sunmamak,

f) tüm gereksiz yardımcı programların kaldırılması veya devre dışı bırakılması,

g) en azından, yardımcı programların uygulama yazılımından mantıksal olarak ayrılması. Uygulanabilir olduğunda, bu tür programlar için ağ iletişimini uygulama trafiğinden ayırmak,

h) yardımcı programların mevcudiyetinin sınırlandırılması (örneğin, yetkili bir değişikliğin süresi boyunca),

i) yardımcı programların tüm kullanımının günlüğe kaydedilmesi.

**8.19 İşletim Sistemlerine Yazılım Kurulumu**

İşletim sistemlerinde yazılım kurulumunu güvenli bir şekilde yönetmek için prosesler ve önlemler uygulanmaktadır.

Değişiklikleri ve işletim sistemlerine yazılım kurulumunu güvenli bir şekilde yönetmek için aşağıdaki yönergeler dikkate alınmaktadır.

a) operasyonel yazılım güncellemelerinin yalnızca uygun yönetim yetkisine sahip eğitimli yöneticiler tarafından gerçekleştirilmes,

b) operasyonel sistemlere yalnızca onaylanmış yürütülebilir kodun ve hiçbir geliştirme kodunun veya derleyicinin kurulmamasını sağlamak,

c) yazılımı yalnızca kapsamlı ve başarılı testlerden sonra kurma ve güncellema

d) ilgili tüm program kaynak kitaplıklarının güncellenmesi,

e) tüm operasyonel yazılımların yanı sıra sistem belgelerinin kontrolünü elinde tutmak için bir konfigürasyon kontrol sistemi kullanmak,

f) değişiklikler uygulanmadan önce bir geri alma stratejisinin tanımlanması,

g) operasyonel yazılıma yapılan tüm güncellemelerin bir denetim günlüğünü tutmak,

h) yazılımın eski sürümlerini, gerekli tüm bilgiler ve parametreler, prosedürler, yapılandırma ayrıntıları ve destekleyici yazılımla birlikte bir acil durum önlemi olarak ve yazılımın arşivlenmiş verileri okumak veya işlemek için gerekli olduğu sürece arşivlemek.

Yeni bir sürüme yükseltme kararı, değişiklik ve sürümün güvenliği için iş gereksinimlerini dikkate almaktadır. (örneğin, yeni bilgi güvenliği işlevselliğinin getirilmesi veya mevcut sürümü etkileyen bilgi güvenliği açıklarının sayısı ve ciddiyeti). Yazılım yamaları, bilgi güvenliği açıklarını ortadan kaldırmaya veya azaltmaya yardımcı olabilecekleri zaman uygulanmaktadır.

Bilgisayar yazılımı, bilgi güvenliği açıkları ortaya çıkarabileceğinden yetkisiz değişiklikleri önlemek için izlenmesi ve kontrol edilmesi gereken dışarıdan sağlanan yazılım ve paketlere (örneğin, harici sitelerde barındırılan modülleri kullanan yazılım programları) güvenebilir.

Operasyonel sistemlerde kullanılan satıcı tarafından sağlanan yazılımlar, tedarikçi tarafından desteklenen bir düzeyde tutulmaktadır. Zamanla, yazılım satıcıları yazılımın eski sürümlerini desteklemeyi bırakacaktır. Kurumumuz, desteklenmeyen yazılımlara güvenmenin risklerini göz önünde bulundurmaktadır. Operasyonel sistemlerde kullanılan açık kaynaklı yazılımlar, yazılımın uygun olan en son sürümüne sahip olmaktadır. Zamanla, açık kaynak kodunun sürdürülmesi sona erebilir, ancak yine de bir açık kaynak yazılım deposunda bulunur. kurumumuz, operasyonel sistemlerde kullanıldığında bakımı yapılmayan açık kaynaklı yazılımlara güvenmenin risklerini de dikkate almalıdır.

Tedarikçiler yazılım yükleme veya güncelleme sürecine dahil olduğunda, fiziksel veya mantıksal erişim yalnızca gerektiğinde ve uygun yetkilendirme ile verilmektedir. Tedarikçinin faaliyetleri izlenmektedir.

Kurumumuz, kullanıcıların hangi tür yazılımları yükleyebileceği konusunda katı kurallar tanımlamakta ve uygulamaktadır.

İşletim sistemlerine yazılım kurulumunda en az ayrıcalık ilkesi uygulanmaktadır. Kurumumuz, hangi tür yazılım yüklemelerine izin verildiğini (örneğin, mevcut yazılımlara yönelik güncellemeler ve güvenlik yamaları) ve hangi tür yüklemelerin yasak olduğunu (örneğin, yalnızca kişisel kullanım için olan yazılımlar ve potansiyel olarak kötü niyetli olup olmadığı bilinmeyen veya bilinmeyen yazılımlar) belirlemektedir.

**8.20 Ağ Güvenliği**

Sistemlerdeki ve uygulamalardaki bilgileri korumak için ağlar ve ağ cihazları güvenlik altına alınmakta, yönetilmekte ve kontrol edilmektedir.

Ağlardaki bilgilerin güvenliğini sağlamak ve bağlı hizmetleri yetkisiz erişimden korumak için kontroller uygulanmaktadır. Özellikle, aşağıdaki maddeler dikkate alınmaktadır.

a) ağın destekleyebileceği bilgilerin türü ve sınıflandırma düzeyi,

b) ağ ekipmanı ve cihazlarının yönetimi için sorumluluklar ve prosesler oluşturmak,

c) ağ diyagramları ve aygıtların (örn. yönlendiriciler, anahtarlar) yapılandırma dosyaları dahil olmak üzere güncel dokümantasyonu sürdürmek,

d) ağlar için operasyonel sorumluluğu, uygun olduğunda ICT sistem operasyonlarından ayırmak,

e) genel ağlar, üçüncü taraf ağlar veya kablosuz ağlar üzerinden geçen verilerin gizliliğini ve bütünlüğünü korumak ve bağlı sistemleri ve uygulamaları korumak için kontroller oluşturmak ağ hizmetlerinin ve ağa bağlı bilgisayarların kullanılabilirliğini korumak için ek kontroller de gerektiğinde uygulanmaktadır.

f) bilgi güvenliğini etkileyebilecek veya bununla ilgili eylemlerin kaydedilmesini ve tespit edilmesini sağlamak için uygun şekilde günlüğe kaydetme ve izleme,

g) hem kurumumuza verilen hizmeti optimize etmek hem de kontrollerin bilgi işleme altyapısı genelinde tutarlı bir şekilde uygulanmasını sağlamak için ağ yönetimi faaliyetlerini yakından koordine etmek,

h) ağdaki sistemlerin kimlik doğrulaması,

i) sistemlerin ağa bağlantısının kısıtlanması ve filtrelenmesi (örn. güvenlik duvarlarının kullanılması),

n) savunmasız ağ protokollerini devre dışı bırakmak .

Kurumumuz, sanallaştırılmış ağların kullanımına uygun güvenlik kontrollerinin uygulanmasını sağlamaktadır. Sanallaştırılmış ağlar, yazılım tanımlı ağları (SDN, SD-WAN) da kapsar. Sanallaştırılmış ağlar, özellikle dağıtılmış bilgi işlem kullanılarak uygulanan sistemler ve uygulamalar için fiziksel ağlar üzerinde gerçekleşen iletişimin mantıksal olarak ayrılması sağlar.ı

j) ekipman ve cihazların ağa bağlantısını tespit etmek, kısıtlamak ve doğrulamak,

k) ağ cihazlarının güçlendirilmesi,

l) ağ yönetim kanallarının diğer ağ trafiğinden ayrılması,
m) ağ saldırı altındaysa kritik alt ağları geçici olarak izole etme (örn. asma köprülerle),

**8.21 Ağ Hizmetlerinin Güvenliği**

Ağ hizmetlerinin güvenlik mekanizmaları, hizmet seviyeleri ve hizmet gereklilikleri belirlenerek, uygulanmakta ve izlenmektedir.

Güvenlik özellikleri, hizmet seviyeleri ve hizmet gereksinimleri gibi belirli hizmetler için gerekli güvenlik önlemleri tanımlanmakta ve uygulanmaktadır. (dahili veya harici ağ hizmeti sağlayıcıları tarafından).

Kurumumuz, ağ hizmeti sağlayıcılarının bu önlemleri uygulamasını sağlamaktadır.

Ağ hizmeti sağlayıcısının mutabık kalınan hizmetleri güvenli bir şekilde yönetme yeteneği belirlenmekte ve düzenli olarak izlenmektedir. Denetim hakkı, kurumumuz ve sağlayıcı arasında kararlaştırılmaktadır.

Kurumumuz ayrıca, uygun güvenlik önlemlerini sürdürdüklerini göstermek için hizmet sağlayıcılar tarafından sağlanan üçüncü taraf tasdiklerini de dikkate almaktadır.

Ağların ve ağ hizmetlerinin kullanımına ilişkin kurallar aşağıdakileri kapsayacak şekilde formüle edilmekte ve uygulanmaktadır.

a) erişime izin verilen ağlar ve ağ hizmetleri,

b) çeşitli ağ hizmetlerine erişim için kimlik doğrulama gereksinimleri,

c) kimin hangi ağlara ve ağ bağlantılı hizmetlere erişmesine izin verildiğini belirlemek için yetkilendirme prosesleri,

d) ağ bağlantılarına ve ağ hizmetlerine erişimi korumak için ağ yönetimi ve teknolojik kontroller ve prosesler,

e) ağlara ve ağ hizmetlerine erişmek için kullanılan araçlar [örneğin, sanal özel ağ (VPN) veya kablosuz ağ kullanımı]

f) erişim sırasında kullanıcının zamanı, konumu ve diğer özellikleri,

g) ağ hizmetlerinin kullanımının izlenmesi.

Ağ hizmetlerinin aşağıdaki güvenlik özellikleri dikkate alınmaktadır.

a) kimlik doğrulama, şifreleme ve ağ bağlantısı kontrolleri gibi ağ hizmetlerinin güvenliği için uygulanan teknoloji,

b) güvenlik ve ağ bağlantısı kurallarına uygun olarak ağ hizmetleri ile güvenli bağlantı için gerekli teknik parametreler,

c) önbelleğe alma (örneğin bir içerik dağıtım ağında) ve kullanıcıların performans, kullanılabilirlik ve gizlilik gerekliliklerine uygun olarak önbelleğe almayı seçmesine izin veren parametreleri,

d) gerektiğinde ağ hizmetlerine veya uygulamalarına erişimi kısıtlamak için ağ hizmeti kullanımına ilişkin prosesler.

**8.22 Ağların Ayrımı**

Kurumumuz, ağlarında bilgi hizmetleri grupları, kullanıcılar ve bilgi sistemleri ayrılmaktadır.

Kurumumuz, büyük ağların güvenliğini, onları ayrı ağ etki alanlarına bölerek ve genel ağdan (örn. internet) ayırarak yönetmeyi düşünmektedir. Alanlar, güven, kritiklik ve hassasiyet seviyelerine (ör. genel erişim alanı, masaüstü alanı, sunucu alanı, düşük ve yüksek riskli sistemler), organizasyonel birimler (ör. insan kaynakları, finans, pazarlama) veya bazı kombinasyonlara göre seçilmiştir. (örneğin, birden çok kurumumuz birimine bağlanan sunucu etki alanı). Ayrım, fiziksel olarak farklı ağlar kullanılarak veya farklı mantıksal ağlar kullanılarak yapılmaktadır.

Kablosuz ağlar, yetersiz tanımlanmış ağ çevresi nedeniyle özel muamele gerektirmektedir. Kablosuz ağların ayrılması için radyo kapsama alanı ayarlaması düşünülmektedir. Hassas ortamlar için, dahili sistemlere erişim izni verilmeden önce , tüm kablosuz erişimlerin harici bağlantılar olarak ele alınması ve bu erişimin, ağ kontrollerine uygun olarak bir ağ geçidinden geçene kadar dahili ağlardan ayrılması düşünülmekteidir . Personel yalnızca kurumumuzun konuya özgü politikalarına uygun kontrollü kullanıcı uç nokta cihazları kullanıyorsa, misafirler için kablosuz erişim ağı personel için olanlardan ayrılmaktadır. Misafir WiFi'sinin personel tarafından kullanılmasını engellemek için, “en azından personellere” WiFi ile aynı kısıtlamalara sahip kurallar tanımlıdır.

**8.23 Web Filtreleme**

Harici web sitelerine erişim, kötü amaçlı içeriğe maruz kalmayı azaltacak şekilde yönetilmektedir.

Kurumumuz, personelinin yasa dışı bilgiler içeren veya virüs ya da kimlik avı materyali içerdiği bilinen web sitelerine erişme riskini azaltmaktadır. Bunu başarmak için kullanılan bir teknik, ilgili web site(ler)inin IP adresini veya etki alanını bloke ederek çalışır. Bazı tarayıcılar ve kötü amaçlı yazılımdan koruma teknolojileri bunu otomatik olarak yapar veya bu şekilde yapılandırılmaktadır.

Kurumumuz, personelin erişmesi veya erişmemesi gereken web sitesi türlerini belirlemektedir. Kurumuz, aşağıdaki web sitesi türlerine erişimi engellemeyi düşünmektedir.

a) geçerli ticari nedenlerle izin verilmediği sürece bilgi yükleme işlevine sahip web siteleri,

b) bilinen veya şüphelenilen kötü amaçlı web siteleri (örn. kötü amaçlı yazılım veya kimlik avı içerikleri dağıtanlar),

c) komuta ve kontrol sunucuları,

d) tehdit istihbaratından elde edilen kötü amaçlı web sitesi,

e) yasa dışı içerik paylaşan web siteleri.

Bu kontrolü uygulamaya koymadan önce kurumumuz, istenmeyen veya uygunsuz web siteleri ve web tabanlı uygulamalara yönelik kısıtlamalar dahil olmak üzere çevrimiçi kaynakların güvenli ve uygun kullanımına yönelik kurallar oluşturmaktadır. Kurallar güncel tutulmaktadır.

Web'e erişim de dahil olmak üzere çevrimiçi kaynakların güvenli ve uygun kullanımı konusunda personele eğitim verilmektedir. Eğitim, kurumumuz kurallarını, güvenlik endişelerini dile getirmek için irtibat noktasını ve meşru iş nedenleriyle kısıtlı web kaynaklarına erişilmesi gerektiğinde istisna sürecini içermektedir. Bir web sitesinin güvenli olmadığını bildiren ancak kullanıcının ilerlemesine izin veren herhangi bir tarayıcı tavsiyesini geçersiz kılmamalarını sağlamak için personele de eğitim verilmektedir.

**8.24 Kriptografi (Şifreleme) Kullanımı**

Kriptografik anahtar yönetimi de dahil olmak üzere kriptografinin etkin kullanımına yönelik kurallar tanımlanmakta ve uygulanmaktadır.

Kurumumuzun kriptografinin etkin kullanımına ilişkin kurallarını uygularken, dünyanın farklı yerlerinde kriptografik tekniklerin kullanımına uygulanabilecek düzenlemeler ve ulusal kısıtlamaların yanı sıra şifrelenmiş bilgilerin sınır ötesi akışı konuları da dikkate alınmaktadır.

Hizmet düzeyi anlaşmalarının veya harici kriptografik hizmet tedarikçileriyle (örneğin bir sertifika yetkilisiyle) yapılan sözleşmelerin içeriği, sorumluluk, hizmetlerin güvenilirliği ve hizmetlerin sağlanmasına yönelik yanıt süreleri konularını kapsamaktadır.

Uygun anahtar yönetimi, kriptografik anahtarların oluşturulması, saklanması, arşivlenmesi, alınması, dağıtılması, kullanımdan kaldırılması ve imha edilmesi için güvenli süreçler gerektiğinde tüm kriptografik anahtarlar, değişikliğe ve kayba karşı korunmaktadır.

Ek olarak, gizli ve özel anahtarlar, yetkisiz kullanıma ve ifşaya karşı korunmaya ihtiyaç duyduğunda anahtarları oluşturmak, depolamak ve arşivlemek için kullanılan ekipman fiziksel olarak korunmaktadır.

**8.25 Güvenli Geliştirme Yaşam Döngüsü**

Yazılım ve sistemlerin güvenli bir şekilde geliştirilmesi için kurallar oluşturulmakta ve uygulanmaktadır.

Güvenli geliştirme, güvenli bir hizmet, mimari, yazılım ve sistem oluşturmak için bir gerekliliktir. Bunu başarmak için aşağıdaki hususlar dikkate alınmaktadır.

a) geliştirme, test ve üretim ortamlarının ayrılması,

b) yazılım geliştirme yaşam döngüsünde güvenlik konusunda rehberlik,

 1) yazılım geliştirme metodolojisinde güvenlik,

 2) kullanılan her programlama dili için güvenli kodlama yönergeleri,

c) şartname ve tasarım aşamasındaki güvenlik gereksinimleri,

d) projelerde güvenlik kontrol noktaları,

e) regresyon testi, kod taraması ve sızma testleri gibi sistem ve güvenlik testleri,

f) kaynak kodu ve yapılandırma için güvenli depolar,

g) sürüm kontrolünde güvenlik,

h) gerekli uygulama güvenliği bilgisi ve eğitimi,

i) geliştiricilerin güvenlik açıklarını önleme, bulma ve düzeltme yeteneği,

j) Gelecekteki lisanslama sorunlarından kaçınırken uygun maliyetli çözümler sağlamak için lisanslama gereklilikleri ve alternatifleri,

Geliştirme dışarıdan temin ediliyorsa kurumumuz, tedarikçinin kurumumuzun güvenli geliştirme kurallarına uyduğuna dair güvence almaktadır.

**8.26 Uygulama Güvenlik Gereklilikleri**

Uygulamalar geliştirilirken veya edinilirken bilgi güvenliği gereklilikleri; tanımlanmakta, belirtilmekte ve onaylanmaktadır.

Uygulama güvenlik gereksinimleri belirlerek ve özenle belirtilmektedir. Bu gereksinimler genellikle bir risk değerlendirmesi yoluyla belirlenir. Gereksinimler, bilgi güvenliği uzmanlarının desteği ile geliştirilmektedir.

Uygulama güvenlik gereksinimleri, uygulamanın amacına bağlı olarak çok çeşitli konuları kapsayabilir.

Uygulama güvenlik gereksinimleri, uygulanabilir olduğu şekilde şunları içermektedir.

a) varlıkların kimliğine olan güven düzeyi [örneğin kimlik doğrulama yoluyla,

b) uygulama tarafından işlenecek bilgi türünün ve sınıflandırma seviyesinin belirlenmesi,

c) uygulamadaki verilere ve işlevlere erişim ve erişim düzeyi ayrımı ihtiyacı,

d) kötü amaçlı saldırılara veya kasıtsız kesintilere karşı dayanıklılık [örneğin arabellek taşmasına veya yapılandırılmış sorgu dili (SQL) enjeksiyonlarına karşı koruma],

e) işlemin oluşturulduğu, işlendiği, tamamlandığı veya saklandığı yargı alanındaki yasal, kanuni ve düzenleyici gereklilikler,

f) ilgili tüm taraflarla ilişkili mahremiyet ihtiyacı,

g) herhangi bir gizli bilginin koruma gereklilikleri,

h) işlenirken, aktarılırken ve dururken verilerin korunması,

i) ilgili tüm taraflar arasındaki iletişimleri güvenli bir şekilde şifreleme ihtiyacı; h) bütünlük kontrolleri ve girdi doğrulama dahil olmak üzere girdi kontrolleri,

j) otomatik kontroller (örn. onay limitleri veya ikili onaylar),

k) çıktılara kimin erişebileceğini ve yetkisini de dikkate alan çıktı kontrolleri,

l) "serbest metin" alanlarının içeriğiyle ilgili kısıtlamalar, çünkü bunlar gizli verilerin (örn. kişisel veriler) kontrolsüz bir şekilde saklanmasına yol açabilir,

m) işlem günlüğü ve izleme, inkar etmeme gereksinimleri gibi iş sürecinden türetilen gereksinimler,

n) diğer güvenlik kontrolleri tarafından zorunlu kılınan gereksinimler (örn. günlük kaydı ve izleme veya veri sızıntısı tespit sistemleri için arayüzler),

o) hata mesajı işleme*.*

**8.27 Güvenli Sistem Mimarisi ve Mühendislik İlkeleri**

Güvenli sistemlerin mühendisliğine yönelik ilkeler oluşturulmakta, dokümante edilmekte, sürdürülmekte ve herhangi bir bilgi sistemi geliştirme faaliyetine uygulanmaktadır.

Güvenlik mühendisliği ilkeleri oluşturularak, belgelenmekte ve bilgi sistemi mühendisliği faaliyetlerine uygulanmaktadır. Güvenlik, tüm mimari katmanlarda (iş, veri, uygulamalar ve teknoloji) tasarlanmaktadır. Yeni teknoloji, güvenlik riskleri açısından analiz edilmeli ve tasarım, bilinen saldırı modellerine göre gözden geçirilmektedir.

Güvenli mühendislik ilkeleri, kullanıcı kimlik doğrulama teknikleri, güvenli oturum kontrolü ve veri doğrulama ve temizleme konusunda rehberlik sağlar.

Güvenli sistem mühendisliği şunları içermektedir.

a) "tasarım gereği güvenlik", "derinlemesine savunma", "varsayılan güvenlik", "varsayılan reddetme", "güvenli başarısız olma", "harici uygulamalardan gelen güvensizlik", "dağıtımda güvenlik" gibi güvenlik mimarisi ilkelerinin kullanımı, "ihlal varsay", "en az ayrıcalık", "kullanılabilirlik ve yönetilebilirlik" ve "en az işlevsellik",

b) bilgi güvenliği açıklarını belirlemeye, güvenlik kontrollerinin belirlenmesini sağlamaya ve güvenlik gereksinimlerini karşılamaya yardımcı olacak güvenlik odaklı bir tasarım incelemesi,

c) gereksinimleri tam olarak karşılamayan güvenlik kontrollerinin belgelenmesi ve resmi olarak onaylanması (örn. güvenlik gereksinimlerinin ağır basması nedeniyle),

d) sistemlerin sertleştirilmesi.

Yerleşik güvenlik mühendisliği ilkeleri, uygulanabildiği yerde, kurumumuz ile kurumumuzun dış kaynak kullandığı tedarikçi arasındaki sözleşmeler ve diğer bağlayıcı anlaşmalar aracılığıyla bilgi sistemlerinin dış kaynak kullanımıyla geliştirilmesine uygulanmaktadır. Kurumumuz, tedarikçilerin güvenlik mühendisliği uygulamalarının kurumumuzun ihtiyaçları ile uyumlu olmasını sağlamaktadır.

Güvenlik mühendisliği ilkeleri ve yerleşik mühendislik prosesleri, mühendislik sürecinde gelişmiş güvenlik standartlarına etkin bir şekilde katkıda bulunmalarını sağlamak için düzenli olarak gözden geçirilmektedir. Ayrıca, yeni potansiyel tehditlerle mücadele etme ve uygulanan teknolojiler ve çözümlerdeki gelişmelere uygulanabilir kalma açısından güncel kalmalarını sağlamak için düzenli olarak gözden geçirilmektedir.

**8.28 Güvenli Kodlama**

Güvenli kodlama ilkeleri yazılım geliştirmeye uygulanmaktadır.

Kurumumuz, güvenli kodlama için iyi yönetişim sağlamak üzere kurumumuz çapında süreçler oluşturmaktadır. Minimum güvenli bir temel oluşturulmakta ve uygulanmaktadır. Ek olarak, bu tür süreçler ve yönetişim, üçüncü taraf yazılım bileşenlerini ve açık kaynaklı yazılımları kapsayacak şekilde genişletilmektedir.

Kurumumuz, sürekli iyileştirme ve öğrenme yoluyla kurumumuzun güvenli kodlama ilkelerine rehberlik etmek için gerçek dünyadaki tehditleri ve yazılım güvenlik açıklarına ilişkin güncel tavsiye ve bilgileri izlemektedir. Bu, hızla değişen tehdit ortamıyla mücadele etmek için etkili güvenli kodlama uygulamalarının uygulanmasını sağlamaya yardımcı olmaktadır.

Güvenli kodlama ilkeleri hem yeni geliştirmelerde hem de yeniden kullanım senaryolarında kullanılmaktadır. Bu ilkeler, hem kurumumuz içindeki geliştirme faaliyetlerine hem de kurumumuz tarafından başkalarına sağlanan ürün ve hizmetlere uygulanmaktadır. Kodlamadan önceki planlama ve ön koşullar şunları içermektedir.

a) hem kurum içi hem de dış kaynaklı kod geliştirmelerinde kullanılacak güvenli kodlama için kurumumuza özgü beklentiler ve onaylanmış ilkeler,

b) bilgi güvenliği açıklarına yol açan yaygın ve tarihsel kodlama uygulamaları ve kusurları,

c) güvenli kod oluşturulmasını zorlamaya yardımcı olmak için tümleşik geliştirme ortamları (IDE) gibi geliştirme araçlarını yapılandırmak,

d) uygun olduğu şekilde, geliştirme araçları ve yürütme ortamları sağlayıcıları tarafından yayınlanan kılavuza uymak;

e) güncellenmiş geliştirme araçlarının (örn. derleyiciler) bakımı ve kullanımı,

f) geliştiricilerin güvenli kod yazma konusundaki nitelikleri,

g) tehdit modelleme dahil olmak üzere güvenli tasarım ve mimari,

h) güvenli kodlama standartları ve ilgili olduğu durumlarda bunların kullanımını zorunlu kılma,

i) geliştirme için kontrollü ortamların kullanımı.

Kodlama sırasında dikkate alınması gerekenler şunları içermektedir.

a) kullanılan programlama dillerine ve tekniklerine özgü güvenli kodlama uygulamaları,

b) ikili programlama, yeniden düzenleme, akran incelemesi, güvenlik yinelemeleri ve test güdümlü geliştirme gibi güvenli programlama tekniklerini kullanmak,

c) yapılandırılmış programlama tekniklerini kullanma,

d) bilgi güvenliği açıklarının kullanılmasına izin verebilecek kodu belgeleme ve programlama kusurlarını ortadan kaldırma,

e) güvenli olmayan tasarım tekniklerinin kullanımının yasaklanması (örneğin, sabit kodlanmış parolaların, onaylanmamış kod örneklerinin ve kimliği doğrulanmamış web hizmetlerinin kullanımı).

Kod çalışır hale getirildikten sonra:

a) güncellemeler güvenli bir şekilde paketlenmekte ve dağıtılmaktadır,

b) bildirilen bilgi güvenliği açıkları ele alınmaktadır,

c) hatalar ve şüpheli saldırılar günlüğe kaydedilmekte ve günlükler, kodda gerektiği şekilde ayarlamalar yapmak için düzenli olarak gözden geçirilmektedir,

d) kaynak kodu, yetkisiz erişime ve kurcalamaya karşı korunmaktedır (örneğin, tipik olarak erişim kontrolü ve sürüm kontrolü gibi özellikler sağlayan yapılandırma yönetimi araçları kullanılarak).

Harici araçlar ve kitaplıklar kullanılıyorsa kurumumuz şunları dikkate almaktadır.

a) harici kitaplıkların yönetilmesini (örneğin, kullanılan kitaplıkların ve sürümlerinin bir envanterini tutarak) ve yayın döngüleriyle düzenli olarak güncellenmesini sağlamak,

b) iyi incelenmiş bileşenlerin, özellikle kimlik doğrulama ve kriptografik bileşenlerin seçimi, yetkilendirilmesi ve yeniden kullanımı,

c) harici bileşenlerin lisansı, güvenliği ve geçmişi,

d) yazılımın bakımının yapılabilir, izlenebilir ve kanıtlanmış, saygın kaynaklardan geldiğinin sağlanması,

e) geliştirme kaynakları ve yapıtlarının yeterince uzun vadeli mevcudiyeti.

Bir yazılım paketinin değiştirilmesi gerektiğinde aşağıdaki noktalar dikkate alınmaktadır.

a) yerleşik kontrollerin ve bütünlük süreçlerinin riske atılması,

b) satıcının onayının alınıp alınmaması,

c) satıcıdan gerekli değişiklikleri standart program güncellemeleri olarak alma imkanı,

d) değişikliklerin bir sonucu olarak kurumumuzun yazılımın gelecekteki bakımından sorumlu olması durumundaki etki,

e) kullanılan diğer yazılımlarla uyumluluk.

**8.29 Geliştirme ve Kabul Aşamasında Güvenlik Testleri**

Güvenlik test süreçleri, geliştirme yaşam döngüsünde tanımlanmalı ve uygulanmaktadır.

Yeni bilgi sistemleri, yükseltmeler ve yeni sürümler, geliştirme süreçlerinde kapsamlı bir şekilde test edilmekte ve doğrulanmaktadır. Güvenlik testi, sistem veya bileşen testinin ayrılmaz bir parçası olmaktadır.

Güvenlik testi, işlevsel veya işlevsel olmayan olarak ifade edilebilecek bir dizi gereksinime göre yapılmaktadır.

Güvenlik testi aşağıdakilerin test edilmesini içermektedir.

a) güvenlik işlevleri [ör. kullanıcı kimlik doğrulaması, erişim kısıtlaması ve kriptografi kullanımı,

b) güvenli kodlama,

c) işletim sistemleri, güvenlik duvarları ve diğer güvenlik bileşenleri dahil olmak üzere güvenli yapılandırmalar,

Test planları bir dizi kriter kullanılarak belirlenmektedir. Testin kapsamı, sistemin önemi, doğası ve getirilen değişikliğin potansiyel etkisi ile orantılı olmalıdır. Test planı şunları içermektedir.

a) ayrıntılı aktivite ve test programı,

b) bir dizi koşul altında girdiler ve beklenen çıktılar,

c) sonuçları değerlendirmek için kriterler,
d) gerekirse başka eylemler için karar.

Kurumumuz, kod analiz araçları veya güvenlik açığı tarayıcıları gibi otomatikleştirilmiş araçlardan yararlanarak ve güvenlikle ilgili kusurların giderildiğini doğrulamaktadır.

Şirket içi geliştirmeler için, bu tür testler başlangıçta geliştirme ekibi tarafından gerçekleştirilmektedir. Ardından, sistemin beklendiği gibi ve yalnızca beklendiği gibi çalışmasını sağlamak için bağımsız kabul testi yapılmaktadır. Aşağıdakiler dikkate alınmaktadır.

a) beklenmeyen girdiler ve koşullar da dahil olmak üzere güvenlik kusurlarını test etmek için ilgili bir unsur olarak kod inceleme etkinliklerinin gerçekleştirilmesi,

b) güvenli olmayan yapılandırmaları ve sistem güvenlik açıklarını belirlemek için güvenlik açığı taraması yapmak,

c) güvenli olmayan kod ve tasarımı belirlemek için sızma testi gerçekleştirme.

Dış kaynaklı geliştirme ve satın alma bileşenleri için bir satın alma süreci izlenmektedir. Tedarikçi ile yapılan sözleşmeler, tanımlanmış güvenlik gereksinimlerini ele almaktadır. Ürünler ve hizmetler satın almadan önce bu kriterlere göre değerlendirilmektedir.

Sistemin kurumumuz ortamına güvenlik açıkları getirmediğinden ve testlerin güvenilir olduğundan emin olmak için test, hedef üretim ortamıyla mümkün olduğunca yakından eşleşen bir test ortamında yapılmaktadır.

**8.30 Dış Kaynak Yoluyla Geliştirme**

Kurumumuz, dış kaynak yoluyla sistem geliştirme ile ilgili faaliyetleri yönetmeli, izlemeli ve gözden geçirmektedir.

Sistem geliştirmenin dışarıdan temin edildiği durumlarda, kurumumuz gereksinimleri ve beklentileri iletmeli ve üzerinde anlaşmalı ve dışarıdan temin edilen işlerin bu beklentileri karşılayıp karşılamadığını sürekli olarak izlemeli ve gözden geçirmektedir. Kurumumuz tüm dış tedarik zincirinde aşağıdaki noktalar dikkate alınmaktadır.

a) dış kaynaklı içerikle ilgili lisans sözleşmeleri, kod sahipliği ve fikri mülkiyet hakları,

b) güvenli tasarım, kodlama ve test uygulamaları için sözleşme gereklilikleri,

c) harici geliştiriciler tarafından dikkate alınacak tehdit modelinin sağlanması,

d) çıktıların kalitesi ve doğruluğu için kabul testi,

e) kabul edilebilir minimum güvenlik ve gizlilik kapasitesi düzeylerinin oluşturulduğuna dair kanıt sağlanması (örn. güvence raporları),

f) teslimatta kötü amaçlı içeriğin (kasıtlı ve kasıtsız) varlığına karşı koruma sağlamak için yeterli testin uygulandığına dair kanıt sağlanması,

g) bilinen güvenlik açıklarının varlığına karşı koruma sağlamak için yeterli testin uygulandığına dair kanıt sağlanması,

h) yazılım kaynak kodu için emanet anlaşmaları (örneğin, tedarikçi iflas ederse)

i) geliştirme süreçlerini ve kontrollerini denetlemek için sözleşmeden doğan hak,

j) geliştirme ortamı için güvenlik gereksinimleri,

k) yürürlükteki mevzuatı (örneğin kişisel verilerin korunmasına ilişkin) dikkate alarak.

**8.31 Geliştirme, Test ve Canlı (gerçek) Ortamlarının Ayrılması**

Geliştirme, test ve canlı ortamlar birbirinden ayrılmalı ve güvenlik altına alınmaktadır.

Üretim sorunlarını önlemek için gerekli olan üretim, test ve geliştirme ortamları arasındaki ayrım düzeyi belirlenmekte ve uygulanmaktadır.

Aşağıdaki öğeler dikkate alınmaktadır.

a) geliştirme ve üretim sistemlerini yeterince ayırma ve bunları farklı alanlarda çalıştırma (örneğin, ayrı sanal veya fiziksel ortamlarda),

b) geliştirme aşamasından üretim durumuna kadar yazılımın konuşlandırılması için kuralların ve yetkilendirmenin tanımlanması, belgelenmesi ve uygulanması,

c) üretim sistemlerine ve uygulamalara yapılan değişikliklerin, üretim sistemlerine uygulanmadan önce bir test veya hazırlama ortamında test edilmesi,

d) tanımlanmış ve onaylanmış durumlar dışında üretim ortamlarında test yapmamak,

e) derleyiciler, editörler ve diğer geliştirme araçları veya yardımcı programların gerekli olmadığında üretim sistemlerinden erişilmemesi,

f) hata riskini azaltmak için menülerde uygun ortam tanımlama etiketlerinin görüntülenmesi;

g) geliştirme ve test sistemleri için eşdeğer kontroller sağlanmadıkça, hassas bilgileri geliştirme ve test sistemi ortamlarına kopyalamamak,

Her durumda, geliştirme ve test ortamları aşağıdakiler dikkate alınarak korunmaktadır.

a) tüm geliştirme, entegrasyon ve test araçlarının (yapıcılar, bütünleştiriciler, derleyiciler, yapılandırma sistemleri ve kitaplıklar dahil) yamalanması ve güncellenmesi,

b) sistemlerin ve yazılımın güvenli konfigürasyonu,

c) ortamlara erişimin kontrolü,

d) ortamdaki değişikliğin ve burada saklanan kodun izlenmesi,

e) ortamların güvenli izlenmesi,

f) ortamların yedeklerini almak.

Tek bir kişi, ön inceleme ve onay olmaksızın hem geliştirme hem de üretimde değişiklik yapma yeteneğine sahip olmamaktadır. Bu, örneğin erişim haklarının ayrılması veya izlenen kurallar aracılığıyla gerçekleştirilebilir. İstisnai durumlarda, yetkisiz değişiklikleri tespit etmek ve bunlara göre işlem yapmak için ayrıntılı günlük kaydı ve gerçek zamanlı izleme gibi ek önlemler alınmaktadır.

**8.32 Değişiklik Yönetimi**

Bilgi işleme tesisleri ve bilgi sistemlerindeki değişiklikler, değişiklik yönetimi proseslerine tabi olmaktadır.

Yeni sistemlerin tanıtılması ve mevcut sistemlerdeki büyük değişiklikler üzerinde anlaşmaya varılan kuralları ve resmi bir belgeleme, şartname, test, kalite kontrol ve yönetilen uygulama sürecini takip etmektedir. Tüm değişikliklerin tatmin edici kontrolünü sağlamak için yönetim sorumlulukları ve prosesleri yürürlükte olmaktadır.

Değişiklik kontrol prosesleri, erken tasarım aşamalarından sonraki tüm bakım çabalarına kadar tüm sistem geliştirme yaşam döngüsü boyunca bilgi işleme tesislerinde ve bilgi sistemlerinde bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için belgelenmekte ve uygulanmaktadır.

Mümkün olan her yerde, BİT altyapısı ve yazılımı için değişiklik kontrol proseesleri entegre edilmektedir.

Değişiklik kontrol prosesleri şunları içermektedir:

a) tüm bağımlılıkları dikkate alarak değişikliklerin potansiyel etkisini planlamak ve değerlendirmek,

b) değişikliklerin yetkilendirilmesi,

c) değişiklikleri ilgili taraflara iletmek,

d) değişiklikler için testler ve testlerin kabulü,

e) dağıtım planları dahil olmak üzere değişikliklerin uygulanması;

f) geri dönüş prosesleri dahil olmak üzere acil durum ve beklenmedik durum hususları,

g) yukarıdakilerin tümünü içeren değişikliklerin kayıtlarını tutmak,

h) işletim belgelerinin ve kullanıcı proseslerinin uygun kalması için gerektiği şekilde değiştirilmesinin sağlanması,

i) BİT süreklilik planlarının ve müdahale ve iyileştirme proseslerinin uygun kalması için gerektiği şekilde değiştirilmesinin sağlanması

**8.33 Test Bilgisi**

Test bilgileri uygun şekilde seçilmekte, korunmakte ve yönetilmektedir.

Test bilgileri, test sonuçlarının güvenilirliğini ve ilgili operasyonel bilgilerin gizliliğini sağlayacak şekilde seçilmektedir. Hassas bilgiler (kişisel olarak tanımlanabilir bilgiler dahil) geliştirme ve test ortamlarına kopyalanmamaktadır.

Test ortamı şirket içinde veya bir bulut hizmetinde oluşturulmuş olsun, test amacıyla kullanıldığında operasyonel bilgilerin kopyalarını korumak için aşağıdaki yönergeler uygulanmaktadır.

a) operasyonel ortamlara uygulananlarla aynı erişim kontrol prosedürlerini test ortamlarına uygulamak,

b) operasyonel bilgilerin bir test ortamına her kopyalanmasında ayrı bir yetkiye sahip olmak,

c) bir denetim izi sağlamak için operasyonel bilgilerin kopyalanması ve kullanılmasının günlüğe kaydedilmesi,

d) test için kullanılıyorsa hassas bilgileri kaldırarak veya maskeleyerek koruma,

e) test bilgilerinin yetkisiz kullanımını önlemek için test tamamlandıktan hemen sonra bir test ortamından çalışma bilgilerinin uygun şekilde silinmesi.

Test bilgileri güvenli bir şekilde saklanmakta (aksi takdirde geçersiz sonuçlara yol açabilecek kurcalamayı önlemek için) ve yalnızca test amacıyla kullanılmaktadır.

**8.34 Tetkik Testi Sırasında Bilgi Sistemlerinin Korunması**

İşletim sistemlerin değerlendirilmesini içeren tetkik testleri ve diğer güvence faaliyetleri, test uzmanı ve uygun yönetim arasında planlanmakta ve kararlaştırılmaktadır.

Aşağıdaki yönergelere uyulmaktadır.

a) uygun yönetim ile sistemlere ve verilere erişim için denetim taleplerini kabul etmek,

b) teknik denetim testlerinin kapsamını kabul etmek ve kontrol etmek,

c) denetim testlerini yazılım ve verilere salt okunur erişimle sınırlandırmak. Gerekli bilgileri elde etmek için salt okunur erişim mevcut değilse, testin denetçi adına gerekli erişim haklarına sahip deneyimli bir yönetici tarafından yürütülmesi,

d) erişim izni verilirse, erişime izin vermeden önce sistemlere erişim için kullanılan cihazların (örneğin dizüstü bilgisayarlar veya tabletler) güvenlik gereksinimlerinin (örneğin antivirüs ve yama) oluşturulması ve doğrulanması,

e) yalnızca sistem dosyalarının yalıtılmış kopyaları için salt okunur dışında erişime izin verme, denetim tamamlandığında bunları silme veya bu tür dosyaları denetim dokümantasyon gereklilikleri kapsamında tutma zorunluluğu varsa onlara uygun koruma sağlama,

f) denetim araçlarının çalıştırılması gibi özel veya ek işleme taleplerinin belirlenmesi ve kabul edilmesi,

g) çalışma saatleri dışında sistem kullanılabilirliğini etkileyebilecek denetim testleri yürütmek,

h) denetim ve test amaçları için tüm erişimin izlenmesi ve günlüğe kaydedilmes