
# Bilgi Güvenliği Politikaları

RHB.EK.05

Yayın Tarihi: 12.08.2021

# 1. Amaç

Bu doküman, Kuruluşta ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, ISO 22301 İş Sürekliliği Yönetim Sistemi ve Kişisel Verilerin Korunması Kanunu Teknik tedbirleri kapsamında veri ve bilgi varlıklarının güvenliğinin sağlanması, sürdürülmesi ve iyileştirilmesi için oluşturulmuş, kuruluş bünyesinde ki tüm çalışanların uyması gereken kuralların tanımlandığı üst seviye bir dokümandır.

# 2. Kapsam

Kule Verici Tesisleri İşletim Ve Teknolojileri A.Ş' ye ait BGYS, İSYS ve KVKK teknik tedbirlerini kapsar.

# 3. Kısaltmalar ve Tanımlar

**Kuruluş:** Kule Verici Tesisleri İşletim Ve Teknolojileri A.Ş

**KVKK:** Kişisel Verilerin korunması Kanunu

**BGYS:** Bilgi Güvenliği Yönetim Sistemi

**İSYS:** İş Sürekliliği Yönetim Sistemi

**Politika:** Bir Kurum, Kuruluş veya kişinin görüş, felsefe, amaç ve tutumunun belirli şekilde ifadesini, bu görüş, felsefe veya amaç doğrultusunda bir hareket planını içeren doküman tipidir.

# 4. Sorumluluk ve Yetki

| Görev | Roller |
|---|---|
| **Dokümanın Hazırlanması:** | BGYS/İSYS YT |
| **Dokümanın Onaylanması:** | Üst Yönetim |
| **Dokümanın Yayınlanması:** | BGYS/İSYS YT |
| **Dokümanın Revizyonu:** | BGYS/İSYS YT |
| **Dokümanın Uygulanması:** | Tüm Çalışanlar |

# 5. Uygulama

Bu doküman kurum içerisinde ISO 27001 bilgi ve veri güvenliğinin sağlanması ve ISO 22301 İş Sürekliliği için asgari uyulması gereken kuralları içermektedir. Aşağıdaki politikalar aşağıda belirtilen amaçları

taşımaktadır.

- Kişisel verilerin korunması için teknik tedbirleri uygulamak
- Bilgi sistemlerinde paylaşılmakta olan her türlü bilgi ve verinin güvenliğini sağlamak
- İş devamlılığını sağlamak ve güvenlik ihlalinden kaynaklanabilecek kanuni riskleri en aza indirmek
- Kurumun itibarını ve yatırımlarını korumak

Politikalar bilgi sistemleri tasarlarken veya işletirken uyulması gereken kuralları açıklamaktadır.
Bu doküman kurum içerisinde çalışan her personeli bağlayıcı niteliktedir. Politikaların ihlali durumunda gerektiğinde disiplin kuralları işletilir ve kurum içinde ihlalde bulunan adına yasal işlem yapılabilir.

## 6. E-Posta Politikası

Bu politika kurum bünyesinde kullanılan, e-posta altyapısına yönelik kuralları içermektedir. Kurum içerisinde kullanılan e-posta hesapları kurum kimliği taşımaktadır. Kurum bünyesinde oluşturulan e-posta hesaplarının tüm personel için doğru kullanımını kapsamaktadır.

### Yasaklanmış Kullanım

- Kurumumuzda e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz ve sözleşmeler ile garanti altına alınmıştır.
- Kişisel veri veya gizli bilgi içeren mailler gönderilmesi gerektiğinde şifrelenerek veya kriptolu şekilde gönderilmelidir.
- Çalışanlar kurum ile ilgili yazışmalarında kurum dışındaki e-posta hesaplarını kullanamazlar.
- Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içeriğe azami derecede özen gösterilir.
- Kurum içindeki özel kişisel veriler ve gizli bilgiler mesajlaşma yoluyla veya eklenerek kurum faaliyetleri dışında gönderilemez ve gönderildiği tespit edildiğinde disiplin prosesleri işletilir.
- Mesajlara eklenmiş çalıştırılabilir dosya içeren e-postalar alındığında hemen silinir ve kesinlikle başkalarına iletilmez.
- Mesaj içeriklerinde dosya eklerinin dışında herhangi bir link paylaşılmış ise alıcıdan geldiği teyit edilmeden açılmaz. (Alıcı ile teyitleşme, gerek telefon gerekse, adres defterinde kayıtlı olan E-Posta adresleri kontrol edilir.)
- Turkcell, Vodafone, TTNET, DHL vb. kurumları gibi gönderilen sahte fatura mailleri kesinlikle

açılmaz, bu kapsamda farkındalık mailleri yapılmaktadır.

- Spam, zincir e-posta, sahte e-posta, reklam e-posta vb. zararlı ve şüpheli postalara yanıt yazılmaz.
- Kullanıcıların kullanıcı bilgilerinin (kullanıcı adı, şifre vb) yazılmasını isteyen e-postalar alındığında derhal alıcı tarafından silinir. Durum Teknik İşletme Şefliğine yazılı olarak bildirilir.
- Kurum Çalışanları E -posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda vb.) gönderemezler.
- PTT Teknoloji tarafından sağlanan Exchange mail hizmeti kullanılmaktadır, mail üzerindeki tüm güvenlik protokolleri açık durumdadır.

## Kişisel Kullanım

- Çalışanlara verilen e-postalar kurum içi ve dışı iletişim için verilmiştir.
- Kurum dışına atılan her e-postanın atında “gizlilik notu” ve sorumluluk notu” yer almaktadır, Kurumun bu e-posta içeriğinden ve niteliğinden dolayı sorumlu tutulamayacağı belirtilmektedir.
- Personel kendi kullanımı için verilen kullanıcı adını ve şifresini başkaları ile paylaşmaz, kullanımı için başkasına veremez, tespiti halinde disiplin prosesleri işletilir.
- Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli, kurumsal mesajlara cevap vermelidir.
- Kurum çalışanları, kurumsal maillerin kurum dışındaki kişiler ve yetkisiz kişilerce görülmesini engellemelidir.
- Kurum çalışanları, kişisel maillerine kurum mailinde gizli bilgi ve kişisel veri içeren dokümanları izinsiz göndermemelidirler.
- Kişiye verilmiş olan kurumsal e-posta hesabı gerektiğinde kurumda yetkilendirilmiş kişiler (üst yönetim, Bilgi İşlem departmanı, Birim sorumluları ) tarafından denetlenebilir.

E-posta sistemi virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış e-postaları tarayacak ve gerektiğinde tehlikeleri ortadan kaldıracak virüs, gateway ve spam çözümleri bulunmaktadır.
Bilgi İşlem Departmanı mail altyapısının güvenli ve sorunsuz çalışmasından sorumludur.

## 7. Şifre Politikası

Bu politikanın amacı kurumumuzda güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve şifrenin değiştirilme sıklığı hakkında standartlar oluşturulmasıdır.

Kullanıcıların kurum içerisinde kullanmış olduğu şifreler, bilgi güvenliği kapsamında kullanıcı hesapları için ilk güvenlik katmanıdır. Kurum çalışanları ve uzak noktadan erişenler aşağıda belirtilen kurallar dâhilinde şifreleme yapmakla yükümlüdür.

- Bütün sistem seviyeli şifreler (root, administrator vb.) en az 12 ayda bir değiştirilmektedir. (Tüm çalışanlara şifrelerini değiştirmesi konusunda periyodik olarak hatırlatmalar yapılmaktadır.)
- Kullanıcılara ilk girişte random şifreler verilmektedir, bu şifreler kullanıcıya sözlü yâda yazılı olarak iletilmektedir, kullanıcılar şifrelerini sisteme tanımlanan kurallar dâhilinde ilk girişte değiştirmek zorundadırlar.
- Şifreler en az 6 karakterlidir. Büyük küçük harf ve rakamdan oluşmaktadır.
- Bütün kullanıcı seviyeli şifreler (e-posta, masaüstü bilgisayar vb.) en az 150 günde bir değiştirilmektedir.
- Daha önce kullanılmış son 2 şifre kullanıcı tarafından tanımlanamamaktadır.
- Bilgi İşlem departmanı, her sistem için farklı kendi şifresini kullanmaktadır.
- Kritik bilgisayarlar da harddisk şifreleme veya bitlocker kullanılmaktadır.
- Şifreler e-posta veya herhangi bir elektronik forma eklenmemektedir.
- Kullanıcılar şifrelerini korumaktan sorumludurlar.

## 8. Anti-Virüs Politikası

Bu politika kurumumuz içindeki bütün bilgisayarları ve mobil cihazları kapsamaktadır. Bunlar tüm masaüstü ve dizüstü bilgisayarlar, sunucular ve mobil cihazlardır. (Cep telefonları, Tabletler vb.)

Tüm bilgisayarlar merkezi yönetimli anti-virüs yazılımı yüklüdür, sunucu tarafında antivirüs kullanılmaktadır, güncellemeleri otomatik olarak yapılmaktadır. Sistem yöneticileri ve kullanıcılar anti virüs yazılımının sürekli olarak çalışır durumda olmasından ve güncellenmesinden sorumludur. Kullanıcılara bilgisayarından anti virüs yazılımını kaldırmaları konusunda uyarılar yapılmış ve

kaldırmaları engellenmiştir.
Virüs bulaşan cihazlar sistem yöneticileri tarafından temizlenerek ağa tekrar bağlanmalıdır. Kullanıcı Bilgi İşlem Sorumlularına, sorunun kaynağının tespiti için hangi işlemleri yaptığı konusunda bilgi vermelidir.

## 9. İnternet Erişim ve Kullanım Politikası

Bu politikanın amacı internet kullanıcılarının güvenli internet erişimi için gerekli olan kuralları kapsamaktadır.

- Kurumun içerişinden kullanıcıların internet erişimleri Fortigate güvenlik duvarı üzerinden sağlanmaktadır.
- Güvenlik gereksinimleri sebebi ile misafir networkü bulunmamaktadır.
- Yasa dışı sitelere erişim sağlamak yasaklanmış ve bloklanmıştır, buna rağmen erişim sağlanması durumunda disiplin prosesleri işletilir.
- Gerektiğinde port bazlı erişimler yasaklanabilir veya kontrollü olarak verilebilmektedir.
- Kurum tarafından onaylanmamış yazılımlar bilgisayarlara kurulmamaktadır.
- Üçüncü kişilerin kurum içerisinden internet ihtiyaçlarına gizlilik ve güvenlik esasları doğrultusunda izin verilmemektedir.
- 5651 sayılı yasaya uygun olarak zaman damgalı loglar minimum 2 yıl saklanmaktadır
- Dışarıdan içeriye gelecek saldırılar için güvenlik duvarı ile kontrolü sağlanmaktadır
- Güvenlik duvarı üzerinde bulunan Application Control, Web Filter, URL Filter, DNS Filter, Virus scanner, SSL Inspection özellikleri açık ve günceldir.

## 10. Sunucu Güvenlik Politikası

Bu politikanın amacı kurum bünyesindeki sunucuların temel güvenlik yapılandırılmasının nasıl olması gerektiğini belirtir. Bu temel güvenlik yapılandırmalarının yapılmasından ve işletilmesinden Bilgi İşlem Sistem Yöneticisi sorumludur.

### Genel Konfigürasyon Kuralları

- Sunucular üzerindeki kullanılmayan servisler ve uygulamalar kapatılmaktadır.

- Uygulama servislerine erişimler loglanmakta ve erişim kontrol logları incelenmektedir.
- Sunucu üstünde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının, yönetim yazılımlarının vb. koruma amaçlı yazılımların güncellik kontrolleri sürekli yapılmaktadır.
- Anti virüs güncellemeleri otomatik, yama güncellemeleri sistem yöneticileri tarafından kontrollü şekilde yapılmaktadır. Bu yama güncelleme işlemi bir test ve onay mekanizmasından geçirilerek uygulanmaktadır.
- Sistem ve uygulama yöneticileri gerekli olmadıkça "administrator", "root" vb. kullanıcı hesaplarını kullanmamaktadırlar, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmaktadırlar, önce kendi kullanıcı hesapları ile giriş yapıp daha sonra genel yönetici hesaplarına geçiş yapmaktadırlar.
- Sunucular fiziksel olarak korunmuş sistem odalarında korunmaktadırlar.
- Güvenlik amaçlı sunucu erişimleri dışarıdan içeri doğru RDP erişimi kapalıdır.
- Sunucu tarafında erişim için IP kısıtlaması bulunmaktadır.

### İşletimsel Sistemler Üzerine Yazılım Kurulumu

- İşletimsel sistemler üzerine yazılım kurulumunda sadece sistem tarafında yer alan sorumlularda yetki bulunmaktadır.
- İşletimsel sistemler üzerine yapılan işlemler loglanmaktadır.
- Üçüncü parti destek firmalarına sözleşmesi olsa dahi yazılım kurulumu izni verilmemektedir.

## 11. Ağ Cihazları Güvenlik Politikası

Bu politika kurumun ağındaki varlıkların sahip olması gereken minimum güvenlik yapılandırılmalarını tanımlamaktadır.

- Ağ cihazları dışarıdan istenmeyen müdahaleleri engellemek için fiziksel olarak kilitli odalarda ve kabinlerde muhafaza edilmektedir, kabinler cihazların çalışması için gerekli ortamı sağlamaktadır.
- Ağ cihazlarını yangın, su baskını, deprem gibi tehlikelerden korumak için yangın algılama ve söndürme sistemleri, ortam sıcaklık, nem, su gibi faktörleri bildiren bildirim sistemleri mevcuttur.

- Yönlendirici giriş portuna gelen geçersiz IP adresleri yasaklanmıştır.
- Yönlendirici ve anahtarlarda çalışan güvenli web servislerine erişim sadece Bilgi Teknolojileri sorumlularına ve yönetime verilmektedir.
- Yazılım ve firmware'ler ilk önce OS platformlarına ait test ortamlarında test edildikten sonra çalışma günlerinin veya saatlerinin dışında çalışan yapıya canlı ortamına taşınmaktadır.
- Yedek yapıda ethernet hattı bulunmaktadır.

## 12. Ağ Yönetimi Politikası

Ağ yönetim politikası, ağın güvenliği ve sürekliliğini karşılayan kuralları belirlemektedir,

- Ağ üzerinde kullanıcının erişebileceği servislerde yetkilendirmeler mevcuttur.
- Sınırsız ağ dolaşımı engellenmiştir.
- Ağ güvenlik duvarı ile korunmakta ve güvenlik duvarı üzerindeki tüm güvenlik protokolleri güncel ve aktif durumdadır.
- İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmıştır (Firewall vb).
- Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmıştır.
- Ağ bağlantıları periyodik olarak kontrol edilmektedir.
- Dışardan yapılan bağlantılarda içeri sadece VPN ile giriş sağlanabilmektedir. VPN hesapları sadece "özel yetkili kullanıcılara" verilmektedir
- Ağ üzerindeki yönlendirme kontrol edilmektedir.
- Ağa bağlı bütün makinelerde kurulum ve yapılandırma parametreleri kurumun güvenlik politika ve standartlarıyla uyumlu olarak yapılmaktadır.
- Ağ üzerinde gerçekleşen işlemler izlenmekte ve loglanmaktadır.
- Kullanılan ağ üzerinde kullanıcılar ve sunucular ayrılmıştır
- Ağ hizmetlerine erişim için kimlik doğrulama sistemleri kullanılmaktadır. (Mac izolasyonu)
- Dışarıdan gelen güvensiz trafik tamamen engellenmektedir.
- Loglar firewall ile incelenmektedir.
- Ağ ve bağlı sistemlerinin iş sürekliliğini sağlamak için yedeklilik sağlanmaktadır.

### Halka Açık Ağlardaki Uygulama Hizmetlerinin Güvenliğinin Sağlanması

- Kurum içinde güvenlik sebebi ile misafir ve ofis networkleri ayrı zone'larda çalışmaktadır..
- Web sitesi üzerinde SSL sertifikası bulunmaktadır,
- Halka açık ağlardan alınacak kişisel verilerde rıza gerekli veri işlemelerinde rıza metni yer almaktadır.

## 13. Uzaktan Erişim Politikası

Bu politikanın amacı herhangi bir yerden kurumun ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar yetkisiz kullanımdan dolayı kuruma gelebilecek potansiyel zararları en aza indirmek için tasarlanmıştır.

- Uzaktan erişim güvenliği sıkı bir şekilde denetlenmektedir, sadece görevlendirilmiş Bilgi Teknolojileri yöneticisi, yetkili personeli veya dışarıdan destek ekipleri tanımlanmış kişiler kullanıcı adı/şifresi ile yerel ağa güvenli şekilde erişim sağlamaktadırlar (VPN)
- Uzaktan bağlanacak ofisler ve kullanıcılar ssl vpn üzerinden kurum ağına ve kaynaklara ulaşabilmektedir.
- Yönetimin onayı olmadan dışarıdan Kurum bünyesine erişim hakkı verilmemektedir.
- Uzaktan erişim ile kuruma erişen bütün bilgisayarlar en son güncellenmiş anti virüs yazılımına sahip olmalıdır.
- Dışardan hizmet alınan kuruluşlara uzaktan erişim hakları süreli olarak tanımlanmaktadır.
- Uzaktan erişim yapan kullanıcı hareketleri loglanmaktadır.
- Uzaktan erişim hakkı tanımlanan kullanıcıların kullanıcı adı ve şifrelerine yönelik otomatik hatırlama özelliği kapalıdır.
- Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların kimlikleri ve hesapları kapatılmakta ve/veya dondurulmaktadır.
- Ayrıcalıklı destek programlarının kullanımında sadece sistem yöneticisi yetkilidir, içerde yapılan destek bağlantılarında Lansweeper üzerinden erişimler sağlanmaktadır.

## 14. Kablosuz İletişim Politikası

Bu politika kurum bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını (dizüstü bilgisayar, cep telefonları, el terminalleri… vs.) kapsamaktadır. Kablosuz cihazların gerekli güvenlik tedbirleri alınmaksızın kurumun bilgisayar ağına erişimini engellemeyi amaçlamaktadır.

- Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmaktadır.
- Erişim cihazlarındaki firmware'ler düzenli olarak güncellenmektedir.
- Erişim cihazları, fiziksel olarak kolay erişilebilecek bir yerde olmaması sağlanmıştır.
- Erişimler için güçlü bir şifre belirlenmiş olup manüel olarak yılda bir şifre değiştirilmesi ile sağlanmaktadır.
- İzinsiz kablosuz ağ erişim durumunda MAC engelleme yapılmaktadır.
- Erişim cihazlarında yetkilendirme ve kurum prosedürleri gereği yasaklı adreslerde bloklama bulunmaktadır.
- Kurum envanter listesinde bulunmayan cihazların Kurum kablosuz ağına bağlanmaları Kurum politikaları gereği yasaklanmıştır.

## 15. Yazılım Donanım Envanteri Oluşturma Politikası

Bu politika kurumun sahip olduğu donanım ve yazılımların envanterinin oluşturulması ile ilgili kuralları belirlemektedir.
Bu politika kurum bünyesinde kullanılan bütün donanım ve yazılımları (PC, Sunucu, yazıcı, işletim sistemleri, vs.) kapsamaktadır. Bu politikanın uygulanmasından BT ekibi sorumludur.

- Kurumda yer alan bütün ekipmanların envanteri oluşturulmalı ve güncel tutulmalıdır.
- Oluşturulan envanter tablosunda minimum şu bilgiler olmalıdır; Varlık Grubu, Ayırt Edici Kimlik No, Marka/Model, Varlık Sahibi, bulunduğu Lokasyon.
- Oluşturulan tablolar güvenli bir ortamda sadece yetkili kişilerin gözetiminde takip edilmelidir.
- Bilgi güncelleme varlık eklemelerinde sürekli ve denetimi periyodik olarak BT ekibi (en az yılda 1 kere) tarafından yapılacaktır.
- Envanter bilgisi doğru bir şekilde tutulmalıdır. Eksik veya yanlış envanter bilgisi ileride yapılacak

donanım ve yazılım değişikliklerinde sağlıklı karar alınmasını engelleyebilir.

- Envanter bilgileri periyodik olarak yılda bir kontrol edilmelidir. Envanter bilgisi eksikliğinden dolayı oluşacak hırsızlık veya değişim ciddi kayıplara yol açabilir.

## 16. İş Sürekliliği Politikası

Kurumda yer alan sistemlerin ve kritik kişilerin sürekliliğini sağlamak amacı ile yedeklilik yapısı uygulanmaktadır.

- Bilgi sisteminin kesintisiz çalışması için gereken önlemler alınmış ve yedek sistemler tasarlanmıştır.
- Acil durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır:
  - Seviye A (Bilgi Kaybı): Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi.
  - Seviye B (Servis Kesintisi): Kurumsal servislerin kesintisi veya kesintiye yol açabilecek durumlar.
  - Seviye C (Şüpheli Durumlar): Yukarıda tanımlı iki seviyedeki durumlara sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.
- Her bir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin kuruma getireceği kayıplar ve bu risk oluşmadan önce ve oluştuktan sonra hareket planları tanımlanmıştır
- BT kapsamında yaşanan acil durumlarda Kurum çalışanları, Bilgi İşlem bölümüne haber vermekte ve gerekli aksiyonlar ivedilikle alınmaktadır.

## 17. Kimlik Doğrulama ve Yetkilendirme Politikası

Bu politika kurumun bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarını tanımlamaktadır. Bilgi sistemlerine erişen kurum çalışanları ve 3. taraf kullanıcılar bu politika kapsamındadır.

- Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri belirlenerek denetim altında tutulmaktadır.
- Kurum içerisindeki tüm kullanıcıların kendilerine özel kullanıcı adı ve şifresi tanımlanır.
- Başarısız kimlik ve şifre denemeleri sistemlerce loglanmaktadır.
- Yetkilendirmeler yetki matrisi kapsamında verilmektedir.

- Gerekli minimum yetkinin verilmesi prensibi benimsenmektedir.
- Erişim ve yetki seviyeleri belirli dönemlerde kontrol edilip gerekli durumlarda güncellenmektedir.
- Tüm kullanıcılar kurum tarafından kullanımlarına tahsis edilen sistemlerdeki veri ve bilgilerin güvenliğinden sorumludur.
- Kullanıcı hareketlerini izleyebilmek için her kullanıcıya kendisine ait bir kullanıcı hesabı açılmaktadır.
- Kullanıcıların hesapları ile yaptıkları hareketler loglanmaktadır.

## 18. Veri Tabanı Güvenlik Politikası (Güvenli Sistem Mühendisliği Prensipleri)

Bu politika, kurumdaki veri tabanı sistemlerinin kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlar. Tüm veri tabanı sistemleri bu politikanın kapsamındadır.

- Veri tabanı sistemleri ve sorumlular belirlenmiştir.
- Veri tabanlarına erişimler yetkilendirilmiştir.
- Veri tabanları ortamlarına erişimler kısıtlanmış ve güvenli alanlarda muhafaza edilmektedir.
- Veri tabanı sistemlerine erişim logları tutulmakta, gerektiğinde Bilgi İşlem departmanı tarafından kontrol edilmektedir.
- Veri tabanı yedekleme politikaları oluşturulmuş, yedeklemeden sorumlu sistem yöneticileri belirlenmiş ve yedeklerin düzenli olarak alındığı kontrol edilmektedir.
- Veri tabanı erişim politikaları “Kimlik doğrulama ve yetkilendirme” çerçevesinde oluşturulmuş olup erişim için belirlenmiş yazılım üzerinden kimlik doğrulaması yapılarak erişim sağlanır.
- Hatadan arındırma, bilgileri yedekten dönme kuralları “ İş sürekliliğine” uygun, kurumun ihtiyaçlarına yönelik olarak oluşturulmuştur.
- Bilgilerin saklandığı sistemler, fiziksel güvenliği sağlanmış sistem odalarında tutulmaktadır.
- Yama ve güncellemeler yapılmadan önce yedek ve ortam güvenliği sağlanmakta, sonrasında ilgili güncellemeler gerçekleştirilmektedir.
- Veri tabanı sunucularında sadece orijinal veri tabanı yönetim yazılımları kullanılmakta, bunun dışında ftp, telnet vb. bağlantılara kapanmıştır.
- Veri tabanı sunucusuna ancak zorunlu hallerde root ve administrator olarak bağlanılmaktadır. Root ve administrator şifresi sadece yetkili kişide bulunmaktadır.

- Bütün kullanıcıların yaptıkları işlem logları kayıt altına alınmaktadır.

## 19. Değişim Yönetimi Politikası (Güvenli sistem mühendisliği prensipleri)

Kurum bilgi sistemlerinde yapılması gereken yapılandırma değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesine yönelik politikaları belirlemektedir.

- Bilgi sistemlerinde değişiklik yapmaya yetkili personel, Bilgi İşlem departmanındaki sistem yöneticileri ve Bilgi İşlem Sorumlusudur. Yapılacak değişiklikler Bilgi İşlem Sorumlusunun onayı ile yapılır.
- 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.

## 20. Bilgi Sistemleri Yedekleme Politikası (Güvenli sistem mühendisliği prensipleri)

Bu politika kurumun bilgi sistemleri yedekleme politikasının kurallarını tanımlamaktadır. Tüm kritik bilgi sistemleri ve bu sistemleri işletilmesinden sorumlu çalışanlar bu politika kapsamındadır.

- Operasyonel ve kritik sistemlerin yedekleri iş sürekliliği planı dahilinde otomatik olarak alınmaktadır
- Alınan yedeklerin testleri periyodik olarak yapılmaktadır.
- Kritik sistemler Veeam Backup ile periyodik olarak yedeklenmektedir. Yedekler ayrı bir sunucuda tutulmaktadır.
- Tüm kritik sunucularda offline replikasyonu bulunmaktadır.
- Bilgi sistemlerinde oluşabilecek hatalar karşısında, sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en aza indirmek için kurumsal veriler düzenli olarak yedeklenmektedir.
- Yedekleme konusuyla ilgili olarak hangi sistemlerin ne kadar sıklıkla yedeklerinin alınacağı Bilgi İşlem departmanı tarafından belirlenmekte ve dokümante edilmektedir.
- Yedekleme ortamları düzenli periyotlarla test edilmekte ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmaktadır.

- Güvenlik ve gizlilik bakış açısı paralelinde farklı lokasyonlara da yedek alınmaktadır,
- Yedekler ile ilgili hangi yedeklerin, hangi program ile hangi sıklıkta ve kim tarafından alındığı bilgileri yedekleme listesinde belirtilmiştir.

## 21. Kapasite Yönetimi

Kurumumuzda sistemlere ait tüm kapasiteler program ara yüzleri ile takip edilmektedir, kapasite artırımı ile ilgili sistem yöneticisi ihtiyaçları üst yönetime bildirmekte ve onay dâhilinde artırımlar yapılmaktadır.

## 22. Mobil Cihaz Politikası

Mobil cihazların kullanımından kaynaklanan risklerin yönetimi ve destekleyici güvenlik önlemleri, tedbirleri almak için bu politika yazılmıştır.

### Kurumsal Kullanım

- Kurum içerisinde laptop ve masaüstü cihazlar kullanılmaktadır.
- Mobil cihazların uygun kullanımı ile ilgili tüm kullanıcılardan taahhüt alınır.
- Kuruma ait taşınabilir mobil cihazları, öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
- Kullanıcılar tüm cihazlarda şifre, antivirüs gibi güvenlik tedbirlerini devre dışı bırakamazlar.
- Kritik bilgisayarlarda bitlocker ve harddisk şifreleme mevcuttur, şifreler Bilgi İşlem departmanınca paylaşılır ve saklanır.
- Kullanıcılar kurum ağında iken mevcut protokollere uygun olarak hareket etmek zorundadırlar, Kurum dışında iken de kurumsal değerlere zarar verecek ve risk ihtiva eden hareketlerden kaçınmak zorundadırlar, olumsuz bir senaryoda sorumluluk kullanıcıdadır, olumsuz durumlarda disiplin süreçleri işletilir.
- Taşınabilir bilgi işleme cihazları gözetimsiz bırakıldıklarında mutlaka fiziksel olarak güvenli bir yerde veya şekilde saklanmalıdır.
- Mobil cihazlar gözetimsiz bırakıldığında otomatik olarak kilitlenmektedir, otomatik kilit zamanı öncesinde gözetimsiz bırakılma durumunda kullanıcı tarafından kilitlenmelidir.

### Uygunsuz Kullanım

- Kuruma ait taşınabilir mobil cihazları hiçbir şekilde yasa dışı, kurum çıkarlarıyla çelişecek veya normal operasyon ve iş aktivitelerini engelleyecek şekilde kullanılamaz.
- Kurum gizli bilgisi veya kişisel veriler taşınabilir mobil cihazlarında şifresiz olarak saklanamaz.
- Kurum tarafından onaylanmış şifreleme yöntemi kullanıcı tarafından uygulanmalıdır.
- Kurum tarafından onaylanmış şifreleme yöntemleri ve güvenli aktarım metotları kullanılmadan kurum bilgisi, kişisel veri taşınabilir mobil cihazlarından transfer edilemez veya bu cihazlara kablosuz olarak aktarılamaz.
- Güvenlik sebebi ile gizli bilgiler ve kişisel veriler masaüstünde saklanmamalı ve yedeklenmemelidir.
- Dışardan aktarılan bilgiler ve kişisel veriler zararlı yazılımlara karşı taramadan geçirilmeden kurum ağına aktarılamaz.

### İzleme

- Kurum, taşınabilir mobil cihazları kullanılarak yapılan tüm işlemleri izleme hakkını KVKK ve ilgili sair mevzuatlar sebebi ile saklı tutar.
- KVKK teknik tedbirler sebebi ile kişisel veri ve gizli bilgiler üzerinde yapılan işlemlerin izlenmesi, kurallar belirlenerek kontrol edilmesi Kurumun yükümlülüklerindendir, bu kurallar gizli bilginin ve kişisel verinin kritikliğine göre kurum tarafından belirlenmektedir.
- Kurum, kullanıcının taşınabilir mobil cihazları ile gerçekleştirdiği aktivitelerle ilgili emniyet kuvvetleri gibi kolluk kuvvetlerine ve yasal taraflara kullanıcının izni olmadan paylaşma hakkını saklı tutar.

## 23. Güvenli İmha ve Silme Politikası

Kurum içerisinde yer alan gizli bilgi, kişisel veri ve kurumsal diğer veri ve bilgilerin idari ve hukuki hükümlere göre belirlenmiş sürelere göre muhafaza edilmesi gerekmektedir.

- Kurum bünyesinde yer alan bilgi ve veriler saklama süreleri sonunda uygun şekilde imha edilir.
- Kâğıt ortamında yer alan bilgi ve veriler okunamayacak şekilde imha ekipmanlarında parçalanarak yok edilir.
- HDD ortamında olanlar yazılımlar ile geri dönülemez olarak formatlanır ve kırılarak parçalanır, bu işlem Bilgi İşlem departmanı, sorumluluğunda ve nezaretinde yapılır.
- Bilgisayarların elden çıkarılması halinde içindeki HDD in silinmiş olması veya imhası mutlaka teknik işletme şefliği tarafından kontrol edilerek emin olunur.

- Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
- İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
- İmha edilen materyallar elektronik atıklar kapsamında yetkili kuruluşlara teslim edilmelidir.
- İmha süreçleri tamamlanmamış kağıt veya soft bilgilerin saklandığı ortamların güvenliği sağlanmalıdır.

## 24. Temiz Ekran Temiz Masa Politikası

Bu politika kurumun çalışma ortamında ekran ve masa kullanımına ilişkin kurallarını tanımlamaktadır. Tüm bilgi sistemleri ve bu sistemleri işletilmesinden sorumlu çalışanlar bu politika kapsamındadır.

- Kullanıcılar, kurum içerisinde kullanılan tüm platformlara kendi kullanıcı adı ve şifreleri ile giriş yaparlar ve şifrelerini kesinlikle başkaları ile paylaşmazlar.
- Kullanıcılar ekranlarının başından süre bağımsız ayrılacakları zaman ekranlarını kilitlemelidirler. Bu bilgiler çalışanlara uyum eğitimiyle ve farkındalık eğitimleri ile verilir.
- Ekranlar hareketsiz bırakılması durumunda 10 dakika sonra otomatik olarak kilitlenecek şekilde kurumda yapılandırılmıştır.
- Masalar üzerinde, gizli bilgi, kişisel veri içeren hiç bir evrak bırakılmaz.
- Gizli bilgi ve kişisel veri içeren dokümanlar ile mutlaka kapalı dosyalar içinde çalışılır ve işlem bitince hemen güvenli alana kaldırılarak muhafaza edilir.
- Masa üzerinde yer alan çalışma evrakları, yazı görünür biçimde bırakılamaz, ters çevirim yapılarak yazıların ( bilginin ) görünmemesi sağlanır.
- Masa düzeni, tertibi ve gizliliği kullanıcı sorumluluğundadır.
- Dökülerek zarar verebileceği nedeniyle, masalar üzerinde çay, kahve, su vb. İçecek ile yiyecek madde bulundurulmaz, güvenli alanlara (Muhasebe, İK ve BT alanları vb.) yiyecek içecek sokulmaz. Bu odalara giriş de kilit ile kontrol edilmektedir.
- Bilgisayar kasaları üzerine, sıvı içecekler, yiyecekler, kitaplar, dosyalar vb. konulmamalıdır.
- Masalarda gizli bilgi ve kişisel veri kapsamında olan hiçbir bilgi içeren evrak – doküman bulundurulmaz. Bu türden ortamlar, kendileri için belirlenmiş dosyalar ve kilitli dolaplar içinde muhafaza edilir.

# 25. Bilgi Transferi Ve Fiziksel Ortam Aktarımı Politikası

Kurum dışına gizli bilgi veya kişisel veri transferi yapıldığında aşağıdaki kurallar uygulanmaktadır;

- Kişisel veri veya gizli bilgi içeren transferler mail üzerinden yapıldığında mutlaka şifrelenmelidir.
- Kişisel veri veya gizli bilgi içeren transferler kurye / kargo ile yapıldığında mutlaka sağlayıcı ile gizlilik sözleşmesi imzalanmalıdır.
- Kurum içerisinde gizli bilgi ve kişisel veri dolaşımı izlenmekte ve kurallar ile düzenlenmektedir.
- Bilgi Teknolojileri kapsamında yer alan donanımlar ve bilgi içeren diğer ekipmanların transferleri BT ekibi ve sorumluları tarafından yapılmaktadır.
- Önemli etkiye sahip bilgi ve varlıkların taşınmasında/aktarımında üçüncü kişiler aracılık edilmez ve kişiye özel bilgi, ilgili kişiye bizzat Bilgi İşlem departmanı tarafından sağlanır.

## Taşınabilir ortam Yönetimi

Bilgisayarlar üzerinde taşınabilir ortamların ( usb, flash bellek, harici disk v.b ) kullanımlarında sadece tanımlanan ve izin verilen ekipmanlarda müsaade edilmiştir, bu izinler mutlaka birim yöneticisi veya üst yönetim izni dâhilinde sağlanmaktadır.
Kullanımdan doğan riskler risk analizinde tanımlanarak üst yönetimce kabul edilmiştir.

## Transfer Protokolleri

Kurum içerisinde sosyal medya platformları (linkedin, facebook v.b), transfer programları (wetransfer v.b) gibi ortamlarda dosya ekleyerek göndermek prosedürel olarak yasaktır.
Kurum içerisinde ayrıcalıklı haklar tanınan kullanıcıların bu hareketleri izlenmekte ve loglanmaktadır, izinler birim yöneticisi veya üst yönetim izni dahilinde sağlanmaktadır.

## Veri Kaybı Önleme Yazılımları

Kurum içerisinde kişisel verilerin kontrol edilmesi, izlenmesi ve güvenliğinin sağlanması adına veri kaybı önleme yazılımları kritik verilerin ve özel nitelikli kişisel verilerin işlendiği kullanıcılar bazında kullanılmaktadır.

# 26. Güvenli Alanlarda Çalışma Usulleri Politikası

Kurum içerisinde kullanıcı konumlandırmaları bilginin her türlü gizlilik ve güvenliğini sağlayacak şekilde tasarlanmıştır.

- Kullanıcı bilgisayarları bilginin gözle çalınmasını engelleyecek şekilde konumlandırılmıştır.
- Kullanıcıların Kurum içerisinde konumlandırılması İSG şartları dikkate alınarak tasarlanmıştır.
- Kritik sistemlerin muhafaza edildiği odaların sorumluluğu ve anahtarları Bilgi İşlem departmanında yer almaktadır.
- Kritik sistemlerin muhafaza edildiği ortamlarda yetkilendirme mevcuttur, yetkiler üst yönetim onayı ile verilmektedir.
- Kritik sistemlerin muhafaza edildiği ortamlarda izleme ve kayıt sistemleri yer almaktadır.
- Kritik sistemlerin muhafaza edildiği ortamlarda yangın algılama ve söndürme sistemleri mevcuttur.
- Kritik sistemlerin muhafaza edildiği ortamların iklimlendirme sistemleri mevcuttur.
- Kritik sistemlerin muhafaza edildiği ortamların ısı, nem, sıvı gibi değişimlerini bildiren bildirim sistemleri mevcuttur.
- Kritik sistemlerin sürekliliğini sağlamak için yedekli yapı kurgulanmıştır.
- Kullanıcı bilgisayarları ve sunucular ekipmanların olası göreceği zararları önleyecek şekilde dizayn edilmiştir.
- Bilgi sistemleri ekipmanları kilitli güvenli alanlarda bulunmaktadır

## 27. Erişim Kontrol Politikası

Kurumda Kişisel Verilerin Korunması Kanunu ve Bilgi Güvenliği kapsamında erişim kontrolü; tanımlama, yetkilendirme, kimlik doğrulama, izlenebilirlik ve kontrol süreçleri ile uygulanmaktadır.
Buna göre tanımlama ile kurumda yetkilerin tanımlanması, kimlik doğrulama ile sisteme hangi öznelerin hangi kullanıcı isimleri ile giriş yapabileceği, yetkilendirme ile öznelerin hangi işlemleri yapmaya veya hangi nesnelere erişmeye yetkili olduğu ve izlenebilirlik ile öznelerin sistemde hangi işlemleri yaptıklarının veya hangi nesnelere eriştiklerinin bilinmesi ve gözlenebilmesi sağlanmaktadır.

### Kimlik Tanımlama

- Kurumda kullanıcı hesapları İnsan Kaynakları tarafından yapılan bildirimler ile sistem yöneticisi tarafından Active Directory üzerinden tanımlanmaktadır.
- Kurumda kullanılan diğer programlarda(muhasebe programı, erp, EBYS v.b) erişimler ilgili yöneten departman sorumluluğunda tanımlanır.
- Kullanıcılar, tanımlanan hesaplarına ilk girişlerinde şifreleri belirlenen kurallar dahilinde ilk girişte değiştirmeye zorlanmaktadır.

- Kurumda bilgi varlıklarına ve verilere erişimi olan kullanıcılar için kendine ait ve benzersiz olarak tanımlanmış hesapları (kullanıcı adı) oluşturulmuştur.
- Her kullanıcı kendisine ait kimliği ve şifresini korumaktan sorumludur.
- Kullanıcıların bir başkasına ait kimliği ve şifreyi kullanarak kurum bilgi varlıklarına erişimleri yasaklanmıştır.
- Kullanıcılar hesaplarını başkalarıyla paylaşamazlar.
- Kurum içerisinde görev değiştiren kullanıcıların hesapları iş gereksinimlerine göre kaldırılır veya yeniden düzenlenir.
- 90 gün kullanılmayan kullanıcı hesapları devre dışı kalacaktır, gerekli durumlarda hesaplar şifreleri değiştirilerek yönlendirilebilir.
- Kurumla ilişiği kesilen kullanıcıları İK tarafından teknik işletme şefliğine bilgi verilerek Kullanıcı hesapları BT ekibi tarafından kaldırılır veya şifresi değiştirilerek yönlendirilir.

## Kimlik Doğrulama

- Kurumda kullanılan tüm ortamlara kullanıcılar, kullanıcı adı ve şifre kombinasyonu ile erişim sağlamak zorundadır.
- Kullanıcı başarılı ve başarısız erişimleri loglanmaktadır.
- Yeni oluşturulan kullanıcı hesaplarına ait kullanıcı adı / parolalar ilk verilişte kullanıcıya yazılı veya sözlü olarak iletilir ve anında değiştirilmesi istenir.
- Kullanıcıların erişimlerinde kullanıcı ve şifreleri gizlenecek şekilde girişler düzenlenmiştir.
- Kullanıcı hesaplarına ait parolalar oluşturulurken “Şifre Güvenliği Politikasına” uyulacaktır.
- Kullanıcılar kimlik doğrulama yaparak erişim sağladıkları sistemlerin başlarından ayrılırken sistemin erişime kapalı olmasını sağlayacaklardır.
- Başkaları tarafından öğrenildiğinden şüphelenilen parolalar hemen değiştirilecektir.

## Yetkilendirme

- Kurum içerisinde tüm yetkilendirmeler birim yöneticisi ve üst yönetim onayı ile verilmektedir.
- Kurum içerisinde gizli bilgi ve kişisel veri niteliği, sorumluluk alanı ve birimi dikkate alınarak dağıtılmaktadır.
- Kurum içerisinde verilen tüm yetkiler sistem yöneticisi tarafından 9 ayda bir periyodik olarak gözden geçirilmektedir.
- Özel olarak yetkilendirme yapılmadığı sürece tüm kişisel veri ve bilgi varlıklarına erişimler kısıtlanmıştır.
- Kullanıcılara sadece iş sorumluluklarını veya iş gereksinimlerini yerine getirmelerine yetecek kadar yetkilendirme yapılacaktır.
- Kullanıcıların yetkileri dahilinde ortamlara yaptıkları erişimler loglanmaktadır.
- Herhangi bir şekilde fazla yetkiye sahip kullanıcıların bu yetkiyi kullanarak iş sorumluluklarının veya iş gereksinimlerinin dışında bilgiye ulaşması yasaklanmıştır.

- Erişim ve yetki seviyelerinin güncelliği bilgi sistemlerindeki bir değişiklik ya da personellerle ilgili değişikliklerde teknik işletme şefliği tarafından sağlanacaktır.
- İş ilişkisi kesilen personellerin hesapları İK tarafından gelen bildirim dahilinde tüm erişim yetkileri iptal edilir.
  **Ref:** Erişim Yetki Matrisi

## Donanımlara Erişim

- Kurumun altyapı ve donanım varlıkları belirlenmiş ve Varlık Envanter Listesinde listelenmiştir.
- Varlık envanter listesinde varlıkların sahibi ve kullanıcıları belirtilmiştir.
- Donanımsal erişim hakkı varlık envanterinde belirtilen varlığın sahibine ve kullanıcısına aittir.
- Kullanıcılar bilgisayarlarına Şifre Güvenliği Politikasına uygun olarak kimlik doğrulama ile erişilecektir.
- BT kapsamında yer alan ekipmanlara erişim izinleri, sadece Bilgi İşlem Yöneticisi tarafından görevlendirilen personellere verilmektedir.
- Gerekli durumlarda Bilgi İşlem sorumlusu veya Bilgi İşlem sorumlusu tarafından yetkilendirilmiş Bilgi İşlem çalışanları erişim yetkisine sahip olurlar.

## Üçüncü Taraf Erişimleri

- Üçüncü taraflara ait Kurum /kuruluşların kurum dahilinde herhangi bir hizmet kapsamında kurumun bilgilerine ve bilgi sistemlerine erişim izni verilmeden önce riskler değerlendirilmektedir.
- Üçüncü taraflara verilecek uzak bağlantı izinlerinde üst yönetim izni alınmak zorundadır.
- Üçüncü tarafların kuruma yapacağı bağlantılarda güvenli erişim protokolleri tercih edilmek zorundadır.
- Üçüncü taraflara sağlanan vpn erişimleri süreli verilmektedir.
- Üçüncü taraflara verilecek uzak bağlantılar loglanmaktadırlar.
- Üçüncü taraflara verilen erişim izinleri minimum ayda bir kontrol edilir.
- Fiziksel erişimlerde mutlaka refakatçi eşliğinde erişimler sağlanmaktadır.
- Üçüncü tarafa ait Kurum /kuruluşların erişecekleri varlıkların güvenliğinin sağlanmasından varlığın sahibi sorumludur.
- Erişim kuralların aykırı hareket eden kişi/tarafların erişim yetkisi kaldırılır.

### Log Yönetimi

Kurum içerisinde loglar bilgi ve veri güvenliğini sağlayacak şekilde kurgulanmış ve kayıt edilmektedir.

- Erişimler 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a uygun olarak loglanmakta ve 2 yıl süre ile saklanmaktadır.
- Sistem yöneticisi logları tutulmaktadır.
- Kullanıcı audit logları tutulmaktadır.
- File server logları tutulmaktadır.
- Erişimlerde kullanıcılar, ayrıcalıklı kullanıcılar, yöneticiler, ayrıcalıklı yöneticiler, sistem yöneticileri ve operatör kayıtları kayıt altına alınmaktadır.

## 28. Fiziksel Erişim Politikası

Kurumda fiziksel güvenliğin sağlanması için gerekli güvenlik tedbirleri alınarak kayıtlar riskler paralelinde saklanmaktadır,

Bu doğrultuda kurumumuza ait lokasyonda;

- Kule de nizamiye giriş kapısı bulunmaktadır.
- Kule de girişler sadece izinler dahilinde yapılabilmektedir, ilgili kişi bilgisi ve izni ile eşlik edilerek giriş sağlanmaktadır.
- Ofis binasında danışma personeli bulunmaktadır.
- Ofis binasına otopark girişlerini kontrol eden güvenlik yer almakta ve girişler kontrollü gerçekleşmektedir.
- Her iki lokasyonda da tüm alanlarda kapalı devre kamera sistemleri mevcuttur, 7/24 izlenmekte ve kayıtlar saklanmaktadır.
- Nizamiye girişlerinde standart ziyaretçi kontrolleri güvenlik personelleri tarafından yapılmaktadır. Bina girişlerinden ziyaretçiler onaylandıktan sonra giriş sağlanmaktadır.
- Departman girişlerinde anahtar ile giriş yöntemleri bulunmaktadır.
- Ofis ana girişi kartlı sistem ile sağlanmaktadır.
- Açık alanlar, koridor ve giriş /çıkışlar kamera sistemleri ile kayıt altına alınmaktadır.
- Yerleşke içerisinde 7/24 görev yapan güvenlik personeli bulunmaktadır.
- Girişlerde güvenlik ve yasal tarafların talepleri doğrultusunda sunulmak üzere kayıtlar Kişisel Verilerin Korunması Kanunu kapsamında alınmakta ve saklanmaktadır, silme ve imha politikası doğrultusunda yok edilmektedir.

- Kritik bilgi ve verilerin bulunduğu ortamlar kilitli olarak tutulmaktadır.
- Kritik veri ve bilgilerin bulunduğu ortamlar izlenmekte ve kayıtlar saklanmaktadır.
- Kritik bilgilerin ve verilerin bulunduğu alanlarda yetkilendirmeler yapılmaktadır.
- İlişiği kesilmiş personellerin bina ve ofis alanlarına erişim izinleri iptal edilir.
- Mesai bitiminden güvenlik görevlisi tüm idari binayı kontrol ederek gerekli güvenlik tedbirlerini sağlar.
- Sistem odasına girmeye yetkili olmayan ama bakım/onarım, danışmanlık vb. gibi amaçlarla sistem odasında çalışma ihtiyacı olan kişiler Bilgi İşlem sorumlusu onayı ile ve Bilgi İşlem sorumlusunun belirlediği yetkili kişilerin nezaretinde sistem odasına girebilirler.(aramızda gizlilik ve güvenlik esaslarını içeren sözleşmeler imzalanır)
- Sistem Odası, arşiv, özlük dosyaları gibi özel ve gizli bilgilerin yer aldığı ortamların erişim hakları birim ve personel bazında yetkilendirilir.

Kurum içerisinde gizli bilgi ve kişisel veri kategorilerini içeren alanlar izleme sistemleri ile kayıt altına alınmakta ve ilgili veriler güvenlikli kilitli dolaplarda saklanmaktadır;

- Personel özlük dosyaları,
- Müşteri dosyaları,
- Tedarikçi dosyaları,
- Hukuksal ve yasal evraklar,

Kritik sistemlerin bulunduğu odalarda aşağıdaki önlemler alınmıştır,

- İçerde ve dışarda izleme sistemi
- Kapıda parmak izi veya şifre ile giriş sistemi ( log tutabilen bir sistem olması beklenmektedir), veya zimmetlenmiş bir anahtar yönetimi,
- Sistem ekipmanlarının kilitli kabinetlerde saklanması,
- Sıcaklık, nem, su, yangın, duman v.b gibi durumlara yönelik alarm üreten bildirim sistemleri,
- Sistem odası içerisine kapı dışında erişimin olmaması,
- Depo olarak kullanılmaması,
- Yükseltilmiş zemin,
- Yeterli düzeyde iklimlendirme sistemleri,

Arşiv odasında aşağıdaki gerekliliklere yönelik tedbirler alınmıştır,

- Yangın algılama ve söndürme sistemleri ,
- İzleme sistemleri,
- Yetkilendirme,( arşiv yetkilisi belirlenmesi ve yetkinin onda bulunması, yada şifre ile giriş yapılması ve kayıtların loglanması gibi tedbirler tanımlanmalı)
- Geçmişe yönelik varsa gereksiz ve imha süresi geçmiş evrakların imha edilmesi,

Bilgi hırsızlığına açık olan alanlarda;

- İzleme sistemleri,
- Personel yanında gizli evrakları saklayabilecekleri kilitlenebilir dolaplar,
- Gözle bilgi çalınmasını engellemek için gizli ve kişisel veri barındıran dokümanların ters çevrilerek masada kullanılması şeklinde tedbirler alınmıştır.

## 29. Güvenli Geliştirme Politikası

Kurum bünyesinde işletimsel sistemler üzerinde yapılan geliştirmelerde her türlü güvenliğinin sağlanması amacıyla uyulması gereken kurallar ve kontrol edilmesi gereken adımlar tanımlanmıştır.

Geliştirme, bakım ve desteğinin sağlanması gibi faaliyetlerin kontrolü, sürekliliğinin sağlanmasından teknik işletme şefliği sorumludur.

### Veri Koruması

Uygulamaların kayıt altına aldığı veya kullandığı her türlü bilginin yetkisiz erişime kapalı olması gerekmektedir. Bu amaç doğrultusunda aşağıdaki adımlar kontrol edilmelidir.

- Web, uygulama ve veri tabanı sunucularının sistem bileşenleri hakkındaki kritik bilgiler gizlenmelidir.
- Uygulama çatısı, veri tabanı, uygulama sunucusu ve web sunucusu gibi kullanılan yazılımların güvenlik yamaları en üst seviyede olmalıdır.
- Kullanılan parolalar ve parolamı unuttum kontrol soru ve cevapları gibi diğer hassas veriler açık metin olarak saklanmamalıdır.
- Uygulamalar, geliştirme ortamından canlı ortamına aktarılırken gereksiz olan dosyalar (örneğin test kodlar, demo programlar, yedek dosyalar) silinmeli, web uygulamalarında kaynak kod aktarılmamalıdır.
- Program kaynak kodları güvenli ortamda saklanmaktadır.

### Hata Yönetimi ve Kayıt Tutma

Uygulamalar hata aldığında veya beklenmedik bir durum ile karşılaşıldığında, çalışma zamanında üretilen hata mesajları içeriğindeki teknik detayların, veri doğruluğunu sağlamak amacıyla Bilgi İşlem ekibine anlık iletilebilmesi şartı sağlanmalıdır.

Erişime açılan her uygulama kimlik denetimine tabi tutulmalıdır, Ön tanımlı kullanıcı hesapları sistemden, veri tabanından ve uygulamadan kaldırılmalıdır.

Kullanıcıların erişebileceği uygulamalar ve uygulama adımları için kimlik ve yetki doğrulaması yapılmalıdır.

### Geliştirme ve Destek Süreçlerinde Güvenlik

- Sistem ve yazılım paketlerindeki değişiklikler Sistem Yöneticisi tarafından koordineli bir şekilde yürütülmektedir.

- Yapılacak tüm değişiklikler öncelikle test ortamlarında test edilmektedir, sistem kabul testlerini başarılı bir şekilde geçen sistem/yazılım paketlerinin entegrasyon işlemine başlanır.
- İşletim platformu değişiklikleri öncesinde Kurum içinde kullanılan kurumsal uygulamaların yeni sistemlere uyumluluğu teorik olarak araştırılır eğer güncellenmesi gereken kompanent, kod, veri tabanı vb. altyapı değişikliklerinin planlaması yapılır.
- Geliştirme test ve bütünleştirme ortamları ayrılmış ve izole edilmiştir.
- İşletimsel sistemlerde yapılacak güncelleme ve yükleme faaliyetlerinde ortam güvenliği sağlanmaktadır.

### Uygulama güvenliği

Kurum içerisinde kullanılan ve geliştirilen yazılımlarda aşağıdaki güvenlik protokollerinin yer alması beklenir;

- Sisteme girişlerde uygulama güvenliğine yönelik giriş yapılan bilgilerin gizlenmesi gereklidir. ( kullanıcı adı/parola)
- Sisteme girişlerde uygulama güvenliğine yönelik reCAPTCHA ve Brute force desteği olmalıdır.
- Sisteme girişlerde uygulama güvenliğine yönelik hatalı şifre ile girişler belirli deneme sonunda bloklanmalıdır.
- Şifre politikası olmalıdır. ( komleks şifreler- sayı, rakam, harf, özel karakter)
- Şifre politikası kapsamında ilk girişte kullanıcıyı değiştirmeye zorlamalıdır.
- Şifre politikası paralelinde belirli periyotlarda değiştirmesi için uyarı vermelidir.
- Şifre unutma kapsamında two-factor authentication sistemleri olmalıdır.
- Yetkilendirme sistemi olmalıdır.( ilgisiz birimlerin ilgisiz verileri görmemeleri ilgisiz alanlara erişimlerinin engellenmesi lazım)
- Sistem üzerinde yapılan tüm işlemlerin loğları tutulmalı ve loglar encription bir şekilde saklanmalıdır. (sadece sistem yöneticisinde erişimler olabilir)
- Sistemde kullanıcılar belirli bir süre işlem yapılmadığında otomatik olarak hesap kapanmalıdır.
- İlgisiz birimlerin erişimine açık olan alanlarda ilgisiz veriler için veri maskeleme yapılmalıdır.
- Web erişimli ise SSL sertifikası bulunmalıdır.
- Silme ve imha politikalarına uygun olarak belirli süreler sonunda belirli verilerin imha edilmesine imkan verecek şekilde sistem tasarlanmalıdır.
- Sisteme kod analizi ve pentest yapılmalıdır.
- Kurumda yer alan Minimum veri politikasına uygun olarak gereksiz verilerin alınmamasına yönelik kontrol ve geliştirme yapılmalıdır.

## 30. Teknik Açıklık ve Zafiyet Taraması

Bilgi sistemlerinin denetlenmesinden önce denetim gereksinimleri belirlenmeli ve denetim gerekli ise, bu denetim çok dikkatli bir biçimde planlanmalı ve bir program hazırlanmalıdır. İşletim sistemleri konusunda denetim faaliyeti sistem ve sistemin uygulamaları tarafından kullanılan veri dosyalarına

erişim sağlayan özel programların kullanılmasına gerek duyabilir. İşletim sistemlerinde bozulmaya yol açmaması ve soruna neden olmaması için bu tür bir kullanım planlanmalıdır.

- Sistemlere ve verilere erişim denetimi için mutabık kalınmalıdır.
- Teknik denetim testlerinin kapsamı kontrol ve kabul edilmelidir.
- Denetim testleri veri ve yazılıma erişimde sadece okuma olarak kısıtlanmalıdır.
- İspat için kopyalama yapılan dosyalar, tamamen silinmeli ve silindiği belgelenmelidir.
- Kapsam dışında yapılacak ek test istekleri kontrol edilmeli ve onaylanmalıdır.
- Sistem erişilebilirliğini etkileyecek testler mesai saatleri dışında yapılmalıdır.
- Tüm erişim izlenen bir kimlik üzerinden yapılmalıdır.
- Denetim sonuçları sadece yetkili kişilerde, elektronik ortamda şifrelenerek baslı ortamda iste kilitli dolaplarda tutulacaktır.
- Yapılan işin kritikliği, gizli bilgi ve kişisel veri oranı dikkate alınarak minimum yılda bir kere bağımsız dış bir kuruluşa penatrasyon testi yapılmaktadır.
- Zafiyet ve açıklık testlerinde tarafsızlık ve bağımsızlık göz önüne alınmalı ve sonuçlar raporlanmalıdır.

## 31. Kriptoloji

- Kriptografik kontroller aşağıdaki maksatlarla kullanılır.
- a. Gizlilik: Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelemenin kullanılması.
- b. Bütünlük/Güvenilirlik: Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için sayısal imzaların veya mesaj doğrulama kodlarının kullanılması.
- c. İnkar edilemezlik: Bir olay veya faaliyetin oluşumu veya oluşmadığının kanıtını elde etmek için kriptografik tekniklerin kullanılması.
- Alınan hizmetler paralelinde bazı platformların kripto uygulamaları ilgili 3. Taraflarca (PTT teknoloji) yönetilmekte ve anahtarlar saklanmaktadır, ilgili kurallar sözleşmeler ile güvence altına alınmıştır.
- Web siteleri üzerinde SSL sertifikası mevcuttur.
- Kuruluşa ait “özel ve genel nitelikli kişisel veriler” ve “gizli bilgiler” gibi kritik veri tabanları yetkisiz erişimlerden korunması için kriptolanması gerekmektedir.
- Sunuculara erişimler şifrelidir.
- SSL sertifikaları BT ekibi tarafından yönetilmektedir.
- Anahtarlar yasal gerekliliklere uygun olarak sağlanır ve muhafaza edilir.

## 32. Sorumluluk ve Yaptırım

Çalışan tüm personeller bu politikaya uygun hareket etmek zorundadırlar, bu politika da yazan kurallara uygun hareket etmeyen personeller hakkında Disiplin Prosedürü’ ne göre işlem yapılır.

| HAZIRLAYAN ONAYI | KONTROL EDEN ONAYI | GENEL MÜDÜR ONAYI |
|---|---|---|
| | | |

## 33. İlgili Dokümanlar

- 6698 Sayılı Kişisel Verilerin Korunması Kanunu
- 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- TS ISO/IEC 27001:2013 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği Yönetim Sistemleri
- TS ISO/IEC 22301 Toplumsal Güvenlik ve İş Sürekliliği Yönetim Sistemi