# 1.0 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

## 1.1 Amaç

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

## 1.2 Kapsam

Üniversitemizin akademik eğitim, öğretim faaliyetleri ile idari faaliyetlerini ve bu faaliyetlerine ilişkin bilgi varlıklarını, bu varlıkların korunması amacıyla yürüttüğü bilgi güvenliği kapsamındaki ilgili iş süreçlerini kapsar.

*İngilizce:*
*It includes the related working processes within the scope of information security that the university conducts to secure academic education-training activities and administrative activities together with the information entities regarding these activities and these entities at all.*

### 1.2.1 İç Kapsam

İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler;

İstinye Üniversitesi bünyesinde bulunan Bilgi Sistemleri ve Teknolojileri Direktörülüğünü kapsar.

Genel Yönetim Organizasyon Şemasında belirtilmiş roller ve görev tanımlarındaki sorumluluklar.
Yerine getirilecek politikalar, hedefler ve stratejiler;

- BGYS Politikaları,
- Yönetimce belirlenmiş yıllık BGYS hedefleri,
- Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),
- Bilgi Güvenliği Yönetim Sisteminin kurulması, işletilmesi ve sürdürülmesi için Bilgi Sistemleri ve Teknolojileri Direktörlüğü tarafından atanan Yönetim Temsilcileri ve BGYS ekibi,
- İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri, kuruluşun kültürü, kuruluş tarafından uyarlanan standartlar, kılavuzlar ve modeller, sözleşmeye ilişkin ilişkilerin; biçim ve genişliğini kapsamaktadır.
- İç Paydaşlar ;
  - Akademik Personel
  - İdari Personel
  - Öğrenciler

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

### 1.2.2 Dış Kapsam

- Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, yasal, mevzuata ilişkin, finansal, teknolojik, ekonomik ortam,
- Tedarikçi ve paydaşların verilerinin gizliliği,
- Kalite Odaklılık,
- Kuruluşun hedefleri üzerinde etkisi bulunan paydaşlarla ilişkiler ve onların algılamaları ve değerleri;
- Üst Yönetim dahil tüm İstinye Üniversitesi çalışanları,
- İlgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartlar, standartlar,
- İstinye Üniversitesi Teşkilat ve Görevleri Hakkında 656 Sayılı KHK Çerçevesinde İlgili diğer Kamu Kurum ve Kuruluşları.
- Dış Paydaşlar ;
  - YÖK
  - Bakanlıklar ve Bağlı Birimleri
  - Büyükelçilikler ve Konsolosluklar
  - Yerel Yönetimler
  - Kamu İhale Kurumu
  - Kredi Yurtlar Kurumu
  - ÖSYM
  - Bilim ve Teknoloji Yüksek Kurulu
  - TÜBİTAK – ULAKBİM
  - Mezunlar

## 1.3 Tanımlar

**BGYS:** Bilgi Güvenliği Yönetim Sistemi.

**Envanter:** Kurum için önemli olan her türlü bilgi varlığı.

**Üst Yönetim:** İstinye Üniversitesi; Rektörlüğü ve Genel Sekreterliği.

**Birim/Bölüm Yöneticisi:** İstinye Üniversitesi; Direktör ve Sorumluları

**Gizlilik:** Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Ör: 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. (Ör: Veri tabanında saklanan verilerin özet bilgileri ile saklanması, dijital imza)

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

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

**Bilgi Varlığı:** İlgili kurum / birim ve ilgili paydaşları için kurumsal süreçlerinde bir değer ifade eden ve bu nedenle uygun şekilde korunması gereken bir varlıktır.
Bilgi varlığı; İstinye Üniversitesi'nin yürüttüğü hizmet süreçlerini sürdürebilmesi için önemli olan varlıklardır. Bu politikaya konu olan süreçler ve paydaşlar kapsamında bilgi varlıkları şunlardır:

- Yazılı/basılı, görsel, işitsel veya elektronik ortamda sunulan her türlü bilgi ve veri,
- Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım,
- Bilginin transfer edilmesini sağlayan ağlar,
- İlgili bölüm/birimlerin çalışanları,

### 1.4 Sorumluluklar

Sorumluluk ve yetkileri belirlenmiş görevlerin nitelik ve yeterlilikleri görev tanımlarında tanımlanmıştır. Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Bilgi Güvenliği Yönetim Sistemi Ekibi sorumludur. BGYS Ekibi ve Yönetim Temsilcileri Üst Yönetim tarafından atanmıştır.

#### 1.4.1 Yönetim Sorumluluğu

İstinye Üniversitesi Üst Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli kaynakları (bütçe sağlamayı, uzman personel, donanım ve yazılım vb.) tahsis edeceğini, sistemin tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder.

Üst Yönetim kademesinde bulunan yöneticiler ve üst yönetimin gerekli gördüğü diğer yöneticiler BGYS' nin kurulumu, uygulanması, sürdürülebilirliği açısından alt kademelerde bulunan personele yardımcı olurlar ve yazılı ya da sözlü olarak güvenlik talimatlarına uyarlar, ihtiyaç duyulduğunda çalışmalara katılırlar.

#### 1.4.2 Yönetim Temsilcisi Sorumluluğu

- BGYS (Bilgi Güvenliği Yönetim Sistemi)'nin planlanması, kabul edilebilir risk seviyesinin belirlenmesi, risk değerlendirme metodolojisinin belirlenmesi,
- BGYS kurulumunda destekleyici ve tamamlayıcı faaliyetler için gerekli kaynakların sağlanması, kullanıcı kabiliyetlerinin sağlanması/iyileştirilmesi ve farkındalığın oluşması, eğitimlerin yapılması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanması,
- BGYS uygulamalarının yürütülmesi ve yönetilmesi, değerlendirmelerin, iyileştirmelerin ve risk değerlendirmelerinin sürekliliğinin sağlanması,

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

- İç denetimler, hedeflerin ve yönetim gözden geçirme toplantıları ile BGYS ve kontrollerin değerlendirilmesi,
- BGYS' de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından sorumludur.

### 1.4.3 BGYS Ekip Üyeleri Sorumluluğu

- Birim/Bölümleri ile ilgili varlık envanteri ve risk analiz çalışmalarının yapılması,
- Sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Yönetim Temsilcisini bilgilendirmesi,
- Birim/bölüm çalışanlarının politika ve prosedürlere uygun çalışmasının sağlanması,
- Birim/Bölümleri ile ilgili BGYS kapsamında farkındalığın oluşması, iletişimin sağlanması, dokümantasyon ihtiyaçlarının belirlenmesi,
- BGYS' de mevcut yapının sürdürülmesi ve sürekli iyileştirilmesinden sorumludur.

### 1.4.4 İç Denetçi Sorumluluğu

İç denetim planı doğrultusunda, görev verilen iç denetimlerde denetim faaliyetlerinin yapılmasından ve raporlanmasından sorumludur.

### 1.4.5 Birim/Bölüm Yöneticileri Sorumluluğu

Bilgi Güvenliği Politikasının uygulanması ve çalışanların esaslara uymasının sağlanmasından, 3. tarafların politikadan haberdar olmasının sağlanmasından ve fark ettiği bilgi sistemleri ile ilgili güvenlik ihlal olaylarının bildirilmesinden sorumludurlar.

### 1.4.6 Tüm Çalışanların Sorumluluğu

- Çalışmalarını bilgi güvenliği hedeflerine, politikalarına ve bilgi güvenliği yönetim sistemi dokümanlarına uygun olarak yürütmekten,
- Kendi birimi ile ilgili bilgi güvenliği hedeflerinin takibini yapmak ve hedeflere ulaşılmasını sağlamaktan,
- Sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmek ve raporlamaktan,
- Üçüncü taraflar ile yapılan hizmet sözleşmelerine (danışmanlık vb.) ilave olarak gizlilik sözleşmesi yapmak ve bilgi güvenliği gereksinimlerini sağlamaktan sorumludur.

### 1.4.7 Üçüncü Tarafların Sorumluluğu

Bilgi güvenliği politikasının bilinmesi ve uygulanması ile BGYS kapsamında belirlenen davranışlara uyulmasından sorumludur.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

### 1.5 Bilgi Güvenliği Hedefleri

Bilgi Güvenliği Politikası, İstinye Üniversitesi çalışanlarına kurumun güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini arttırmak ve bu şekilde kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, güvenilirliğini ve imajını korumak ve üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunlukları sağlamak amacıyla kurumun tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarının korunmasını hedefler. Yönetim tarafından belirlenen hedefler belirlenmiş periyodlarda izlenir ve yönetimin gözden geçirme toplantılarında görüşülür.

### 1.6 Risk Yönetim Çerçevesi

Kurumun risk yönetim çerçevesi; Bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Risk Analizi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar. Risk işleme planının yönetiminden ve gerçekleştirilmesinden BGYS Yürütme Komitesi sorumludur. Tüm bu çalışmalar, varlık envanteri ve risk değerlendirme talimatında detaylı olarak anlatılmaktadır.

### 1.7 Bilgi Güvenliği Genel Esasları

**a)** Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, İstinye Üniversitesi çalışanları ve 3. taraflar bu politikaları bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

**b)** Bu kural ve politikalar, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.

**c)** Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001 "Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimler (Information Security Management Systems Requirements)" standardını temel alarak yapılandırılır ve işletilir.

**d)** BGYS'nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların katkısıyla yürütür. BGYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yönetim Temsilcisi sorumluluğundadır.

**e)** Kurum tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça kuruma aittir.

**f)** Çalışanlar, danışmanlık, hizmet alımı Tedarikçi ve Stajyer ile gizlilik anlaşmaları yapılır.

**g)** İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.

**h)** Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut kurum çalışanlarına ve yeni işe başlayan çalışanlara verilir.

**i)** Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.

**j)** Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.

**k)** Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**l)** Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.
**m)** Kuruma ait bilgi varlıkları için kurum içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.
**n)** Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.
**o)** Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır.
**p)** Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.
**q)** Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
**r)** Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.
**s)** Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.

### 1.8 Politikanın İhlali ve Yaptırımlar

İstinye Üniversitesi Bilgi Güvenliği Politikasına ve Standartlarına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar için İlgili Mevzuata göre, 3. Taraflar için de geçerli olan sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.

### 1.9 Yönetimin Gözden Geçirmesi

Yönetim gözden geçirme toplantıları BGYS Yönetim Temsilcisi Organize edilerek, Üst Yönetim ve Birim/Bölüm yöneticileri katılımı ile gerçekleştirilir. Bilgi Güvenliği Yönetim Sisteminin uygunluğunun ve etkinliğinin değerlendirildiği bu toplantılar en az yılda bir kez gerçekleştirilmektedir.

### 1.10 Bilgi Güvenliği Politika Dokümanı Güncellenmesi ve Gözden Geçirilmesi

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yönetim Temsilcileri sorumludur.

Doküman, en az yılda bir kez gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa üst yönetime onaylatılarak yeni versiyon olarak kayıt altına alınmalıdır. Her revizyon tüm kullanıcıların erişebileceği şekilde yayınlanmalıdır.

## 2.0 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKA LİSTESİ

İstinye Üniversitesi BGYS politikaları listesi aşağıdaki gibidir.

P01 BİLGİ SİSTEMLERİ GENEL KULLANIM POLİTİKASI
P02 PERSONEL GÜVENLİĞİ POLİTİKASI

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

P03 İNTERNET ERİŞİM POLİTİKASI
P04 E-POSTA POLİTİKASI
P05 ANTİ-VİRÜS POLİTİKASI
P06 ŞİFRE POLİTİKASI
P07 KABLOSUZ İLETİŞİM POLİTİKASI
P08 UZAKTAN ERİŞİM POLİTİKASI
P09 KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI
P10 FİZİKSEL GÜVENLİK POLİTİKASI
P11 SUNUCU GÜVENLİK POLİTİKASI
P12 AĞ CİHAZLARI GÜVENLİK POLİTİKASI
P13 AĞ YÖNETİMİ POLİTİKASI
P14 VERİTABANI GÜVENLİK POLİTİKASI
P15 DEĞİŞİM YÖNETİMİ POLİTİKASI
P16 GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI
P17 SANAL ÖZEL AĞ (VPN) POLİTİKASI
P18 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI
P19 BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI
P20 YAZILIM GELİŞTİRME
P21 KABUL EDİLEBİLİR KULLANIM POLİTİKASI
P22 ORTAMIN ELDEN ÇIKARILMASI POLİTİKASI
P23 TEÇHİZATIN ELDEN ÇIKARILMASI POLİTİKASI
P24 TEMİZ MASA TEMİZ EKRAN POLİTİKASI
P25 KRİPTOGRAFİK KONTROLLER POLİTİKASI
P26 ZİYARETÇİ KABUL POLİTİKASI
P27 TAŞINABİLİR CİHAZ POLİTİKASI
P28 BİLGİ VE YAZILIM ALIŞVERİŞİ POLİTİKASI
P29 ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI
P30 VARLIKLARA YÖNELİK SORUMLULUK POLİTİKASI
P31 BASILI ÇIKTI VE DAĞITIM POLİTİKASI
P32 BİLGİ SINIFLANDIRMA POLİTİKASI
P33 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI

### 2.1 Tanımlar

**Ağ:** (Network**)** Bilgisayarların iletişim hatları aracılığıyla veri aktarımının sağlandığı sistem, bilgisayar ağıdır.

**Alfanümerik**: Latin alfabesindeki harfleri (A-Z, a-z) ve Arap rakamlarını (0-9) kullanan karakter dizisini tanımlamakta kullanılan bir sıfattır.

**Antivirüs Programı:** Bilgisayarın zararlı programlardan korunması için hazırlanan güvenlik yazılımdır.

**Bayt:** (Byte) Elektronik ve bilgisayar bilimlerinde genellikle 8 bitlik dizilim boyunca 1 veya 0 değerlerini bünyesine alan ve kaydedilen bilgilerin türünden bağımsız bir bellek ölçüm birimidir.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**Bit:** Bilgi sistemlerinde kullanılan en küçük bilgi birimidir. Yani programlama ve haberleşmede, bir bit bilgi depolama ve haberleşme veya bağlantının en küçük ve temel ünitesidir.

**BIOS:** (Basic input output system) İşletim sistemi ile donanım arasındaki bütün bağımsız sürücü programlarını yönetir. Diğer bir deyişle Anakart'ın (Bilgisayar merkezi kartı) birçok özelliğini kullanmamıza olanak sağlayan yazılım, sistem ve donanımlarımız arasında bağlantı kurar.

**BGYS:** Bilgi Güvenliği Yönetim Sistemi

**Cihaz:** Bilgi işleme ve depolama amaçlı kullanılan PC (kişi tahsis edilen bilgisayar), laptop, cep telefonu, sunucu, veri depolama cihazı (storage), el terminali ve yazıcılardır.

**DDOS Atağı: (**Distributed Denial of Service Attack), çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşur, bunlar genellikle bir veya birden fazla web sunucusudur. Bu sistemler saldırganlar tarafından çeşitli yöntemler kullanılarak bağdaştırılır.

**Dizin:** (Indeks) Excel, Word dosyaları gibi bilgi kaynaklarının içindeki bilgi parçacıklarına ulaşmak için konu başlık, yer adları kişi adları gibi erişim uçlarına ulaşmak için kullanılan ayrıntılı alfabetik listedir.

**Domain:** Domainler kayıtlı isimlerdir ve şirketler genelde kendi şirketlerinin isminde domain alırlar. Bir domainin sonunda tr, es, au gibi ülke kodları ya da domain türüne bağlı olarak com, net, org, gov, edu gibi uzantılar yer alabilir. Alan adları IP adresi denilen, bilgisayarların birbirini tanımasını sağlayan numara sisteminin daha basitleştirilmiş ve akılda kalması için kelimelerle ifade edilmiş halidir.

**Erişim Kontrol Sistemi:** (Access Control System) Bir bilgi işlem sistemine hangi kullanıcının, hangi haklarla erişebileceğinin ve bu sistem üzerinde hangi işlemleri yapmaya yetkin olduğunun belirlenmesi ve yönetilmesidir.

**Firmwareleri:** Elektronik eşyalarda bulunan donanımların veya cihazın işlevlerini nasıl yerine getireceklerini bildiren ve genellikle tekrar yazılabilir olan ufak kodlardır. Firmware salt okunurdur, okunabilir fakat yazılamaz.

**Firewall:** (Güvenlik Duvarı veya Ateş Duvarı) Güvenlik duvarı yazılımı, bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir.

**Gateway:** (Ağ Geçidi) Farklı ağ iletişim kurallarını kullanan iki bilgisayar ağı arasında veri çerçevelerinin iletimini sağlayan ağ donanımıdır.

**Haber Grubu:** Mail ya da web ortamında belli bir uzmanlık alanında tartışma veya fikir alışverişi yapılan platformdur.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**Heksadesimal:** (Hexadecimal) 16 tabanlı sayı sistemidir. Hxx bilgisayar belleğindeki 8 bitlik baytları göstermek için kullanılan bir kestirme yoldur. Bu sayı sistemine "16 tabanlı sayı sistemi" denilmesinin nedeni, 16 tane sembolden oluşmasıdır. Sembollerden 10 tanesi rakamlarla (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), geri kalan 6 tanesi harflerle (A, B, C, D, E, F) temsil edilir.

**IP:** İnternet'te her bilgisayarın bir IP (Internet Protokol) adresi vardır. Bir IP adresi, noktalarla ayrılan dört rakam grubundan oluşur, her grupta en fazla 3 rakam olabilir; "85.102.156.141" şeklindedir. İnternete bağlanan her bilgisayara sistem tarafından verilen bir ayırt edici numara, yani bir tür "adrestir. IP numarası sayesinde bilgisayarlar internette diğer bilgisayarlarla veri alışverişi yapar. Yani bilgisayarınızın IP numarası sayesinde, herhangi bir web sitesindeki bilgiler sizin bilgisayarınıza kadar ulaşır.

**IpSec: (**Internet Protocol Security) protokolü, IP paketlerini kimlik doğrulamasına (authentication) ve şifrelemeye (encryption) tabi tutarak IP iletişimini güvenli hale getiren bir protokol takımıdır

**IpSec VPN:** IpSec VPN, merkez ofiste bulunan bir güvenlik duvarı (firewall) ya da ağ geçidi (gateway) ile internet üzerinden güvenli bir tünel oluşturarak uç noktaları merkeze bağlama mantığıyla çalışan bir bağlantı çeşididir. Mobil cihazlar ya da kişisel cihazlarla IpSec VPN kullanmak mümkün değildir.

**İstemci:** Yerel ağ ya da internet üzerinde, belli bir hizmeti (ya da hizmetleri) vermekle görevli olan ana bilgisayara (sunucu) bağlanan diğer bilgisayarların her birine verilen genel isimdir. İstemciler, ana bilgisayara bağlanarak sunulan hizmetten yararlanırlar.
**İşletim Sistemi:** Bilgisayarda çalışan, bilgisayar donanım kaynaklarını yöneten ve çeşitli uygulama yazılımları için yaygın servisleri sağlayan yazılımlar bütünüdür.

**Kriptografi:** İletilen bilginin istenmeyen şahıslar tarafından anlaşılmayacak bir biçime dönüştürülmesinde kullanılan tekniklerin bütünüdür. Diğer bir deyişle gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür.

**Kümeleme:** (Clustering) Birçok bilgisayarı birlikte tek bir bilgisayar gibi göstererek çalıştırma tekniğidir.

**L2TP:** Bilgisayar ağlarında kişisel sanal ağı destelemek için kullanılan tuneling protokolüdür. Kendi içinde hiçbir gizlilik ya da şifreleme içermez. Tünel yapısı ile bilgi transferi sağlayan şifreleme protokolünden yararlanır.

**MAC:** Bilgisayar arası iletişim belirli kurallar çerçevesinde gerçekleşir. Her bilgisayarın iletişim için kullandığı nasıl ki IP adresi varsa bu iletişim sırasında kullanılan ağ cihazlarının da tanımlanması için bir adrese gerek vardır. MAC Adress; Bir bilgisayar ağında, bir cihazın ağ donanımını tanımaya yarayan hexadecimal sayı sistemi ile ifade edilen her ağ cihazına özel olarak atanan 48 bitlik adreslere verilen isimdir.

**Misafir Ağı:** Şirket dışından Şirkete gelenlerin güvenli bir şekilde internete erişimini sağlayan ağdır.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**Passphrase:** Bir parola veya bir bilgisayar sisteminde veri erişimini kontrol etmek için kullanılan kelime ya da metin dizisidir.

**Penetrasyon Testi:** Bilişim Sistemlerini oluşturan ağ altyapılarını, donanım, yazılım ve uygulamalara kötü niyetli birinin saldırmasını öngören yöntemler kullanılarak yapılan saldırı ve müdahaleler ile güvenlik açıklarının tespit edilip bu açıklarla sisteme sızılmaya çalışılması ve tüm bu işlemlerin raporlanmasıdır.

**Port:** Bilgisayar ile çevre birimleri arasında iletişimi sağlayan fiziksel arayüzdür.

**PPTP:** (Point to Point Tunnel Protocol) Noktadan Noktaya Tünel Protokolü" anlamına gelmektedir. PPTP; VPN'in tünel protokollerinden birisidir.

**Public Key:** Bu yöntemde kullanıcıların 2 adet şifresi bulunur. Bu şifrelerden birisi herkese açık (umumi,public key) diğeri ise gizli (private, hususi) şifredir. Çalışma mantığına göre umumi olan şifre herkese rahatça dağıtılabilir ve bu şifreden hususi olan şifreye ulaşmanın matematiksel bir yolu bulunmamalıdır. Ayrıca umumi şifre ile şifrelenmiş mesajın hususi şifre ile açılmasının bir yolunun bulunması gerekir.

**Private Key:** İletişimin kurulabilmesi için bu yöntemde de iki anahtara gerek vardır, ancak anahtarlar temel olarak aynıdır. Her iki anahtar ile de aynı işlevler yerine getirilir.

**RDP:** (Remote Desktop Protocol) Türkçe uzak masaüstü protokolü anlamına gelmektedir. Kişisel bilgisayar kullanarak "Uzak Ara Bağlantısı" (RDP) protokolü ile bağlanılan, dünyanın her noktasından, şirket verilerine kolay, hızlı, güvenli ve esnek erişim sağlaması ile tanınan bir teknolojidir.

**Root:** Tam yetkili kullanıcı yani yönetici demektir. Windows işletim sistemlerindeki yönetici (administrator) kavramıyla eş anlamlı bir kelimedir.

**Script:** Herhangi bir program dilinde yazılmış uygulama parçalarının tümünün kodlarını içeren kod bütününe script adı verilir.

**SSID:** (Service Set Indentifier/Hizmet seti kimliği) Bir kablosuz ağı tanımlayan addır.

**SSL:** (Secure Socket Layer) SSL kişisel gizlilik ve güvenilirlik sağlayan, network üzerindeki bilgi transferi sırasında bilginin bütünlüğü ve gizliliği için sunucu ile istemci arasındaki iletişimin şifrelenmiş şekilde yapılabilmesine imkan veren bu sayede gizliliğinin ve bütünlüğünün korunmasını sağlayan bir güvenlik protokolüdür.

**SSL VPN:** Son kullanıcı tarafında bir yazılıma ya da donanıma gerek kalmadan işletim sistemlerinin sağladığı İnternet tarayıcılarının kullanılmasıyla bir ağa güvenli bir biçimde bağlantı çeşididir. Mobil cihazlar ya da kişisel cihazlarla SSL VPN kullanmak mümkündür.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**Statik IP:** IP adresleri İnternet Hizmet Sağlayıcıları tarafından atanır ve bu adresler zaman içerisinde değişebilir. Statik IP adresleri ise değişmez, atandığı cihaz veya sunucu için sabit olarak kalır.

**Sunucu:** Bir bilgisayar ağı üzerinden kullanıcı isteklerine yanıt veren bilgisayar teknolojisidir.

**Sürücü:** Bilgisayarın donanım ve aygıtlarla iletişim kurmasını sağlayan bir yazılımdır.

**Switch:** (Ağ anahtarı) Bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımıdır.

**Tünel:** Kurumsal ağa erişmek için kullanılan uygulamaların kullandığı veri gizleme yöntemidir.

**UTP kablosu:** Korumasız bükümlü kablodur. Bilgisayarlar arası veri iletişiminde kullanılır.

**Virüs Pattern:** Antivirüs programının virüsleri tanıma amacıyla kullandığı imza dosyasıdır.

**VLAN:** (Virtual Local Area network) Ağ kullanıcılarının ve kaynaklarının bir switch üzerindeki portlara bağlanarak yapılan mantıksal bir gruplamadır.

**VPN:** Virtual Private Network'ün (Sanal Özel Ağ) kısaltması olup, ağlara güvenli bir şekilde uzaktan erişimde kullanılan bir teknolojidir. Sanal bir ağ uzantısı yarattığından uzaktan bağlanan makine konuk gibi değil, ağa fiziksel olarak bağlıymış gibi görünür.

**Yönlendirici:** (Router) Ağdaki bilgisayarların yönlerini bulmalarına kılavuzluk eder. Bir başka deyişle ağdaki IP paketlerini bir ağdan başka bir ağa taşımaya yarayan cihazlara router denmektedir.

## 3.0 P01 BİLGİ SİSTEMLERİ GENEL KULLANIM POLİTİKASI

### 1.1 Genel Bakış

Kurumumuz bilgi paylaşımı ve güvenliği konularında tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmek amacıyla "Bilgi Güvenliği Politikalarını" hazırlamıştır. Bilişim ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir güvenlik bütün çalışanların içerisine dahil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

### 1.2 Amaç

Bu politikanın amacı kurum bünyesindeki bilişim cihazlarının ve yazılımlarının uygun kullanımı hakkında standart oluşturmaktır. Uygunsuz kullanım kurumu virüs saldırılarına, ağ sistemlerinin çökmesine hizmetlerin aksamasına ve bunların yaptırımlara dönüşmesine sebep olabilir.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

### 1.3 Kapsam

Bu politika kurumun bütün çalışanları, sözleşmelileri, kurum adı altında çalışan bütün kişiler ve aynı zamanda kurumun sahip olduğu ve kiraladığı bütün cihazları kapsamaktadır.

### 1.4 Politika

Genel Kullanım ve sahip olma ile güvenlik ve kişiye ait bilgiler aşağıdaki gibi açıklanmıştır.

#### 1.4.1 Genel Kullanım ve Sahip Olma

**a)** Kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da kurumun bünyesinde oluşturulan tüm veriler kurumun mülkiyetindedir.
**b)** Çalışanlar bilgi sistemlerinden kendi kişisel kullanımı için makul seviyede yararlanabilirler.
**c)** Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmelidir.
**d)** Güvenlik ve ağın bakımı amacı ile yetkili kişiler cihazları, sistemleri ve ağ trafiğini burada tanımlanan politikalar çerçevesinde gözlemleyebilir. Kurum, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
**e)** 25 kullanıcıdan daha büyük ağlarda domain yapısı oluşturulmalıdır. Bu durumda bütün bilgisayarlar domaine login (bağlı) olmalıdır. Domaine bağlı olmayan bilgisayarlar yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.
**f)** Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalıdır ve kopyalanmamalıdır.
**g)** Bilgisayarlar üzerinden işle ilgili belgeler, resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
**h)** Kurumda sorumlu Bilgi Sistemleri ve Teknolojileri personeli ve ilgili teknik personel dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemeler hiçbir surette değiştirilmemelidir.
**i)** Bilgisayarlara hiçbir surette lisanssız program yüklenmemelidir.
**j)** Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre politikasına göre hareket edilmelidir.

#### 1.4.2 Güvenlik ve Kişiye Ait Bilgiler

**a)** Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları tanımlanmalıdır.
**b)** Şifreleri güvenli bir şekilde saklamalı ve hesap bilgileri başka kimseyle paylaşılmamalıdır. Sistem seviyeli şifreleri 6 ayda bir kullanıcı seviyeli şifreler ise en az 6 ayda bir değiştirilmelidir.
**c)** Bütün PC ve Laptoplar otomatik olarak 20 dakika içerisinde şifreli ekran korumasına geçebilmelidir.
**d)** Laptop bilgisayarlar güvenlik açıklarına karşı korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır.
**e)** Laptop bilgisayarın çalınması / kaybolması durumunda, durum fark edildiğinde en kısa zamanda yetkili kişiye haber verilmelidir.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**f)** Kuruma ait cep telefonu, tablet ve el terminali cihazlarının gerekli güvenlik tedbirlerini almaktan cihaz kullanıcısı sorumludur.
**g)** Çalışanlar tarafından gönderilen maillerde şöyle bir açıklama olmalıdır.

**Türkçe metin:**
"Bu e-posta mesajı ve ekinde bulunabilecek dosyalar yalnız mesajın alıcı hanesinde kayıtlı kullanıcı/kullanıcılar içindir. Mesajın alıcısı değilseniz, lütfen hemen göndericiyi uyarınız. Mesajı dağıtmayınız, kopyalamayınız, içeriğini açıklamayınız ve çıktı almaksızın siliniz. Bu mesajda kayıtlı görüş ve düşünceler hiçbir şekilde İstinye Üniversitesine atfedilemeyeceği gibi, kurumumuz açısından bağlayıcı da değildir. Virüs ve kötü amaçlı yazılımların bu mesajda yerleşmesinin engellenmesi amacıyla gerekli tüm önlemler alınmış olsa da bu mesajın sisteminizde yaratabileceği kayıp ve zararlardan dolayı kurumumuz hukuken sorumluluk kabul etmez. İstinye Üniversitesi'nin alanında dünya çapında yürüttüğü faaliyetlere ilişkin bilgi almak için internet sitemizi (www.istinye.edu.tr) ziyaret edebilirsiniz. "

**İngilizce metin:**
"This e-mail message and the files that may be found in its attachment are only for the user(s) registered in the recipient section of the message. If you are not the recipient of the message, please alert the sender immediately. Do not distribute the message, do not copy it, do not explain its content and delete it without printing. The views and opinions recorded in this message cannot be attributed to Istinye University in any way, nor are they binding for our institution. Although all necessary measures have been taken to prevent viruses and malware from settling in this message, our institution does not legally accept any liability for any loss or damage that this message may cause on your system. You can visit our website (www.istinye.edu.tr) to get information about the activities carried out by Istinye University worldwide."

**h)** Çalışanlar bilinmeyen kimselerden gelen dosyaları açmamalıdırlar. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler.
**i)** Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve gerekirse dosyaları sıkıştırılmalıdır.

### 1.4.3 Uygunsuz Kullanım

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.

#### 1.4.3.1 Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler hiçbir istisna olmadan standartlaştırılmıştır.

**a)** Herhangi bir kişi veya kurumun izinsiz kopyalama, devlet sırrı, patent veya diğer kurum bilgileri, yazılım lisansları vs. haklarının çiğnenmesi,

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**b)** Basılı ve dijital yayınların izinsiz kopyalanması, çoğaltılması, basılı yayınların dijital formata dönüştürülmesi, lisans gerektiren yazılımların kopyalanması ve dağıtılması,
**c)** Zararlı programların ağa veya sunuculara bulaştırılması,
**d)** Kendi hesabınızın şifresini başkalarına vermek veya kendi hesabınızı kullandırması,
**e)** Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışması,
**f)** Ağ güvenliğini etkilemek, ağ haberleşmesini bozması,
**g)** Kullanıcı kimlik tanıma yöntemlerinden kaçması,
**h)** Program/script/komut kullanarak kullanıcının bağlantısını etkilemesi,
**i)** Kurum bilgilerini kurum dışından üçüncü şahıslara iletmesi,
**j)** Kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programları kurmak ve kullanmak yasaktır.

#### 1.4.3.2 E-mail ve Haberleşme Aktiviteleri

**a)** Kurum dışından web posta sistemini güvenliğinden emin olunmayan bir bilgisayardan kullanması,
**b)** İstenilmeyen e-posta mesajlarının iletilmesi. (Bunlar karşı tarafın özellikle istemediği reklam mesajlarını içeren mailler olabilir),
**c)** E-posta veya telefon vasıtası ile taciz etmesi,
**d)** E-posta başlık bilgilerini yetkisiz kullanması veya değiştirmesi,
**e)** Zincir e-postaları oluşturması veya iletmesi,
**f)** Yetkili kişilerin izni olmadan haber gruplarına iletmesi yasaktır.

## 4.0 P02 PERSONEL GÜVENLİĞİ POLİTİKASI

### 1.1 Amaç

Kurumun bilgi kaynaklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyesi kendisine verilen yetki ve sorumlulukları iyi anlaması ve yerine getirmesiyle çok yakından bağlantılıdır. Bu nedenle kurum, ilgili personelin seçimi sorumluluk ve yetkilerin atanması, işten çıkması, eğitilmesi, vb. konularının güvenlik ile ilgili boyutunu ne şekilde ele alacağını bu politika ile belirler.

### 1.2 Kapsam

Personel Güvenlik Politikası, Kurum bilgi sistemlerini kullanan tüm çalışanlarını kapsamaktadır.

### 1.3 Politika

Personel Güvenliği Politikaları aşağıdaki gibidir.

**a)** Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
**b)** Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaklanmalıdır.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**c)** Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.
**d)** Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
**e)** Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
**f)** Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.
**g)** Çalışanlara kamuya açık alanlarda, açık ofis ortamlarında ve ince duvarları olan odalarda gizliliği olan konuşmaların yapılmaması hatırlatılmalıdır.
**h)** İş tanımı değişen veya kurumdan ayrılan kullanıcıların erişim hakları düzenlenmeli ya da pasife alınmalıdır.
**i)** Kurum bilgi sistemlerinin işletilmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.
**j)** Yetkiler "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı " rollerin sorumlulukların paylaştırılması ile ilgilidir ve bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.
**k)** Çalışanlar kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler görev ve yetkileri hakkında periyodik olarak eğitilmelidir.
**l)** Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token (şifrematik), akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

## 5.0 P03 İNTERNET ERİŞİM POLİTİKASI

### 1.1 Amaç

Bu politika ile Kurumumuzun güvenli internet erişimi için sahip olması gereken standartları belirlenmiştir. 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.

### 1.2 Kapsam

Bu politika İstinye Üniversitesi'nin bütün kullanıcılarını kapsamaktadır.

### 1.3 Politika

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

Kurum bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkmalıdır. Ağ güvenlik duvarı kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

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 sağlayabilmelidir.

**a)** Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (kumar, şiddet vs.) yasaklanabilmelidir.
**b)** Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme sistemleri kullanılmalıdır. Anti-virüs gateway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik virüslere karşı taranmalıdır.
**c)** Ancak yetkilendirilmiş sistem yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahip olmalıdır. (ftp, telnet, vb.)
**d)** Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.
**e)** Üçüncü şahısların kurum internetini kullanmaları bilgi sistemleri yetkililerinin uygun görmesi durumunda Misafir Ağı üzerinden sağlanmalıdır.

## 6.0 P04 E-POSTA POLİTİKASI

### 1.1 Amaç

Bu politikanın amacı kurumun e-posta altyapısına yönelik kuralları ortaya koymaktır. Kurumda oluşturulan e-postalar resmi bir kimlik taşımaktadır. Bunun yanı sıra e-posta basitliği ve hızı nedeni ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır.

### 1.2 Kapsam

Bu politika kurumda oluşturulan e-postaların doğru kullanımını içermektedir ve bütün çalışanları kapsamaktadır.

### 1.3 Politika

Bu politika yasaklanmış kullanım ve kişisel kullanım olarak aşağıdaki gibidir.

#### 1.3.1 Yasaklanmış Kullanım

**a)** Kurumun e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen Bilgi Sistemleri ve Teknolojilerine haber verilmelidir.
**b)** Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
**c)** Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında kesinlikle başkalarına iletilmemeli ve Bilgi Sistemleri ve Teknolojileri'ne bilgi verilmelidir.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**d)** Kişisel kullanım için internet sitelerine üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

**e)** Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır ve Bilgi Sistemleri ve Teknolojileri'ne bilgi verilmelidir.

**f)** Kullanıcıların kullanıcı kodu / şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir ve Bilgi Sistemleri ve Teknolojileri'ne bilgi verilmelidir.

**g)** Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, fikri mülkiyet içeren malzeme vb.) gönderemezler.

### 1.3.2 Kişisel Kullanım

**a)** Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden e-posta erişimi için donanım /yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

**b)** Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.

**c)** Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.

**d)** E-posta adresine sahip kullanıcının herhangi bir sebepten (emekli olma, işten ayrılma gibi nedenlerle) kurumdaki değişikliğinin İnsan Kaynakları Direktörlüğü tarafından Bilgi Sistemleri ve Teknolojileri Direktörlüğü'ne bildirilmesi gereklidir.

### 1.3.3 Elektronik Posta Adreslerinin Kullanım Amacı ve Mülkiyet

İstinye Üniversitesi' ne (Kuruma) ait alan adları üzerinden çalışanların ismi üzerine açılmış elektronik posta adresleri kişisel mail olarak kullanılamaz. Söz konusu elektronik posta adresleri kuruma ait işlerin ve faaliyetlerin gereği gibi, aksamadan, zamanında gerçekleştirilmesi adına kişilere tanımlanarak sadece zilyetliği teslim edilmiş olup mülkiyet hakkı her zaman alan adı sahibine aittir. Söz konusu elektronik postalara, hiçbir zaman kişisel bilgiler ihtiva ettiği iddiasıyla işverenin erişimi engellenemez, engellenmeye çalışılamaz. Kuruma ait alan adı üzerinden yapılan elektronik gönderilerin Kurum'u temsil ettiği göz önünde bulundurulmalı ve amacı dışında kullanılmamalıdır.

### 1.3.4 E-Posta Yönetimi

Kurum, e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve altyapıyı sağlamakla sorumludur. Kurumda bu sürecin başarılı bir şekilde çalışmasından da Bilgi Sistemleri ve Teknolojileri birimi sorumludur.

### 1.3.5 E- Posta Virüs Koruma

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslere bulaşmış e-postalar anti-virüs sistemleri tarafından analiz edilip temizlenmelidir. Bilgi Sistemleri ve Teknolojileri bu sistemden sorumludur.

## 7.0 P05 ANTİ-VİRÜS POLİTİKASI

### 1.1 Amaç

Kurumdaki bütün bilgisayarların efektif virüs algılama ve engelleme standardına sahip olması için gereklilikleri belirlemektir.

### 1.2 Kapsam

Bu politika İstinye Üniversitesindeki olan bütün bilgisayarları kapsamaktadır ve Bilgi Sistemleri ve Teknolojileri sorumluluğundadır.

### 1.3 Politika

Anti-virüs politikası kapsamındaki politikalar aşağıdaki gibidir.

**a)** Domainde olan bilgisayarlar anti-virüs yazılımına sahip olmalıdır ve belli aralıklarla düzenli olarak güncellenmelidir.
**b)** Buna ek olarak anti-virüs yazılımı ve virüs patternleri otomatik olarak güncellenmelidir.
**c)** Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmalıdır.
**d)** Sistem yöneticileri anti-virüs yazılımının sürekli ve düzenli çalışması ve bilgisayarların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
**e)** Zararlı programları (solucan, truva atı vs.) kurum bünyesinde oluşturmak ve dağıtmak yasaktır.
**f)** Hiçbir kullanıcı herhangi bir sebepten dolayı anti-virüs programını sistemden kaldıramamalıdır.

## 8.0 P06 ŞİFRE POLİTİKASI

### 1.1 Amaç

Bu politikanın amacı güçlü bir şifre oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkında standart oluşturmaktır.

### 1.2 Kapsam

Bu politika kullanıcı hesabı olan (Bilgisayar ağına erişen ve şifre gerektiren kişiler ) bütün kullanıcıları kapsamaktadır.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

### 1.3 Politika

Şifre bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. Kurum çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifre belirlemekle sorumludurlar.

#### 1.3.1 Genel

**a)** Bütün sistem seviyeli şifreler (örnek, root, administrator) en 6 ayda bir değiştirilmelidir.
**b)** Bütün kullanıcı seviyeli şifreler Yönetim dahil (örnek, e-posta, web vs.) en az 6 ayda bir değiştirilmelidir.
**c)** Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
**d)** Kullanıcı, şifresini başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazmamalıdır.
**e)** Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.
**f)** Şifrelerde Türkçe karakter kullanılmaması tavsiye edilir.

#### 1.3.2 Ana Noktalar

##### 1.3.2.1 Genel Şifre Oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs. Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

Zayıf şifreler aşağıdaki karakteristiklere sahiptir.

- Şifreler az karaktere sahiptir.
- Şifreler sözlükte bulunan bir kelimeye sahiptir.
- Şifreler aşağıdaki gibi ortak değere sahiptir.
    - Ailesinin, arkadaşının sahip olduğu bir hayvanın veya bir sanatçının ismine sahiptir.
    - Bilgisayar terminolojisi ve isimleri, komutlar, donanım veya yazılım gibi
    - “universite” , “istinye” gibi
    - AaaBb, qwerty ,qazwsx, 123321 gibi sıralı harf veya rakamlar

Güçlü Şifreler aşağıdaki karakteristiklere sahiptir.

- Küçük ve büyük karakterlere sahiptir. (A-Z , a-z)
- Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir.(0-9,!,@,&=(,}?,\)
- Alfanümerik karaktere sahiptir.

- Herhangi bir dildeki argo lehçe veya teknik bir kelime olmamalıdır.

##### 1.3.2.2 Şifre Koruma Standartları

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

Kurum bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanılmamalıdır ve kimse ile paylaşılmamalıdır. İlgili şifreler Kuruma ait gizli bilgiler olarak düşünülmelidir. Değişik sistemler için farklı şifre kullanılmalıdır.

Aşağıdakiler şifreler ile ilgili yapılmayacaklar listesidir.

**a)** Herhangi bir kişiye telefonda şifre vermek,
**b)** E-posta mesajlarında şifre belirtmek,
**c)** Üst yöneticinize şifreleri söylemek,
**d)** Başkaları önünde şifreler hakkında konuşmak,
**e)** Aile isimlerini şifre olarak kullanmak,
**f)** Şifreleri işten uzakta olduğunuzda iş arkadaşlarınıza bildirmek,
**g)** Uygulamalardaki "şifre hatırlatma" özelliklerini seçmek,

#### 1.3.2.3 Uygulama Geliştirme Standartları

Uygulama geliştiricileri programlarındaki aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

- Bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.
- Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.

#### 1.3.2.4 Uzaktan Erişen Kullanıcılar İçin Şifre Kullanımı

Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılmalıdır.

## 9.0 P07 KABLOSUZ İLETİŞİM POLİTİKASI

### 1.1 Amaç

Bu politika kablosuz cihazların gerekli güvenlik tedbirleri alınmaksızın kurumun bilgisayar ağına erişimini engellemeyi amaçlamaktadır. Sadece bu politikanın güvenlik kriterlerine uyan cihazlar kurumun bünyesinde kullanabilirler.

### 1.2 Kapsam

Bu politika kurum bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını kapsamaktadır. Kablosuz veri transferi sağlayabilen cihazları kullananlar ve Bilgi Sistemleri ve Teknolojileri bu kapsam içerisindedir. Kuruma bağlantısı olmayan herhangi bir cihaz veya bilgisayar ağı bu politikanın kapsamı içerisinde değildir.

### 1.3 Politika

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

Kablosuz iletişim politikası aşağıdaki gibidir.

### 1.3.1 Onaylanmış Teknoloji

Bütün kablosuz erişim cihazları Bilgi Sistemleri ve Teknolojileri tarafından onaylanmış olmalıdır ve belirlenen güvenlik ayarlarını kullanmalıdır.

### 1.3.2 Güvenlik Ayarları

**a)** Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır.
**b)** Bilgi Sistemleri ve Teknolojileri tarafından erişim cihazlarındaki firmwareleri düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili güncellemeleri sağlar.
**c)** Kullanıcıların erişim cihazları kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü cihaz resetlendiğinde (cihazın ilk ayarlarına geri dönmesi) fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.
**d)** Bilgi Sistemleri ve Teknolojileri tarafından varsayılan SSID isimlerini kullanılmamalıdır. SSID bilgisi içerisinde kurumla ilgili bilgi olmamalıdır.
**e)** Erişim cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dahil olmalıdırlar.
**f)** Erişim cihazları statik IP adresleri kullanmalıdır. Aynı zamanda donanım adresleme kullanılmalıdır.
**g)** Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

## 10.0 P08 UZAKTAN ERİŞİM POLİTİKASI

### 1.1 Amaç

Bu politikanın amacı herhangi bir yerden kurum çalışanlarının veya tedarikçilerin kurumun bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar kaynaklarının yetkisiz kullanımından dolayı kuruma gelebilecek potansiyel zararları minimize etmek için tasarlanmıştır. Bu zararlar şunlardır; Kurumun gizli ve hassas bilgilerinin kaybı, prestij kaybı ve içerideki kritik sistemlerde meydana gelen zararlar vb.

### 1.2 Kapsam

Bu politika kurumun bütün çalışanlarını, sözleşmelileri veya tedarikçileri ve kısaca kurumun herhangi bir birimindeki bilgisayar ağına uzaktan veya yakından erişen bütün kişi ve kurumları kapsamaktadır.

Bütün uzaktan erişim uygulamaları bu politika tarafından kapsanmaktadır.

### 1.3 Politika

Uzaktan erişim politikası aşağıdaki gibidir.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**1.4 Genel**

**a)** Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

**b)** Uzaktan erişim metotları ile kuruma bağlantılarda bilgi sistemlerinin güvenliğinin sağlanması için aşağıdaki politikalara göz atmak gerekmektedir.

Şifre Politikası
Sanal Özel Ağ (VPN) Politikası

**1.4.1 Gereklilikler**

**a)** İnternet üzerinden kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. Bu, veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec VPN, L2TP, SSL VPN, PPTP vb. protokollerinden birini içermelidir.

**b)** Mümkünse uzaktan erişim güvenliği bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one time password authentication) veya güçlü bir passphrase (uzun şifre) destekli public /private key sistemi kullanılması tavsiye edilmektedir. Daha fazla bilgi için P06 Şifre politikasına bakınız.

**c)** Uzaktan erişim gerçekleştiren kullanıcıların veya tedarikçilerin erişim şifreleri 6 ayda bir değiştirilecektir. Verilen şifreler kurumun şifreleme politikasına uygun olmalıdır.

**d)** Uzaktan erişim gerçekleştiren tedarikçiler kurumun bilgisinin ekran çıktısını alamaz, transfer edemez ve kurum dışına çıkartamaz. Aksi taktirde oluşacak yasal yükümlülüklerden sorumlu olacaktır.

**e)** Kurum çalışanları hiçbir şekilde kendilerinin login (bağlantı) ve e-posta şifrelerini aile bireyleri dâhil olmak üzere hiç kimseye vermemelidirler.

**f)** Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar.

**g)** Çalışanlar kurum ile ilgili çalışmalarında kurumun dışındaki e-posta hesaplarını kullanmamalıdırlar.

**h)** Uzaktan bağlananlar makinesinde zararlı kod, truva atı vs. olduğundan şüpheleniyorsa bağlantıyı gerçekleştirmemelidir.

**i)** Uzaktan erişim yöntemi ile kuruma erişen bilgisayar ağında güvenlik tedbirleri alınmış olmalıdır. (Örn: Firewall, domain altyapısı vs.)

**j)** Kurum ağına erişecek tüm kullanıcı ve kurumlar ile gizlilik sözleşmesi yapılmış olmalıdır.

**k)** Periyodik olarak yapılan kontrollerle veya görev değişikliği/işten ayrılma bildirimi Bilgi Sistemleri ve Teknolojilerine iletildiğinde kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

**l)** Kurum, uzaktan erişim verdiği kullanıcı veya kurumlarda alması gereken güvenlik tedbirlerinde herhangi bir aksaklık gördüğünde uzaktan erişim bağlantısını eksiklik düzelinceye kadar kesme hakkına sahiptir.

**m)** Kurum güvenli erişimin sağlanabilmesi için gerekli gördüğü takdirde kullanıcının veya kurumun sadece belli zaman aralıklarında veya istek yapılan durumda uzaktan erişimine izin verebilir.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

## 11.0 P09 KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI

### 1.1 Amaç
Bu politika kurum çalışanlarının, bilgi güvenliği ve iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dâhilinde gerekli müdahaleyi yapabilmelerine yönelik standartları belirlemektedir.

### 1.2 Kapsam
Bilgi güvenliğine yönelik tehlike durumlarında sistemlere yapılacak direkt saldırılar, zararlı kod içeren programlar, kişilerin sisteme sızması, bilginin hırsızlığı, dışarıdan veya içeriden gerçekleştirilebilecek saldırılar bu kapsamdadır. Acil durum yönetimi Bilgi Sistemleri ve Teknolojilerini kapsamaktadır.

### 1.3 Politika
Kurum çalışanlarının, bilgi güvenliği veya iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dâhilinde gerekli müdahaleyi yapabilmelerine yönelik standartlar aşağıda belirtilmiştir.

**a)** Acil durum sorumluları atanmalıdır. Yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir.
**b)** Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin uygulama veya veri tabanı sunucularından donanım ve yazılıma ait problemler oluştuğunda yerel veya uzak sistemden yeniden kesintisiz çalışma sağlanabilmelidir.
**c)** Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlaması için aynı ortamda kümeleme veya uzaktan kopyalama veya pasif sistem çözümlerini hayata geçirilmelidir.
**d)** Acil durumlarda kurum içi iş birliği gereksinimleri tanımlanmalıdır.
**e)** Acil durumlarda sistem logları incelenmek üzere saklanmalıdır.
**f)** Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.
**g)** Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
**h)** Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
**i)** Acil durumlarda Acil Destek Ekibine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zarar tespit edilerek süratle daha önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.
**j)** İlgili yönetici tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.

## 12.0 P10 FİZİKSEL GÜVENLİK POLİTİKASI

### 1.1 Amaç
Bu politika kurum personeli ve kritik kurumsal bilgilerin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve kurum binalarına yetkisiz girişlerin yapılmasını önlemek amacını taşımaktadır.

### 1.2 Kapsam
Kurum binalarında yer alan bilgi varlıklarına erişim sağlayan tüm fiziksel güvenlik konularını kapsamaktadır.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

### 1.3 Politika

Fiziksel Güvenlik politikaları aşağıdaki gibidir.

**a)** Kurumsal bilgi varlıklarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.
**b)** Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.
**c)** Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlarına girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.
**d)** Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
**e)** Kritik sistemler erişim yetkisi ile belirlenmiş alanlarda bulundurulmalıdır.
**f)** Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.
**g)** Kuruma giriş yapacak ziyaretçi veya kurye teslimatları yetkili görevliler gözetiminde gerçekleştirilmelidir.
**h)** Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.
**i)** Fotoğraf, video, ses vb. kayıt cihazlarının yetki verilmeyen kişiler tarafından güvenli alanlara (Sistem Odaları, İK, Öğrenci İşleri, BST Ofisleri, Arşiv Odaları) sokulması yasaklanmalıdır.

**13.0**

## 14.0 P11 SUNUCU GÜVENLİK POLİTİKASI

### 1.1 Amaç

Bu politikanın amacı kurumun sahip olduğu sunucularının temel güvenlik konfigürasyonları için standartları belirlemektir. Bu politikanın etkili kullanılması ile Kurum bünyesindeki bilgilere ve teknolojiye yetkisiz erişimler engellenmesi amaçlanmaktadır.

### 1.2 Kapsam

Bu politika kurumun sahip olduğu bütün dahili sunucular için geçerlidir.

### 1.3 Politika

Sunucu Güvenlik politikalar aşağıdaki gibi iki başlıkta ele alınmıştır.

#### 1.3.1 Sahip Olma ve Sorumluluklar

Kurum bünyesindeki bütün dahili sunucuların yönetiminden sadece Bilgi Sistemleri ve Teknolojileri sorumludur. Sunucu konfigürasyonları sadece bu Bilgi Sistemleri ve Teknolojileri tarafından veya onaylı danışmanlık kurumları tarafından Bilgi Sistemleri ve Teknolojileri gözetiminde yapılacaktır.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**a)** Bütün sunucular (kurumun sahip olduğu) ilgili kurumun yönetim sistemine kayıtlı olmalıdır.
**b)** Sunucuların Yeri ve Sorumlu Departmanları,
**c)** Seri Numarası, Marka ve Model Bilgileri,
**d)** Donanım Özellikleri,
**e)** Bakım Bilgisi,
**f)** Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

### 1.3.2 Genel Konfigürasyon Kuralları

**g)** İşletim sistemi yönetimi kurumun Bilgi Sistemleri ve Teknolojileri talimatlarına göre yapılmalıdır.
**h)** Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
**i)** En az 1 hafta süreyle loglanmalıdır. (IP bazlı)
**j)** Kurum dışı yapılan bağlantılar bilgi sistemlerinin belirlediği kurallara göre yapılmalıdır.
**k)** Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

### 1.4 Gözlemleme

**a)** Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalı ve yasalarla belirlenmiş süreler kadar saklanmalıdır.
**b)** Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.
**c)** Denetimler yetkili organizasyonlar tarafından kurum bünyesinde belli aralıklarda yapılmalıdır.
**d)** Denetimlerde kurumun işleyişine zarar vermemesi için maksimum gayret gösterilmelidir.
**e)** Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
**f)** Sunucuların yazılım ve donanım bakımları periyodik olarak sistem yöneticileri tarafından yapılmalıdır.
**g)** Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve loglanmalıdır.

## 15.0 P12 AĞ CİHAZLARI GÜVENLİK POLİTİKASI

### 1.1 Amaç

Bu politika Kurumun ağındaki ağ cihazlarının sahip olması gereken minimum güvenlik konfigürasyonlarını tanımlamaktadır.

### 1.2 Kapsam

Kurumun ağına bağlı olan ağ cihazları için geçerlidir. Bilgi Sistemleri ve Teknolojileri sorumluluğundadır.

### 1.3 Politika

Bütün yönlendirici ve anahtarlar aşağıdaki konfigürasyon standartlarına sahip olmalıdır.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**a)** Bilgisayar ağında bulunan tüm cihazların MAC adres bilgileri envanterde yer almalıdır.
**b)** Yönlendirici ve anahtarlar kurumun yönetimi altında olmalıdır.
**c)** Yazılım ve firmware güncellemeleri güncel tutulmalıdır.
**d)** Bilgisayar ağında bulunan kabinetler, aktif cihazlar, UTP kabloları, cihazların portları etiketlenmelidir.
**e)** Kritik olan cihazlar erişimi kısıtlanmış sistem odalarında tutulmalıdır.
**f)** Kritik cihazların konfigürasyon bilgileri ve kritik ağ cihazları yedeklenmelidir.

## 16.0 P13 AĞ YÖNETİMİ POLİTİKASI

### 1.1 Amaç

Kurumun bilgisayar ağında yer alan bilgilerin ve ağ alt yapısının güvenliği, gizlilik, bütünlük ve erişilebilirlik kavramları göz önüne alınarak sağlanmalıdır. Yetkisiz erişimle ilgili tedbirler alınmalıdır. Ağın güvenliği ve sürekliliğini sağlamak amacıyla birtakım kontroller gerçekleştirilmelidir. Ağ Yönetimi politikası bu gereksinimleri karşılayan kuralları belirlemek amacıyla geliştirilmiştir.

### 1.2 Kapsam

Kurum bilgisayar ağının sistem ve ağ yöneticileri olan Bilgi Sistemleri ve Teknolojileri faaliyetlerini Ağ Yönetimi Politikasına uygun şekilde yürütmekle yükümlüdür.

### 1.3 Politika

Ağ yönetim politikası aşağıdaki gibidir.

**a)** Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için özel kontroller uygulanmalıdır.
**b)** Ağ üzerinde kullanıcının erişeceği servisler kısıtlanmalıdır.
**c)** İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmalıdır.
**d)** Ağ erişimi gerek duyulduğunda VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır.
**e)** Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.
**f)** Ağ üzerindeki yönlendirme kontrol edilmelidir.
**g)** Bilgisayar ağına bağlı bütün makinelerde kurulum ve konfigürasyon parametreleri kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.
**h)** Sistem tasarım ve geliştirmesi yapılırken kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmalıdır.
**i)** İnternet trafiği erişim ve kullanımı izleme politikası ve ilgili standartlarda anlatıldığı şekilde izlenmelidir.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**j)** Bilgisayar ağındaki adresler, ağa ait konfigürasyon ve diğer tasarım bilgileri 3.şahıs ve sistemlerin ulaşamayacağı bir şekilde saklanmalıdır.

**k)** Ağ üzerindeki firewalllar üzerinde, ilgili konfigürasyon dokümanlarında belirtilen servisler dışında tüm servisler kapatılmalıdır.

**l)** Bilgisayar ağıyla ilgili sorumlulukları desteklemek amacıyla ağ dokümantasyonu hazırlanmalı, ağ cihazlarının güncel konfigürasyon bilgileri saklanmalıdır.

## 17.0 P14 VERİTABANI GÜVENLİK POLİTİKASI

### 1.1 Amaç
Kurumun veri tabanı sistemlerinin, kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlar.

### 1.2 Kapsam
Tüm veri tabanı sistemleri, bu politikaların kapsamı altında yer alır.

### 1.3 Politika
Veri tabanı güvenlik politikası aşağıdaki gibidir.

**a)** Kritik verilere erişim işlemleri (okuma, değiştirme, silme, ekleme) loglanır. Log kayıtlarına, idarenin izni olmadan kesinlikle hiçbir şekilde erişim yapılamaz.

**b)** Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılır ve uygun yedekleme politikaları oluşturulur. Yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli alınması sağlanır ve yedekleme talimatına uyulur.

**c)** Bilgilerin saklandığı sistemler, fiziksel güvenliği sağlanmış sistem odalarında tutulur.

**d)** Veri tabanı sistemlerinde yapılacak bakım onarım, yama ve güncelleme çalışmalarından önce, ilgili yetkililer bilgilendirilir.

**e)** Ortaya çıkan beklenmedik durumlarda, destek için önceden belirlenmiş personel ile iletişime geçilir.

**f)** Veri tabanı sunucularına erişim şifreleri yönetim tarafından saklanır.

**g)** Bağlanacak kişilerin kendi adına kullanıcı adı verilir ve yetkilendirme yapılır.

**h)** Bütün kullanıcıların yaptıkları işlemler, loglanır.

## 18.0 P15 DEĞİŞİM YÖNETİMİ POLİTİKASI

### 1.1 Amaç
Kurumun bilgi sistemlerinde yapılması gereken konfigürasyon değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesine yönelik politikaları belirler.

### 1.2 Kapsam
Tüm bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

### 1.3 Politika

Değişim yönetim politikaları aşağıdaki gibidir.

**a)** Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.
**b)** Yazılım ve donanım envanteri oluşturularak güncel tutulmalıdır.
**c)** Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmelidir.
**d)** Değişiklikler gerçekleştirilmeden önce Bilgi Sistemleri ve Teknolojileri Birimi tepe yöneticisinden onay alınmalıdır.
**e)** Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.
**f)** Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
**g)** Teknoloji değişikliklerinin kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmelidir.
**h)** Değişiklik yönetimini işletmek için bir talep yönetim sistemi kurmak ve işletmek önemlidir. Talebin nasıl alınacağı ve değerlendirileceği gibi esaslar tanımlanmalıdır.
**i)** Değişiklik onayının, "hangi kontroller ne şekilde yapıldıktan sonra verileceği" tanımlanmalıdır.
**j)** Değişiklik öncesi test süreci tanımlanmalıdır.
**k)** Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler tanımlanmalıdır.

## 19.0 P16 GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI

### 1.1 Amaç

Bu politikanın amacı kurumun bilgisayar ağının (firewall, sunucu vs.) güvenlik açıklarına karşı taranması hususunda politika belirlemektir.

Denetim Sebepleri:

- Bilgi kaynaklarının bütünlüğü ve gizliliğini sağlamak,
- Kurumun güvenlik politikalarına uyumunun kontrolü için güvenlik açıklarının tespit edilmesi,
- Gerektiği zaman kullanıcıların veya sistemin aktivitelerini kontrol etmek.

### 1.2 Kapsam

Bu politika Kurum bünyesinde sahip olunan bütün bilgisayar ve haberleşme cihazlarını kapsamaktadır. Bu politika kurumun bünyesinde bulunan fakat kurumun sahip olmadığı herhangi bir sistemi de kapsamaktadır. Denetim yapan kişi veya kurum hizmetlerin durdurulması aktivitesi yapmayacaktır.

### 1.3 Politika

İstenildiğinde denetim yapan kurumların bireylerine erişim izni verilecektir. Kurumun birimleri denetim yapan kuruma ağ taraması yapması için protokol, adres bilgileri, ağ bağlantıları hakkında bilgi verecektir.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**Tarama Esnasında Muhatap Olan Kişi:** Kurum denetimi yapan kuruma oluşabilecek sorunlar hakkında danışabileceği bir kişiyi yazılı olarak bilgi verecektir.

**Tarama Periyodu:** Kurum ve denetimi yapan kurum denetim yapılacak zamanı yazılı olarak bildirecektir.

**Gizlilik Anlaşması:** Kurum ile güvenlik taraması yapacak kurum, tarama sonucunda elde edilecek bilgilerin hiçbir şekilde üçüncü şahıslara aktarılmayacağına dair gizlilik anlaşması yapacaklardır.

## 20.0 P17 SANAL ÖZEL AĞ (VPN) POLİTİKASI

### 1.1 Amaç
Bu politikanın amacı VPN protokolünün kullanımı hakkındaki standartları belirlemektir.

### 1.2 Kapsam
Bu politika VPN ile müşteri ağına bağlanacak kurumları, 3. tarafları, geçici çalışanları ve diğer bütün personeli kapsamaktadır

### 1.3 Politika

Kurum yetkili çalışanları, geçici çalışanlar ve üçüncü şahıslar VPN'in faydalarından yararlanabilirler. Buna ek olarak,

**a)** VPN kullanım hakkı verilen kişiler yetkisiz kişilere bu hakkı kullandırmaması için gerekli tedbirleri almakla sorumludur.
**b)** Kurum ağına bağlanıldığında, PC'den çıkan ve giren trafik sadece VPN kanalından iletilecektir.
**c)** Çift tünel sistemine izin verilmeyecektir, sadece tek ağ bağlantısına izin verilecektir.
**d)** Kuruma ait bilgisayarlara sahip olmayan kişiler Kurumun VPN ve ağ politikalarına uygun bir şekilde cihazlarını konfigüre edeceklerdir.
**e)** Sadece kurumun onay verdiği kullanıcılar VPN'i kullanabileceklerdir.

## 21.0 P18 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

### 1.1 Amaç
Kurumun bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarını tanımlamaktır.

### 1.2 Kapsam
Kurum bilgi sistemlerine erişen personel ile kurum dışı kullanıcılar bu politika kapsamı altındadır.

### 1.3 Politika
**a)** Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenmelidir.
**b)** Kurum sistemlerine erişmesi gereken kurum kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanmalıdır.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**c)** Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve logon olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, denetim altında tutulmalıdır.
**d)** Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
**e)** Kullanıcılar da kurum tarafından kullanımlarına tahsis edilen sistemlerin güvenliğinden sorumludur.
**f)** Sistemlerin başarılı ve başarısız erişim logları düzenli olarak tutulmalı, tekrarlanan başarısız logon girişimleri incelenmelidir.
**g)** Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
**h)** Sistemlere bağlanan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.

## 22.0 P19 BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI

### 1.1 Amaç
Bilgi Sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekir. Bu politika yedekleme kurallarını tanımlamaktadır.

### 1.2 Kapsam
Tüm kritik bilgi sistemleri ve bilgi sistemlerinin işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.

### 1.3 Politika
Bilgi sistemleri yedekleme politikası aşağıdaki gibidir.

**a)** Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekmektedir.
**b)** Verinin operasyonel ortamda kritikliğine göre online veya offline yedekleri alınmalıdır. Taşınabilir ortamlar fiziksel olarak bilgi işlem odalarından farklı odalarda ve güvenli bir şekilde saklanmalıdır.
**c)** Kurumsal kritik verilerin saklandığı sistemler ile sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme yapısı dokümante edilmelidir.
**d)** Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
**e)** Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
**f)** Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
**g)** Yeni sistem ve uygulamalar devreye alındığında yedekleme listeleri güncellenmelidir.
**h)** Yedekleme işlemi için geçerli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**i)** Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
**j)** Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dahilinde tamamlanabileceğinden emin olunması gerekir.
**k)** Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
**l)** Yedekleme standardı ile doğru ve eksiksiz yedek kayıt kopyalarının bir felaket anında etkilenmeyecek bir ortamda bulundurulması gerekmektedir.
**m)** Veri Yedekleme Standardı; yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği belirlenmelidir.

## 23.0 P20 YAZILIM GELİŞTİRME

### 1.1 Amaç

Yazılım Geliştirme üzerindeki kontroller, kurumların günlük operasyonlarını yürütmek için kullandıkları yazılımların oluşturulması esnasında kullanılan kontrol mekanizmalarıdır. Programların geliştirilmesi esnasında uygulanması gereken kontroller, yazılımların kontrollü bir şekilde geliştirilmesini sağlamayı hedeflemektedir. Bu şekilde güvenlik kriterlerinin hem yazılımın geliştirilmesi aşamasında hem de geliştirilen yazılım uygulamaya alındıktan sonra gözetilmesi sağlanır. Bu politika yazılım geliştirme hakkındaki kriterleri ortaya koymaktadır.

### 1.2 Kapsam

Bu politika kurumda yazılım geliştirme alanında faaliyet gösteren kişi ve kurumları kapsamaktadır.

### 1.3 Politika

Yazılım geliştirme üzerindeki kontroller şu temel kriterlere uygun şekilde oluşturulmalıdır.

**a)** Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.
**b)** Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje alt yapısının uygun olduğundan emin olmalıdır.
**c)** İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.
**d)** Sistem geliştirmede, ihtiyaç analizi fizibilite çalışması, tasarım, geliştirme, test ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.
**e)** Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.
**f)** Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak ilgili yönetim tarafından verilmelidir.
**g)** Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.
**h)** Yazılımlar envanterleri çıkarılarak muhafaza edilmelidir.

## 24.0 P21 KABUL EDİLEBİLİR KULLANIM POLİTİKASI

### 1.1 Amaç

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

Kabul Edilebilir Kullanım Politikasının amacı, Kurum personelinin sistem, bilgi ve varlıkların gizlilik, bütünlük ve erişilebilirlik özelliğini garantilemek için yapması ve uyması gereken iş kurallarını kendilerine iletmektir.

**1.2 Kapsam**

Bu politika; Kurum personeli ve Yükleniciler için olup tüm kurum bilişim etkileşimli kritik bilgi varlıklarını kapsar.

**1.3 Politika**

**a)** Güvenlikten, İstinye Üniversitesi personeli, iş yapan Yüklenici Kurumlar ve İlgili tüm personel, kendi alanlarına ait Güvenlik Politikalarına uymak zorundadır.

**b)** Bilgi Güvenliği Politikaları, İstinye Üniversitesi tarafından çalışanlarına, yeni işe başlayanlara ve Yüklenici kurumlara duyurulacaktır.

**c)** İstinye Üniversitesi ortamında tutulan ve iletilen tüm bilgiler; kurumun malıdır ve bu bilgileri izleme ve denetleme hakkına sahiptir.

**d)** İstinye Üniversitesi'nin gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Kurumun iş gereksinimi dışında bu bilgilerin kopya edilmesi ve iletilmesi yasaktır.

**e)** İstinye Üniversitesi personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş güvenlik cihazlarını korumaktan sorumludur. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.

**f)** Hiçbir personel, bilgisayarlarından anti virüs koruma yazılımını devre dışı bırakamaz.

**g)** Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.

**h)** Hiçbir personel izin almadan kendi PC' sinden veya başka bir kaynak kullanarak, İstinye Üniversitesi'nin Bilişim Ağını tarayamaz, izleyemez veya dinleyemez.

**i)** İstinye Üniversitesi onaylı resmi Penetrasyon testleri haricinde, bilgisayar sunucuları için içeriden veya dışarıdan port taraması yapılması yasaktır.

**j)** Hiçbir personel, kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.

İstinye Üniversitesi adına iş yapan Yüklenici Kurum personeli; İstinye Üniversitesi'nin izni ve onayı olmadan İstinye Üniversitesi'nin bilgilerini başkaları ile paylaşamaz. İstinye Üniversitesi izni olmadan iç ağ ve internet üzerinden bilişim ağlarını tarayamaz ve Penetrasyon testleri gerçekleştiremez.

**1.4 Yaptırım**

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

## 25.0 P22 ORTAMIN ELDEN ÇIKARILMASI POLİTİKASI

**1.1 Amaç**

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

Bilgilerin yedeklendiği, taşındığı, dolaşıma sunulduğu ortamların, ortamlarda taşınan verilerin uygunsuz kişilerin kullanımına geçmemesi, üçüncü şahıslara yönelik hukuki süreçleri başlatmaması, hassas bilgi içeren bilginin izinsiz kişilere sızmasını minimuma indirmek için elden çıkarılmasının kurallarını ortaya koymak.

**1.2 Kapsam**
Basılı, yazılı her tür ortamın amaç maddesindeki çekinceler çerçevesinde elden çıkarılması, değiştirilmesi veya dönüştürülmesidir.

**1.3 Politika**
Bu politika aşağıdaki 2 başlıkta ele alınmıştır.

**1.3.1 Kağıt Ortam**

Kayıtların Kontrolü Prosedürüne göre Yönetim Temsilcisi saklama süresi dolan kayıtları İmha Tutanağı imzalayarak imha eder.

**1.3.2 Elektronik Ortam**

**a)** CD, DVD, disket, harici hard disk, flash bellek gibi taşınabilir ortamlar aşağıdaki seçeneklerine göre elden çıkarılırlar. Elden çıkarma sırasında İmha Tutanağı imzalanarak dosyalanırlar.
**b)** Yaşam süresini doldurmuş her türlü veri içeren ortam tekrar kullanılamayacak şekilde belirlenmiş yöntemlerle imha edilmeli ve 3.tarafların eline geçmemesi sağlanmalıdır.

**1.4 DÖKÜMANLAR**
İmha Tutanağı

## 26.0 P23 TEÇHİZATIN ELDEN ÇIKARILMASI POLİTİKASI

**1.1 Amaç**
Sisteme bağlı ya da bağlı olmayan sunucu ve ağ cihazlarının elden çıkarılmasının nasıl yapılacağını açıklar.

**1.2 Kapsam**
Sistemden çıkartılacak sunucu, bilgisayar ve ağ cihazlarını kapsar.

**1.3 Politika**
Yaşam süresi tamamlamış ya da işlev görmez hale gelmesi sebebiyle elden çıkarılacak her türlü bilgi teknolojileri ekipmanı uygun olarak elden çıkarılmalıdır.

Elden çıkarılacak tüm donanımların bilgi depolayan kısımları sökülerek imha edilmelidir ve imha Tutanağı imzalayarak kayıt altına alınmalıdır.

**1.4 DÖKÜMANLAR**
İmha Tutanağı

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

## 27.0 P24 TEMİZ MASA TEMİZ EKRAN POLİTİKASI

### 1.1 Amaç
Bu politikanın amacı çalışanların mesai saatleri içi veya dışında kendilerine görevleri gereği paylaşılmış olan bilgilerin yetkisiz erişimler veya uygunsuz kullanımı sonucunda basına gelebilecek riskleri ortadan kaldırmaktır.

### 1.2 Kapsam
Çalışma masaları, ekranlar, basılı dokümanlar, belgeler, kayıtlar.

### 1.3 Sorumluluklar
Tüm çalışanların bu politikaya uygun hareket etmesinden tüm çalışanlar sorumludur.

### 1.4 Politika
**a)** Çalışma sonunda kâğıt ortamında ya da elektronik cihazlar üzerinde tutulan "gizli ya da çok gizli" bilgiler güvenlikli ortamlarda (kilitli güvenli ortamlar vb.) saklanmalıdır.

**b)** Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler belirlenmiş yöntemlerle imha edilmelidir.

**c)** Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) yetkisiz erişimlere bırakılmamalıdır. Cihazlar üzerinde belge, doküman bırakılmamalıdır.

**d)** Her türlü ekrandan ulaşılabilen bilgiler, şifreler, anahtarlar ve kodlar, bilginin sunulduğu sistemler, ana makineler (sunucu), PC'ler vb. cihazlar şifresiz kullanılmamalıdır

**e)** Ekranlarda çalışılmaması durumunda devreye girecek ekran koruması (parola) tüm PC'lerde, notebooklar da etkinleştirilmelidir.

**f)** Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir.

**g)** Hassas bilgiler içeren evraklar, bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir.

## 28.0 P25 KRİPTOGRAFİK KONTROLLER POLİTİKASI

### 1.1 Amaç
Bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunmasıdır.

### 1.2 Kapsam
Bu politikanın uygulanmasından tüm çalışanlar sorumludur.

### 1.3 Politika
Kriptografik kontroller aşağıdaki maksatlarla kullanılır;

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**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.
**d)** Personelin gönderdiği maillerde, hiçbir şekilde yönetici, kullanıcı gibi hesap şifreleri bulundurulmamalıdır.
**e)** İnternete açık kritik veri içeren uygulamalara kriptolu (şifreli) bağlantı ile bağlanılmalı, kripto (şifre) kullanmayan yöntemler tercih edilmemelidir. Düz metin kullanarak veri alışverişi yapan yöntemlerin kullandığı portlar gerekirse kapatılmalıdır.
**f)** Kripto kullanımı ile hangi iş bilgisinin korunacağı ile ilgili genel prensipler belirlenmelidir.
**g)** Taşınabilir ortam, cihaz ve iletişim hatlarında iletilen hassas bilginin korunması için şifreleme mekanizmalarının kullanımı belirlenmelidir.
**h)** Organizasyon çapında etkin bir uygulama için uyarlanması gereken standartlar ortaya konulmalıdır.
**i)** Kriptografik anahtarların korunması, şifrelenmiş bilginin kaybolması, tehlikeye düşmesi veya hasar görmesi durumunda tekrar geri alınması ile ilgili metotları içeren anahtar yönetimi uygulanmalıdır.
**j)** Politikanın uygulanması, anahtar üretimini de içeren anahtar yönetimi ile ilgili görevler ve sorumluluklar belirlenmelidir.

## 29.0 P26 ZİYARETÇİ KABUL POLİTİKASI

### 1.1 Amaç
Bu politikanın amacı Kuruma dışarıdan gelen misafirlerin kabulü, kuruluş içinde dolaşmaları ve kuruluştan uğurlanmaları ile ilgili kuralları belirlemektir.

### 1.2 Kapsam
Bu politikanın uygulanmasından başta Bilgi Sistemleri ve Teknolojileri ve tüm çalışanlar sorumludur.

### 1.3 Politika
Ziyaretçi Kabul politikası aşağıdaki gibidir.

**a)** Dışarıdan ziyaret amaçlı gelen kişiler kuruluş girişinde güvenlik tarafından karşılanır ve ziyaret edeceği idarecinin onayı ile kuruluşa kabulü yapılır.

**b)** Gelen ziyaretçi Müdürlük seviyesinde ziyaret gerçekleştiriyorsa Güvenlik tarafından ziyarete geldiği kişiye kadar getirilir.

**c)** Ziyaretçiler sadece toplantı odalarında ve personel odalarında ağırlanır.

**d)** Dışarıdan ziyaret amaçlı gelen kişiler yönetim ofisleri, arşiv odası ve sistem odası gibi yerlere alınmamalıdır.

**e)** Kargo elemanları teslimatlarını güvenliğe teslim etmelidirler. Bunun dışında kuruluşa girişleri yasaktır.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**f)** Ziyarete gelen kişiler ile ilgili bilgiler Güvenlik tarafından ziyaretçi takip sistemi ile kaydedilir.

**1.4 Yaptırım**
Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

## 30.0 P27 TAŞINABİLİR CİHAZ POLİTİKASI

**1.1 Amaç**
Bu politikanın amacı İstinye Üniversitesine ait bilgi içeren taşınabilir cihazların kullanımı ile ilgili kuralları belirlemektir.

**1.2 Kapsam**
Bu politikanın uygulanmasından İstinye Üniversitesi'nin tüm yönetici ve çalışanlar sorumludur.

**1.3 Politika**
Kuruluşa ait bilgi içeren taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilir.

**a)** Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.

**b)** Kuruluşa bilgisayar, taşınabilir bellek ve PDA cihazlara dışarıdan herhangi bir yazılım, siyasi propaganda, ırkçılık, şiddet, pornografi veya erotizm içeren resim, film veya müzik kopyalanamaz ve cihaz içerisinde bulundurulamaz.

**c)** Kuruluş telefon hatları ve bilgisayarlar üzerinden üçüncü taraf kişilerle borç alacak ilişkisi, tehdit, küfür, kuruluş itibarını zedeleyecek şeyler ve yasa dışı olan iletişim kurulamaz.

**d)** Bilgisayarlar ve PDA cihazlar üzerindeki anti virüs programları hiçbir nedenle devre dışı bırakılamaz.

**e)** Taşınabilir bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar olanaklar dahilinde ağ üzerinde ilgili adrese kaydedilmelidir.

**f)** Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

## 31.0 P28 BİLGİ VE YAZILIM ALIŞVERİŞİ POLİTİKASI

**1.1 Amaç**
Bu politikanın amacı İstinye Üniversitesi ve diğer organizasyonlar arasında gerçekleşebilecek herhangi bir bilgi kaybı, değişikliği veya yanlış kullanımı önlemektir.

**1.2 Kapsam**
Bu politikanın uygulanmasından tüm çalışanlar sorumludur.

**1.3 Politika**

**a)** Organizasyon, elektronik transferlere yönelik logların tutulmakta olduğundan emin olmalıdır.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**b)** Organizasyonun yazılımlarını veya verilerini kullanmakta olan üçüncü taraflar, gerekli koruma ölçütlerini içeren bir yazılı sözleşme imzalamalıdır. Böylece üçüncü tarafların söz konusu bilgiyi izinsiz kullanması, değiştirmesi veya çoğaltması engellenmiş olacaktır.
**c)** Elektronik ortamda sözleşmenin yapıldığı üçüncü taraflarla, kağıt üzerinde de anlaşma yapılmalıdır.
**d)** Bilgi ve veri alışverişinden önce dış tarafların kimliklerinin tespit edilmesi gerekir.
**e)** 3. Şahıslar ya da tedarikçiler ile yapılacak dosya paylaşımları kurum içinde konumlandırılmış olan dosya paylaşım sistemleri üzerinden yapılmalıdır.
**f)** Üçüncü taraflara yollanan bilgisayar ortamı yeni olmalı veya herhangi bir bilgi içermemelidir.
**g)** Yetkisi olmayan çalışanlar tarafından gönderilen e–mailler, organizasyonu bağlamaz.
**h)** İş iletişiminin sağlanması için sadece organizasyon tarafından yetkilendirilen çalışanların e–mail adresleri kullanılmalıdır.
**i)** Organizasyon web sitesinin korunması sağlanmalıdır.
**j)** Gizli bilgiler sadece uygun data serverlarda kayıt altına alınmalıdır.
**k)** Yazılım yükleme veya yazılım güncellemelerini yapma ve sistem bakımını gerçekleştirme yetkisi sadece Bilgi Sistemleri ve Teknolojilerindedir.
**l)** Kritik bir dosyada çeşitli değişikliklerin yapılması durumunda, dosyanın yedeği alınmalıdır.
**m)** Organizasyonda bilgi sistemleri aracılığı ile gönderilen mesajlar, saldırgan veya ayrımcılık içeren bildiriler içermemelidir. Organizasyonun bilgi sistemi sadece iş gereklilikleri için kullanılmalıdır.
**n)** Bir e – mail'e gizlilik içermekte olduğuna dair bir not eklendiğinde, bu mesajı sadece e – mailin gönderildiği kişinin maili aldığından emin olunmalıdır.
**o)** E – mail'lerde taranmış imzalar bulunmamalıdır.
**p)** Organizasyonun çalışanları çeşitli tartışma gruplarına katılmamalıdır.
**q)** E – mail yoluyla gönderilen bilgiler, bu bilginin kimden gelmekte olduğunu içermelidir.
**r)** E – mail yoluyla gönderilen bilgiler, spesifik bir geri dönüş adresi içermelidir.
**s)** Gizlilik içeren bilgiler, handsfree telefonlarda görüşülmemelidir.
**t)** Silinebilir ortamlara kaydedilmiş olan gizli bilgilerin kullanımdan sonra silinmesi gerekir.
**u)** Gizlilik içeren bilgiler telefon aracılığı ile paylaşılmamalıdır.
**v)** Çalışanlar gizlilik içeren bilgileri telesekreterlere veya sesli mesajlaşma sistemlerine kaydetmemelidir.
**w)** Toplantılarda yapılan video konferanslar, yönetim veya katılımcılar tarafından izin verilmedikçe kaydedilmemelidir.
**x)** İşle ilgili tüm aramalar kuruluş telefonları kullanımı ile yapılmalıdır.
**y)** Gizlilik içeren bilgilerin umumi yerlerde konuşulmaması gerekir.
**z)** Bilgi sistemleri sadece iş için kullanılmalıdır.
**aa)** Gizli bilgilerin cep telefonlarında veya telsizler aracılığı ile paylaşılması kesinlikle yasaktır.
**bb)** Üçüncü taraflar, kuruluşta bir toplantıya katılmak durumunda olduklarında, bu kişilerin gizli bilgiler barındıran bölgelerde dolaşması engellenmelidir.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**cc)** Gizli bilgilerin bir toplantıda tartışılması durumunda, toplantı süresince, bu bilginin gizli olduğu ve dinleyenlerin bu bilginin gizliliğini korumaları gerektiği belirtilmelidir.

**dd)** Kuruluşun intranetine yerleştirilen her bilgi veya uygulama daha önceden yetkili kişiler tarafından onaylanmalı ve kuruluşun malı olarak kalmaya devam etmelidir. Bu bilgiler kuruluşun bilgileri olarak saklı tutulacaktır.

**ee)** Kuruluş içindeki donanım malzemelerin yerini değiştirmek için Bilgi Sistemleri ve Teknolojileri Ekibinden izin alınmalıdır.

### 1.4 Yaptırım

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise insan kaynakları yönetmeliğince belirlenmiş disiplin süreçleri tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

## 32.0 P29 ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI

### 1.1 Amaç

Bu politikanın amacı İstinye Üniversitesi'nin bilgi varlıklarının ve bilgi işleme tesislerine üçüncü taraflar tarafından ulaşılması durumunda güvenliğini sağlamaktır.

### 1.2 Kapsam

Bu politikanın uygulanmasından İstinye Üniversitesi ve Bilgi Sistemleri ve Teknolojileri sorumludur.

### 1.3 Politika

**a)** Kurum dışından gelen bakım ve tamir çalışanları, diğer tedarikçilerde de olduğu gibi, kurum içinde olduğu süre boyunca bir gizlilik anlaşması imzalamalıdır.

**b)** Sadece uygun yetkileri almış olan çalışanların organizasyonun bilgi veya iletişim sistemlerine erişimi vardır.

**c)** Üçüncü taraflarla herhangi bilgi alışverişi yapılmadan önce bir gizlilik anlaşması yapılmalıdır.

**d)** Üçüncü taraflara kurumun ağına erişim izni verilmeden önce bilgisayarlarını güvenliğe almaları gerekir. Kuruluş, üçüncü taraflara herhangi bir uyarıda bulunmadan ağa olan erişimlerini kesebilir.

**e)** Kuruluş isminin halka yayınlanacak dokümanlarda kullanılabilmesi için üçüncü tarafların uygun kişiler tarafından yetkilendirilmesi gerekir.

**f)** Tedarikçiler kuruluşun sistemlerine erişmeden önce koşulların tanımlanmakta olduğu bir gizlilik anlaşması imzalanmalıdır.

**g)** Gizli bilgilerin dağıtımı gereken durumlarda üçüncü taraflara bu bilgileri iletilmeden önce gizlilik sözleşmesi imzalatılmalı, sonrasında bu bilgiler paylaşılmalıdır.

## 33.0 P30 VARLIKLARA YÖNELİK SORUMLULUK POLİTİKASI

### 1.1 Amaç

Bu politikanın amacı İstinye Üniversitesi'nin, organizasyonel varlıklarının uygun koruma yöntemlerini belirlemektir.

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

**1.2 Kapsam**
Bu politikanın uygulanmasından Bilgi Sistemleri ve Teknolojileri sorumludur.

**1.3 Politika**
Varlıklara yönelik sorumluluk politikası aşağıdaki gibidir.

**a)** Her sene bir bilgi sistemleri envanteri yapılmalı ve bu konuda görevlendirilmiş kişiye bu liste verilmelidir. Bu çalışmanın amacı kuruluşun varlıklarını tespit etmek ve bu varlıkların kaybedilmesinin engellenmesini sağlamaktır.
**b)** Yeni üretilen bilginin bir sahibinin belirlenmesi ve bu bilginin uygun biçimde sınıflandırılması gerekir.
**c)** Satın alınacak herhangi bir yazılım veya donanım Bilgi Sistemleri ve Teknolojileri ile satın alınması ve bilgi güvenliği standartları ile uyumlu olması gerekir.
**d)** Organizasyonun sahip olduğu tüm sistemlerin yönetimi, kullanıcı ayrıcalıklarının takibi ve erişim kontrol loglarının izlenmesi Bilgi Sistemleri ve Teknolojileri tarafından yapılmalıdır.

## 34.0 P31 BASILI ÇIKTI VE DAĞITIM POLİTİKASI

**1.1 Amaç**
Bu politikanın amacı İstinye Üniversitesinde basılı bilgisayar çıktısı ve dağıtılması ile ilgili kuralları tanımlamaktır.

**1.2 Kapsam**
Bu politikanın uygulanmasından tüm çalışanlar sorumludur.

**1.3 Politika**
Basılı çıktı ve dağıtım politikası aşağıdaki gibidir.

**a)** Tüm kritik bilgisayar raporlarının; bilginin hassasiyet seviyesine göre bir güvenlik sınıflandırma değeri olacaktır. Sınıflandırmayı bilgi sahibi kendisi yapacaktır.
**b)** Kâğıt ortamında basılı "Gizli" tanımlı raporların sadece hitap edilen kullanıcıya ulaştırılmasını güvence altına alacak metotlar belirlenecektir.
**c)** Kritik raporların dökümünü alan kullanıcı, rapor içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.
**d)** Herhangi bir kişi kendine ait olmayan kritik bir dokuman bulur ise olay bildiriminde bulunur ve doküman ilgilisine iletilir.
**e)** "Gizli Sınıflandırmasına tabi" kâğıt belgeleri kilitli dolap ve kasalarda muhafaza edilecektir.
**f)** "Gizli Sınıflandırmasına tabi" kâğıt bilgileri faks ile iletilmeyecektir.
**g)** "Gizli Sınıflandırmasına tabi" bilgi içeren çıktılar ağ ortamında paylaşılmış yazıcılardan yazdırılıyorsa yazdırma işini başlatan kullanıcı beklemeden yazdırılan belgenin bulunduğu alana gidecek ve çıktının başkaları tarafından görülmesine imkan vermeyecektir.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

**1.4 Yaptırım**
Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

## 35.0 P32 BİLGİ SINIFLANDIRMA POLİTİKASI

**1.1 Amaç**
Bu politikanın amacı İstinye Üniversitesi'nin bilgi varlıklarını uygun koruma altına alınmasını sağlamaktır.

**1.2 Kapsam**
Bu politikanın uygulanmasından tüm çalışanlar sorumludur.

**1.3 Politika**
Bilgi sınıflandırma politikası aşağıdaki gibidir.

**a)** 3.Taraf veya kuruluşun personeline yönelik tehlike arz eden herhangi bir ürün veya hizmet, bu tehlikenin doğasını açıklayacak biçimde tanımlanmalıdır.
**b)** Tüm bilgiler, aksi onaylanmadığı sürece gizli bilgi olarak nitelendirilmelidir.
**c)** Bir depolama ortamının çeşitli seviyelerde gizlilik içermesi durumunda, en yüksek gizlilik seviyesi içeren bilgiler öncelikli olarak kabul edilir.
**d)** Kullanıcılar, Bilgi Sistemleri ve Teknolojilerinin sağlamış olduğu olanaklar dahilinde kendi bilgisayarlarının yedeklerini almaktan veya aldırmaktan sorumludur.
**e)** Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
**f)** Sistemlere logon olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir. Kullanıcı haklarını izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
**g)** Fotokopi cihazlarını kullanan İstinye Üniversitesi çalışanları cihazlar üzerinde bırakmış olduğu dokümanlardan sorumludur.
**h)** Kişiler tarafından yazılmış herhangi bir resmi dokümanın silinmez mürekkeple yazılması ve uygun şekilde işaretlenmesi gerekir. Yapılacak herhangi bir değişikliğin altı çizilmeli, tarihlenmeli ve yeniden onaylanmalıdır.
**i)** Gizli dokümanların tüm sayfaları numaralandırılmalıdır.

**1.4 Yaptırım**
Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

## 36.0 P33 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI

**1.1 Amaç**

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |

Bu politikanın amacı İstinye Üniversitesi'nin bilgi güvenliği olay ihlal süreçlerini belirler.

**1.2 Kapsam**
Bu politikanın uygulanmasından tüm personel sorumludur.

**1.3 Politika**
Olay ihlal bildirim ve yönetim politikası aşağıdaki gibidir.

**a)** Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.
**b)** Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
**c)** Bilgi güvenliği ihlali oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.
**d)** Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır. İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
**e)** Güvenlik ihlaline neden olan taraflarla ilgili resmi bir disiplin sürecine başvurulmalıdır.
**f)** Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor etmelidir.
**g)** Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, DDOS atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlalleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınmalıdır.
**h)** Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.
**i)** İç problem analizi, adli incelemeler veya üretici kurumdan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.
**j)** Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.
**k)** Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.
**l)** Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;

- Kanıtın mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,
- Kanıtın niteliği ve tamlığını gösteren ağırlığı.

**1.4 Yaptırım**

| Hazırlayan | Onaylayan |
|---|---|
| **BGYS YÖNETİM TEMSİLCİSİ** | **GENEL SEKRETER** |

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

| Hazırlayan | Onaylayan |
|---|---|
| BGYS YÖNETİM TEMSİLCİSİ | GENEL SEKRETER |