SİSTAŞ SAYISAL İLETİŞİM SAN. VE TİC. A.Ş.

SAHİBİ: Bilgi Güvenliği Ekibi

ONAYLAYAN: Yönetim Kurulu Başkanı

İçindekiler

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.

Kapsam

Firmanın satış, teknik destek ile idari faaliyetlerini ve bu faaliyetlerine ilişkin bilgi varlıklarını, bu varlıkların korunması amacıyla yürüttüğü bilgi güvenliği kapsamındaki ilgili iş süreçlerini kapsar.

- **İç Kapsam**

  İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler;

  SİSTAŞ bünyesinde bulunan Bilgi Sistemleri ve Teknolojileri birimini kapsar.

  Yerine getirilecek politikalar, hedefler ve stratejiler;

  - BGYS Politikaları,
  - Yönetimce belirlenmiş yıllık BGYS hedefleri,
  - Bilgi Güvenliği Yönetim Sisteminin kurulması, işletilmesi ve sürdürülmesi için Yönetim 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;
    - İdari Personel
    - Teknik Personel

- **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,
  - Üst Yönetim dahil tüm SİSTAŞ çalışanları,

Giriş

Bilgi sistemleri ve teknolojileri sürekli gelişmekte, yenilenmektedir. Gelişen teknoloji; kurumlara donanım, işletim sistemleri, ağ yapıları ve birçok uygulamada çeşitlilik sağlamaktadır.

Bilgi sistemlerinin yapısının, Şirket'in ölçeği, faaliyetlerin ve sunulan ürünlerin niteliği, çeşitliliği ve stratejik hedefleri ile uyumlu olması; bilgi sistemleri ile içerdiği verinin güvenilir, doğru, eksiksiz, izlenebilir, tutarlı, erişilebilir ve ihtiyaçları karşılayacak nitelikte oluşturulması esastır. Bilgi sistemleri asgari olarak;

- Şirket'le ilgili tüm bilgilerin yurt içinde elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanılmasına veya yedeklenmesine ve kullanılmasına,
- Sızma testi yapılabilmesine,
- Muhasebe kayıtlarının Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurulu tarafından belirlenen usul ve esaslara uygun şekilde muhasebeleştirilmesine imkân verecek yapıda tesis edilir.
- Bilgi sistemlerinin sürekli biçimde işlerliğini sağlamak üzere iş sürekliliği planı oluşturulur. Söz konusu planın işlerliği ve yeterliliği düzenli olarak test edilir; ihtiyaç duyulması halinde gerekli tedbirler alınır. İş sürekliliğinin planlanmasında, kritik bilgi teknolojileri varlıkları ile süreçleri belirlenir; bunlara ilişkin iş etki analizi ile risk değerlendirmesi yapılır.
- Bilgi sistemleri ile içerdiği verinin güvenli biçimde saklanması esastır. Bu çerçevede, veriler, güvenlik hassasiyet derecelerine göre sınıflandırılır, her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilir ve buna göre yedeklenir. Bilgi sistemlerinin güvenliği ve yedekleme sistemlerinin işleyişi düzenli olarak test edilir ve test sonuçlarına göre ihtiyaç duyulması halinde gerekli değişiklikler yapılır.
- Bilgi sistemlerinin geliştirilmesi, test edilmesi ve işletilmesi süreçlerinde görevler ayrılığı ilkesi uygulanır. Bilgi sistemleri yönetim sürecinde görev alan bölüm ve çalışanların görev, yetki ve sorumlulukları yazılı olarak belirlenir. Görevler ayrılığı ilkesine uygunluk düzenli olarak test edilir;
- Faaliyetlerin yürütülmesi sırasında bilgi sistemleri aracılığıyla edinilen ve saklanan müşteri ve Şirket bilgilerinin gizliliğini sağlamak esastır. Müşteri bilgilerinin, yasalarla

yetkili kılınmış merciler dışındaki taraflarla paylaşımına ilişkin uygulama esasları yazılı olarak belirlenir.

- Bilgi sistemleri kullanılarak gerçekleştirilen ve şirket faaliyetlerine ait kayıtlarda değişikliğe neden olan işlemlere ilişkin olarak yeterli detayda ve açıklıkta denetim izleri oluşturulur. Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli tedbirler alınır.

Kurumlar bilgi sistemlerini organize ederken bazı standartlar belirlemelidir. Bu standartlar, bilginin korunması, bütünlüğünün sağlanması, gizliliği, erişebilirliği dikkate alınarak hazırlanır. Bilginin iç ve dış taraflar arasında iletimi, internet üzerinden erişilebilir olması, elektronik ortamda tutulması bilgi güvenliği risklerini artırmakta dolayısıyla korumak için gerekli standartlarında çoğaltmaktadır.

Bu doküman; Sistaş Sayısal İletişim'de uyulması gereken standartlar ve talimatları içermektedir. Bu standartlar aşağıda belirtilen amaçları taşımaktadır.

- Bilgi sistemlerinde gizlenen, paylaşılan, idari ve mali verilerin güvenliğini sağlamak.
- Teknolojik ekipmanları korumak
- İş sürekliliğini sağlamak
- Yatırımları korumak
- Kanuni riskleri önlemek
- Kurumun itibarını korumak

Bu Bilgi Güvenliği Politikası bu kurumun tüm çalışanlarını ilgilendirmektedir. Her çalışan politikaları dikkatle okuyup, kendisine uygun olan bölümleri tatbik etmek zorundadır.

Tanımlar

BGYS: Bilgi Güvenliği Yönetim Sistemi.

Envanter: Kurum için önemli olan her türlü bilgi varlığı.

Üst Yönetim: SİSTAŞ; Yönetim Kurulu.

Birim/Bölüm Yöneticisi: SİSTAŞ; Genel Müdür Yardımcısı

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; SİSTAŞ'ın yürüttüğü hizmet süreçlerini sürdürebilmesi için önemli olan varlıklardır. Bu politikaya konu olan süreçler ve 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,
- İlgili bölüm/birimlerin çalışanları,

1. Güvenlik Politikası

Üst yönetim tarafından onaylanmış bir bilgi güvenliği politikası oluşturulmuştur. Bu politika üst yönetimin bilgi güvenliği yönetimi ile ilgili taahhüdünü ve kurumsal yaklaşımını yansıtmaktadır.

Şirket Bilgi Güvenliği Politikası ile

- Kişisel bilginin mahremiyetinin korunmasını sağlamak amacıyla müşteri ve personel bilgilerinin gizliliğini korur.
- Bilginin bütünlüğünü koruyacak ve sürekli erişilebilirliğini garanti altına alacak altyapıyı ve kontrolleri hayata geçirir.
- Tasarım, geliştirme, test ve uygulama süreçlerinde görevler ayrılığı prensibine uygun yetkilendirmeyi sağlar ve kritik işlemlerde onay mekanizması tesis eder.
- Geliştirme, Test ve Üretim ortamlarının fiziksel ve mantıksal olarak ayrılmasını sağlar
- Kullanıcıların yetkilendirilmesinde gerekli olan minimum yetkilendirme prensibinin sağlanması ve yetkilerin düzenli olarak kontrol edilmesini sağlar.
- Dış ağlardan gelebilecek tehditlere karşı ağ güvenliğini tesis eder.
- Internet sayfası aracılığıyla sunduğu hizmetlerde, servisin şirket tarafından sağlandığını doğrulayacak teknikler kullanır.
- Bilgi güvenliği faaliyetlerinin yönetilmesini ve koordinasyonunu sağlamak amacıyla bir bilgi güvenliği organizasyonu oluşturur.
- Tüm personele yeterli seviyede farkındalık programı uygular ve bilgi güvenliği gerekliliklerinin karşılanması için tüm çalışanların katılımını sağlar.
- Bilginin işlendiği alanlarda bilginin güvenliğinin sağlanabilmesi amacıyla gerekli fiziksel ve çevresel güvenlik önlemlerini alır.
- Bilgi sistemleri edinim, geliştirme ve bakımında güvenlik gerekliliklerinin neler olduğunu belirler ve hayata geçirir.
- Belirlenen bilgi güvenliği politikalarına, süreçlerine, yasal ve düzenleyici zorunluluklara çalışanların uymalarını yazılı taahhütlerini alarak zorunlu tutar.
- İş faaliyetlerindeki kesintileri önlemek ve bilgiye sürekli erişimi sağlamak için iş sürekliliği faaliyetleri gerçekleştirir.
- Bilgiye erişimi kontrol etmek ve yetkisiz erişimleri önlemek için ilgili tüm alanlarda gerekli güvenlik kontrollerini hayata geçirir.

2. Bilgi Güvenliği organizasyonu

Şirket yönetimi bilgi güvenliği organizasyonunu Şirket bünyesinde oluşturur. Bu kapsamda Şirket'te güvenlik politikalarının bütünsel bir yaklaşımla oluşturulması, sürdürülmesi ve yönetilmesine ilişkin çalışmalar Bilgi Güvenliği Yönetim Süreci kapsamında yürütülür.

Şirket'in güvenlik kontrol süreçlerini koordine edecek, yönetecek rol ve sorumluluklar Bilgi Güvenliği Rol ve Sorumluluklar Yönetmeliği kapsamında belirlenir ve ilgili kişilere atanır.

3. Bilgi güvenliği rol ve sorumlulukları

Bilgi Güvenliğinin Şirket'te planlanması, uygulanması ve kontrol edilmesi faaliyetlerini gerçekleştirmek amacıyla, Bilgi Güvenliği ve Risk Komitesi, Bilgi Güvenliği Yetkilisi, Fiziksel Güvenlik Sorumlusu, Bilgi Varlıkları Sahipleri ve Şirket çalışanları görev alır. İlgili tarafların bu kapsamdaki görev ve sorumlulukları Bilgi Güvenliği Rol ve Sorumluluklar Yönetmeliği'nde açık olarak tanımlanır.

Şirket Bilgi Güvenliği Politikası Bilgi Güvenliği Yetkilisi tarafından hazırlanır, Bilgi Güvenliği ve Risk Komitesi tarafından yılda en az bir defa gözden geçirilir ve Yönetim tarafından onaylanır. Bilgi Güvenliği Politikası oluşturulurken Şirket'in güvenlik stratejisi, güvenlik gereksinimleri, yasal ve düzenleyici zorunluluklar göz önünde bulundurulur. Kurum Üst Yönetimi Bilgi Güvenliği Politikası'nın hayata geçirilmesini sağlar.
Kurum Üst yönetimi Bilgi Güvenliği yetkilileri olarak atadığı personeller, Bilgi Güvenliği Rol ve Sorumluluklar Yönetmeliğinde açıkça belirtilmiştir.

3.1. Kurum Üst Yönetim Sorumlulukları

- Güvenlik Politikasının kurum içinde uygulanmasına destek vermek.
- BGYS sorumlusunu atamak.
- Risk değerlendirme yaklaşım dokümanını onaylamak.
- Risk analizinde kritik seviyenin üstündeki riskleri onaylamak.

3.2. BGYS Sorumlusu Sorumlulukları

- BGY Güvenlik Politikasını gözden geçirerek üst yönetimin onayına sunmak.

- Eğitimleri planlamak ve gerçekleşmelerini sağlamak
- BGYS dokümanları hazırlamak ve uygulanmasını sağlamak.
- Bilgi işlem yetkililerinin yapmış olduğu faaliyetleri kontrol etmek ve onaylamak.
- Gereken iyileştirmeler ve geliştirmeler konusunda üst yetkililere brifingler vermek,

3.3. Bilgi İşlem yetkilisi sorumlulukları

- Şirket içinde kullanılan sunucuların kurulumu, güncellenmesi ve sistemin çalışırlılığının devamı için gerekli süreçlerin takibi ve uygulanmasını sağlamak.
- Şirket kullanıcıları için elektronik posta hesabı alımı ve kullanımı, kullanımdan kaldırılmasını sağlamak.
- Yeni işe başlayacak olan personelin bilgilerini ilgili sisteme (Exchange, mail server, v.b.) girip ilgili personel için kullanacak cihazları (Cep telefonu, bilgisayar, v.b.) teslim etmek ve işten ayrılan personellerin cihazlarını teslim almak.
- Personellerin ağ erişim yetkisi vermek yada kaldırmak,
- Alt yapının kurulumu, kontrolü ve güvenliğinden Bilgi işlem yetkilileri sorumludur.
- BGYS'nin yönetilmesinden Bilgi işlem yetkilileri sorumludur.
- Tüm yapılan çalışmalar için BGYS sorumlusuna brifingler vermek.

4. Sunucu işletim sistemi standardı

Sunucu İşletim Sistemi Lisans alımına paralel olarak Windows 2003 Server, Windows Server 2008 veya Windows Server 2012'dir.

Windows AD (Active Directory) Yapısı ve Windows AD yapısında bulunması gereken sunucu yazılımları:

Site: Bir AD yapısında en az bir adet bulunur. Farklı coğrafi konumlar için ayrı site tanımları yapılır. Her site tanımı için ayrı bir subnet tanımı yapılır ve site subnete üye edilir.
Root DC (Merkezi Domain Kontrol Sunucusu) : Domainin ilk kurulduğu merkezi görevleri üzerinde barındıran sunucudur. Root DC seçilirken;

1. Üzerinde AD haricinde kritik bir uygulama çalışmamasına (Veri tabanı ya da uygulama sunucusu gibi) dikkat edilir.

2. Donanım özelliklerinin üzerindeki uygulamaları tam destekliyor olması gerekir.
3. Donanım bileşenleriyle ilgili herhangi bir sorununun olmaması gerekir.

DC: Root DC'nin üzerindeki uygulamaların bir kısmı başka bir DC'ye aktarılabilir veya Uygulamaların yedekli olması ve yük dengelemesi için root DC üzerindeki aynı uygulamalar aynı anda diğer DC üzerinde çalıştırılır. Bir domain içinde en az 2 adet DC bulunmalıdır.

DHCP (Dynamic Host Control Protokol) Server: Root DC üzerinde çalışması faydalıdır.

Scope tanımları: DHCP sunucusu üzerinde IP adres bloğunun alt bölümlere ayrılması içindir. Switchlerde tanımlı Vlan IP adres bloğuna karşılık gelen IP yapılandırmasını sağlar.
Scope tanımı yapılırken;

- İlk 30 tane IP adresi Statik verilmek üzere ayrılır. Scope tanımı 31. IP adresinden başlatılır.
- Varsayılan ağ geçidi mutlak tanımlanmak zorundadır.
- DNS sunucu ayarları en az 2 adet tanımlanmalıdır.
- Önemli makine ve kişilerin IP adresleri Rezerve tanımı yapılarak sürekli aynı IP adresi verilmesi sağlanır. Rezerve IP adresler son IP adresinden başlayarak aşağıya doğru verilir.
- Kira bitiş süresi 999 gündür.

DNS (Domain Name System) : IP adresinden isim veya isimden IP adresi çözmeye yarar. Bir AD içinde en az bir adet bulunmak zorundadır. Bir site içinde en az 2 tane olması gerekir. 1. DNS Root DC üzerinde olmalıdır. 2. DNS ise yükü az olan başka bir DC üzerinde olabilir.

WINS (Windows Internet Name System) : Bir site içinde Windows AD dışında sisteme bağlı bilgisayar varsa 1 adet olması gerekir.

5. Switch Standartları:

Tüm switchlerin aynı marka olması yönetim ve kullanım açısından faydalıdır. Ancak zaman içerisinde yapılan alımardan dolayı farklılıklar gösterebilir. Sistaş standart model olarak Alcatel-Lucent firmasının ürettiği L2 ve L3 switchleri kullanmaktadır.

Kenar Switchler: Çeşitli modellerde L2 switch lerdir.

- 100 mt mesafede ve bağlantısı elektriksel ortamdan geçmeyen switchler, bakır UTP (Category-5e) kablo ile bağlanır.

6. Kablo ve Kablolama Ürünleri Standartları

6.1.Bakır Ürünleri:

- Data kabloları ve bağlantı bileşenleri **Kategori-5e/6** (Cat-5e/Cat6) standartlarına uygun ürünler olmalıdır. Tüm uçlar bitildikten sonra bilgi işlem tarafından test edilir. Bilgisayar ile Switch portu arasında başka herhangi bir cihaz kullanılmaz. Kabloya ek veya fiziksel zarar verecek herhangi bir müdahale yapılamaz. Bağlantı direkt olarak bilgisayar ile Switch arasında yapılır.
- Bilgisayar Ethernet portundan çıkıp switche portuna kadar olan kablo mesafesi 100 mt.dir.
- Bilgisayar ile data prizi arasında bilgi işlem tarafından yapılan pacth cord kablo kullanılır. Bilgisayar ile data prizi arasındaki mesafe 3 mt.den fazla ise eldeki mevcut malzeme duruma göre 5, 7 veya 10 mt. Cat-6 patch cord kullanılabilir. Burada toplam mesafesinin 100 mt.yi geçmemesi gerekir.
- Telefon bağlantıları için standart telefon kablosu kullanılır.Data prizi ile telefon arasında normal telefon kablosu kullanılabilir.

7. Kullanıcı Adı Standartları

7.1.Kullanıcı İsim Standardı:

Kullanıcı İsmi: Kullanıcı Adı ve soyadının tamamı arasında .(nokta) olarak verilir.

Örnek: Sistaş Sayısal (sistas.sayisal).

Toplam karakter sayısı 10 karakterden fazla ise anlamlı kısaltmalar yapılabilir. Kullanıcı başka bir kişinin kullanıcı hebasını kesinlikle kullanamaz. Kullanıcının birden fazla ön ismi varsa ön isimlerin baş harfleri kullanıla bilinir. Aynı kullanıcı isimlerinin çakışması durumunda kullanıcı adının sonuna rakam eklenebilir.

7.2.Kullanıcı Hesabı Güvenlik Ayarları:

Parola Politikaları :

- Parola en az **8** karakterden oluşmalıdır. Parola içinde A-Z, a-z, 0-9, #-$ karakter gruplarından en az 3 tanesinden karakter içermesi zorunludur. Ancak hatırlama güçlüğü çeken kullanıcılarda bu esnetilebilmektedir.
- En fazla 90 günde bir kez mutlaka parola değiştirilmelidir.
- Parola değişikliklerinde en son kullanılan 5 parola tekrar girilemez.

Hesap Politikaları :

- Parola girişi sırasında 4 kez yanlış giriş yapılırsa kullanıcı hesabı 30 dakika boyunca kilitlenir.
- 31 dakika sonra hesap kilidi otomatik olarak açılır.
- 10 dakika kullanılmayan bilgisayarda otomatik olarak ekran koruyucu devreye girer. Ekran koruyucusunun açılması için mutlaka kullanıcı parolasının veya sistem yönetici yetkisi olan bir kullanıcının parolasının girilmesi gereklidir.

Güvenlik Politikaları:

- Hesap kilitlenmelerinde veya parolanın hatırlanamaması gibi durumlarda kullanıcının kendisi, Bilgi İşlem Sistem Destek Bölümünü arayarak parolasının değiştirilmesini talep eder.
- Hiçbir kullanıcı kendisinden başka bir kimsenin kullanıcı hesabını kullanamaz. Böyle durumlardan hesabı kullanılan kişinin kendisi sorumludur.
- Kullanıcının şirkette olmayacağı zamanları, 3 iş gününden fazla ise önceden Bilgi İşlem Sistem Destek bölümüne yazılı olarak bildirir. Örn: Yıllık izin, mazeret izinleri gibi. Kullanıcının hesabı Bilgi İşlem Sistem Destek bölümü tarafından istenilen süre kadar, geçici olarak devre dışı bırakır.

- Çeşitli sebeplerden dolayı kullanıcı hesabına müdahale edilmesi ancak ilgili kullanıcının idari amiri veya bölüm koordinatörünün yazılı onayı ile mümkün olur.
- Kullanıcı hiçbir şekilde sisteme yazılım ekleme veya sistemden yazılım kaldırma işlemi yapamaz
- Kullanıcının sistemdeki yaptığı;
- Herhangi bir nesneye erişimi (Klasör, Dosya, Yazıcı vb.),
- Herhangi bir nesneye erişme veya erişememe durumu,
- Oturum açma/kapama olayları,
- Güvenlik ilkelerinin değişimleri,
- Hesaplarla ilgili değişiklikler,
- Sistem olaylarının değişiminde (güvenlik günlüğünü etkileyen olaylar, sistem açılıp/kapanması gibi)
- Otomatik olarak sistem tarafından kaydedilir. Kayıtların incelenmesinin istenmesi durumunda, kullanıcının veya idari amirlerinin yazılı talebi ile gerçekleşir.

8. E-Posta Standartları

8.1. E-Posta Adres Standardı

E-posta verilirken kullanıcı adı ve soya adı arada bir kota koyulacak şekilde yazılır.

Örnek: Sistaş Sayısal (sistas.sayisal@sistas.com.tr)

8.2. E-Posta Yazılım Standardı

- E-posta gönderme ve alma programı Microsoft Outlook, Mozilla Thunderbird kullanılmaktadır.

- Kullanıcılara ilk kullanımda şifreleri yazılı olarak teslim edilir. Kullanıcılar ilk girişlerinde şifrelerini değiştirmeleri zorunlu tutulmaktadır.

- Kullanıcının talep etmesi durumunda e-posta şifresi kendisine yazılı olarak verilebilir. Kullanıcı web sayfasını kullanarak kendi bilgisayarı haricinden de e-posta gönderip alabilir.

8.3. E-Posta Gönderme/Alma Standartları

- Otomatik olarak gönderme alma süresi 5 dk.dır.
- Hesap ayarlarında kullanıcı Adı soyadının sonuna Parantez () içinde çalıştığı bölüm adı yazılır. Örn: Sistaş Sayısal (Bilgi-İşlem)
- Varsayılan e-posta biçimi HTML'dir.
- Standart e-posta şablonuna kullanıcı imzası dışında herhangi bir nesne eklenemez. Örn: Arka plan resimleri, renkli ve hareketli nesneler.
- Dosya gönderme şekilleri,
  - Maksimum e-posta gönderme/alma boyutu 10 MB'tır. Özel durumlarda Bilgi-İşlem bu boyutu artırma ve düşürebilir.
  - Daha çabuk gitmesi için yüksek boyuttaki dosyalar zip formatında sıkıştırılarak gönderilir.
  - Otomatik olarak çalıştırılabilecek dosya formatları (.exe, .com, .pif gibi) virüs tehlikesine karşı e-posta sunucusu ve MS Outlook tarafından otomatik olarak erişime kapatılır. Çok zorunlu olması durumunda bu tip dosyalar zip formatında sıkıştırılarak gönderilir.
  - Reklam amaçlı e-postalar, hareketli videolar, pornografik içerikli olabilecek e-postalar, e-posta sunucusu tarafından otomatik olarak bloklanır, kullanıcıya iletilmez.

9. Yeni İşe Başlayanlar Kullanıcılar İçin Yapılması Gereken İşlemler

9.1. İşe alınacak ve bilgisayar kullanacak personelde aranılacak temel hususlar,

9.1.1. Temel Bilgisayar Bilgisi

- Bilgisayar hakkında genel bilgi sahibi olmak
- Bilgisayarı düzgün bir biçimde açma/kapama işlemlerini bilmek
- Bilgisayarın çalışmasını etkileyecek fiziksel koşulları bilmek

9.1.2. Temel İşletim Sistemi Bilgisi

- Windows temelli işletim sistemlerini daha önceden kullanmış olmak,

- Programları çalıştırabilmek,
- Ağa göz atmak ve ağdaki diğer bilgisayarlar ve paylaşımlara erişebilmek,
- Ağdaki yazıcıyı kendi bilgisayarına tanıtmak,
- Tanımlı yazıcıların temel ayarlarını değiştirebilmek (Windows'ta)
- Dosya kaydetmek, silmek, kopyalamak, isim değiştirmek ve aranılan bir dosyayı düzgün bir şekilde bulabilmek,
- Windows Masaüstü ayarlarını değiştirebilmek,
- Herhangi bir dosyayı sıkıştırabilmek ve açmak,
- Herhangi bir dosyayı başka bir kişiye e-posta ile göndermek

9.1.3. Temel Ofis Yazılımları Bilgisi

9.1.3.1. Microsoft Word

- Boş dokuman oluşturmak,
- Oluşturulan dokumanda düzgün belge hazırlamak,
- Basit paragraf, satır ve sekme ayarlarını yapabilmek,
- Basit tablolar hazırlayabilmek,
- Yazılan dokumanı uygun yazıcıya gönderebilmek,
- Yazılan dosyayı e-posta ile gönderebilmek,
- Temel Word ayarlarını bilmek ve değiştirmek

9.1.3.2. Microsoft Excel

- Boş dokuman oluşturmak,
- Hücre biçimlendirmesi hakkında temel bilgiler,
- Basit formüller hazırlayabilmek ve uygulamak,
- Basit tablolar hazırlayabilmek, tablo biçimlendirmesi hakkında genel bilgi sahibi olmak
- Yazılan dokumanı uygun yazıcıya gönderebilmek,
- Yazılan dosyayı e-posta ile gönderebilmek,
- Temel Excel ayarlarını bilmek ve değiştirmek,

- Oluşturulan verileri süzebilmek

9.1.3.3. Microsoft Outlook

- Microsoft Outlook hakkında genel bilgi
- Yeni e-posta oluşturmak,
- Doğru bir biçimde yeni e-posta göndermek, Gelen e-postayı yanıtlamak veya başka bir kullanıcıya göndermek ,
- Adres defterini kullanmak, yeni kişi ekleme, değiştirme veya silmek,
- Adres defterinde olmayan kullanıcılara e-posta göndermek,
- Posta kutularını yönetmek,
- Görev tanımlamak ve düzenlemek,
- Outlook Takvimini kullanabilmek,
- Temel Outlook ayarlarını bilmek ve değiştirmek,

Not:

Yukarıdaki özellik tanımları temel bilgisayar işlemleri içindir. Bilgisayar kullanabilmek için gereken özelliklerdir. Çalışılacak bölüm ve yapılacak işin niteliklerine göre bu tanımlar ve aranılan nitelikler ilgili idare amirlileri ve insan kaynakları bölümü tarafından genişletilebilir. Bilgi İşlem Bölümü bu tip durumlarda İnsan Kaynakları ve İlgili Bölüm ile koordineli olarak çalışır.

Kullanıcının istenilen temel nitelikleri taşımaması durumunda, kullanıcının eğitiminden, bilgi eksikliğinden dolayı doğabilecek veri ve iş kayıplarından İnsan Kaynakları ve İlgili İdare amirleri sorumludur.

9.2. Yeni Bilgisayar Temini ve Teslimi

Yeni işe başlayan kullanıcılar en az işe fiili olarak başlamadan bir gün önce ilgili bölüm amiri ve İnsan Kaynakları bölümü tarafından personel adı, soyadı, çalışacağı bölüm ve görevi yazılı olarak bildirilir.

Yeni işe başlayacak personel, başka bir personelin bilgisayarını kullanacaksa (İşten ayrılma veya görev değişikliği sebebiyle) bölüm koordinatörünün yazılı onayı alınarak Bilgi İşlem Sistem Destek Bölümü tarafından sistem ayarlamaları yapılır.

Eğer fazladan bilgisayar ihtiyacı varsa istek ilgili bölüm amiri tarafından, bölüm koordinatörü onayı alınarak en az 5 iş günü öncesinden Bilgi İşlem Sistem Destek Bölümü'ne yazılı olarak Yeni Bilgisayar ve Kullanıcı Talep Formu vasıtası ile iletilir. Bilgi İşlem Sistem Destek Bölümü mevcut imkanlarla ihtiyacı karşılar eğer yeni bilgisayar alımı gerekiyorsa Satın Alma süreçlerine bağlı kalınarak ihtiyaç karşılanır. Her iki durumda da Bilgi İşlem Sistem Destek Bölümü talebi yapan idare amirini talebin karşılanma zamanı ve yapılacak işlemler hakkında yazılı olarak bilgilendirir.

Eğer talep zamanında karşılanamıyorsa Bilgi İşlem Sistem Destek Bölümü stok olarak envanterde tuttuğu bilgisayar donanım sistemini talebi karşılamak üzere kullanır. Yeni alınacak bilgisayar donanımı stok olarak envantere girilir.

Talep edilen bilgisayar donanımı standart kullanımdan farklı ise özel donanım ve yazılım istekleri ayrıca Yeni Bilgisayar ve Kullanıcı Talep Formu'nda ayrıca belirtilir.

Bilgisayar donanımı ve yazılım temininden sonra 1 iş günü içerisinde, devam eden diğer işlemleri aksatmayacak şekilde yazılım kurulumları ve ayarlamalarını yaparak kullanıcıya teslim eder. Teslim sırasında kullanıcı ve Bilgi İşlem Sistem Destek Bölümü yetkilisi beraber ayarları kontrol ettikten sonra Donanım ve Yazılım Envanterini içeren sözleşme kullanıcı ve Bilgi İşlem Sistem Destek Bölümü tarafından imzalanır. Sözleşme Bilgi İşlem Sistem Destek Bölümü tarafından dosyalanır.

9.3. Kullanıcı Hesaplarının Tanımlanması:

- Yeni kullanıcı açılması durumunda 4.1. maddesindeki kurallara göre Windows AD sisteminde kullanıcı hesabı açılır.

- 5.1. maddesindeki kurallara göre e-posta hesabı açılır. Listeden uygun parola verilir.

9.4. Kullanıcı Hakları Ataması

Eğer kullanılan yazılımlar tarafından herhangi bir sorun çıkmıyorsa varsayılan olarak tüm kullanıcılar kendi bilgisayarlarında kısıtlı kullanıcı grubuna atanır. Bu işlemler dışında yazılım gereği veya özel durumdan dolayı kullanıcıya lokalde power user veya System administrator yetkisi verilmiş ise sistem ayarlarını değiştirme yetkisine ulaşır. Bu durumdan dolayı kullanıcının kendi kullandığı bilgisayar üzerinde Bilgi İşlem Sistem Destek Bölümü tarafından tanımlanmış ayarları değiştirmesi sonucu oluşacak veri veya iş kaybından kendisi sorumludur.

Yeni Bilgisayar ve Kullanıcı Talep Formu'nda belirtilen erişim yetkileri Windows AD hesabı ve Portal hesabında tanımlanır.

9.5. Ağ Erişim Yetkileri

Ağ trafiğinde güvenliği sağlamak amacıyla, ağ kontrol güvenlik sistemleri bulunur. Ağ güvenliğinde dış güvenlik duvarı, IPS, iç güvenlik duvarı, SSM gibi katmanlı güvenlik mimarisi (bir güvenlik katmanının aşılması durumunda diğer güvenlik katmanının devreye girdiği) kullanılır. Ağ güvenliğinde kullanılan sistemler, sürekli gözetim altında tutulur. Dış ağ ile kurulan bağlantılarda VPN ve SSL kullanılır.

Kullanıcının ağ üzerinde yetkisi dahilinde olan paylaşılmış nesnelerde oluşturacağı veri ve iş kaybından, kendisi ve erişim yetkisini onaylayan amirleri sorumludur.

9.6. Eğitim

Personelin kurum ve çalışması hakkında gerekli bilgiye sahip olması ve çalışma esnasında hata riskini en aza indirmek için eğitim gereklidir.

- Eğitim stratejisi ile bilişim stratejisi aynı doğrultudadır.

- Bilgi İşlem yöneticileri, personel için bugün ve ileride gerekecek yetenekleri teknikleri tespit eder ve gerekli eğitimi verir.
- Kullanılan standart yazılımların eğitimleri verilmektedir.
- Eğitim verenler, kurumun mevcut ve uzun vadeli politikaları ile paralellik gösteren bir şekilde eğitimden geçmiştir, gerekli sertifikalara sahiptir.
- Bilgi İşlem yöneticileri, bilişim eğitimi bütçelerini kontrol eder.

10. Görev Değişikliği Olan Kullanıcılar İçin Yapılması Gereken İşlemler

Görev değişikliği olan kullanıcı en az işe fiili olarak başlamadan bir gün önce ilgili bölüm amiri ve İnsan Kaynakları bölümü tarafından personel adı, soyadı, eski çalıştığı bölümü, görevi ve yeni çalışacağı bölümü, görevi yazılı olarak bildirilir. Yeni donanım ve/veya yazılım ihtiyacı varsa Yeni Bilgisayar ve Kullanıcı Talep Formu doldurularak Bilgi İşlem Sistem Destek Bölümü'ne gönderilir. Bundan sonraki işlemlerde 6.2. maddesi takip edilir.

Kullanıcının tüm hesap işlemleri ve erişim hakları gözden geçirilir ve yeni tanımları yapılır. Eski kullandığı donanım ve yazılımlar kontrol edilerek Bilgi İşlem Sistem Destek Bölümü tarafından teslim alınır. Ayrıca kullandığı dosyalar idare amiri tarafından kontrol edilir ve teslim alınır.

11. İşten Ayrılan Kullanıcılar İçin Yapılması Gereken İşlemler

İşten ayrılacak olan kullanıcı, işten ayrılmadan en az 1 (bir) iş günü önce ilgili bölüm amiri ve İnsan Kaynakları bölümü tarafından personel adı, soyadı, çalıştığı bölümü ve görevi yazılı olarak bildirilir.

İlgili idare amiri ve İnsan Kaynaklarından yazılı onay alınarak kullanıcı Windows AD Hesabı, acil yapılması gerekiyorsa yazılı onayın gelmesinden sonra 30 dk. Aksi durumda kullanıcıdan yazılım, donanım ve dosyaları teslim alındıktan sonra aynı iş günü içerisinde 5 iş günü boyunca devre dışı bırakılır. 5 iş günü sonunda devre dışı bırakılan kullanıcı hesabı ilgili bölüm idari amirleri tarafından aksi yazılı bir talep gelmemişse sistemden tamamen silinir.

Kullanıcının e-posta hesabının parolası değiştirilir ve 1 hafta boyunca sistemde tutulur. 1 hafta sonunda bölüm idare amiri tarafından aksi bir talep gelmemiş ise sistemden silinir.

Ayrıca İdare Amiri eğer yazılı olarak talep ederse kullanıcının e-posta hesabı talep edilen başka bir e-posta hesabına Bilgi İşlem Sistem Destek Bölümü tarafından otomatik olarak yönlendirilir.

Tüm işlemler tamamlandıktan sonra, 2 ay içinde ayrılan personelin yerine yeni bir personel alınmayacaksa ilgili idare amirimin onayı alınarak bilgisayar donanımı Bilgi İşlem Sistem Destek Bölümü'ne alınır ve diğer bölümlerin ihtiyaçlarını karşılamak için kullanılır.

12. Yeni Bilgisayar Donanımı Taleplerinin Değerlendirilmesi

Bilgi İşlem Departmanı gelen bilgisayar isteklerini değerlendirirken bu isteği yapan birim amirine; bu talep edilen bilgisayarın hangi amaçla kullanılacağını ve ne tür uygulamalar çalıştırılacağını sorar. Alınan cevap doğrultusunda talep edilen bilgisayarın donanım özelliklerini Bilgi İşlem Departmanı yapar.

13. Yeni Bilgisayar Yazılımı Taleplerinin Değerlendirilmesi

Talep edilen bilgisayar yazılımı talebi ilgili birim amiri tarafından Kurum Üst Yönetimine mail yolu ile iletilir. Kurum üst yönetimi uygun görmesi halinde Bilgi İşlem Sistem Destek Bölümü'ne e-posta yolu iletilir.

Yazılım daha önceden kullanılmış veya test edilip onaylanmış ise imkanlar dahilinde talep karşılanır. Lisansı eksikse satın alma süreçlerine uygun olarak sipariş verilir.

Yazılımın Üretici Firması ve seçilecek ürün net olarak belirlenmemiş ise, istenilen yazılım özellikleri Bilgi İşlem Sistem Destek Bölümü'ne yazılı olarak ayrıca verilir. Bilgi İşlem Sistem Destek Bölümü istenilen özellikteki yazılımları araştırıp demo amaçlı kurulumlarını sağlar. Demo sırasında uygun görülen yazılım satın alma süreçlerine uygun olarak sipariş verilir.

14. Donanım Stoğu Tutulması

Bilgi İşlem Sistem Destek Bölümü herhangi bir arıza durumunda arızayı daha çabuk gidermek ve iş kaybını minimuma indirmek için belirli bazı donanımların stoğunu tutar.

Belirlenen donanımlardan belirlenen sayı veya daha fazla oranda stok tutulur. Ayrıca stok seviye sınırı konularak bu seviyenin altına inen donanımların yeni siparişleri verilir.

Örnek:

Donanım Adı	Stok Sayısı
Komple Sistem	1
Ana Kart	1
Hard Disk	2
Monitör	1
Ram	5
Ekran Kartı	1
Güç Ünitesi	2
CD Sürücü	1
Ethernet Kartı	1
Klavye	5
Fare	5
Kasa	1
Lazer Yazıcı	1
Barkod Yazıcı Kafası	1
Speaker	1

Not:

- RAM'ler ana kart modellerine göre farklılık gösterdiğinden. Envanterde bütün ana kartlara uygun en az 1 çeşit RAM bulundurulur.
- Aciliyet gerektirmeyen durumlarda satın alma süreçlerinin hafifletilmesi ve iş kazancı için siparişler toplu olarak ve sayıdan fazla verilebilir. Bu tip durumlarda fiyat değişimleri göz önünde bulundurulur.
- Yukarıdaki liste dışında kalan network aktif cihazları (Router, Switch, Modem) ve sunucu sistemleri maliyetlerinin yüksek olması, kullanımının sadece belirli özelliklere dayanmasından dolayı, çok az satın alınması veya hiç alınmaması ve arızalanma olasılığının düşük olmasından dolayı stoğu tutulmaz. Bu açık yapılan bakım anlaşmaları ve sözleşmelerle giderilir.

15. Satın Alma Süreçleri

Bilgi İşlem Departmanı, gerek kendi talepleri gerekse departmanlardan gelen alım taleplerini fiyatlandırır. Bu fiyatlandırma Kurum Üst Yönetimine e-posta yolu ile yollanarak onay beklenir. Alınan onay doğrultusunda satın alma işlemi gerçekleştirilir.

16. Makine Adı Standartları

Makine adları bölüm isimlerinden oluşacaktır. Bölümde birden çok bilgisayar olması halinde makine isimlerinin sonuna artan değerde sayı eklenecektir. Makine açıklamaları ise kullanıcı isimlerinden oluşacaktır.

Örnek:

Departman: Bilgi İşlem

Kullanıcılar:

Sistaş Sayısal,

Sistaş Sayısal İletişim

Makine isimleri ve Açıklamalar:

Makine Adı: Bilgiislem1 Açıklama: Sistaş Sayısal,

Makine Adı: Bilgiislem2 Açıklama: Sistaş Sayısal İletişim

17. Firewall Standartları

Berqnet 200 Fw çeşitli kullanım ve güvenlik standartları gelmektedir. Sistaş Sayısal İletişim'in internet ve Dış erişime yönelik bütün bağlantıları, bu firewall üzerinden geçmektedir. Bu sistem için mevcut prosedür ;

- Berqnet 200 Firewall'un bütün port'ları default olarak kapalı durumdadır.
- Sadece Şirketin Uygulama Server'ları bir kısıtlamaya uğramadan (Policy) dış erişim hakkına sahiptir.
- Şirketin dışardan erişim alması gerektiği durumlarda (Point To Point Sistaş ion), SIP Sistaş ion, sadece bağlantı yapılması gereken şirketin, Dış ip'sine ve, yetkilendirme verilecek olan sistemin Statik ip'sine yetki verilir.
- Sistem üzerinde Değişim ve Silme yetkilendirmeleri sadece; Bilgi Sistemleri Yöneticisine aittir.

18. Bina Güvenlik Standartları

Girişlerde güvenlik personeli bulunmaktadır.

Bilgi işlem sistem odası kamera ile takip edilmektedir.

Gizlilik içeren dökümanların bulunduğu bölgelerde/katlarda güvenlik daha hassastır. Bu odalara giriş yetkisi sınırlandırılmıştır. Girişler sadece yetkililere özel anahtarlar ile yapılmaktadır.

19. Bakım

Teçhizat, elektrik kesintileri ve destek hizmetlerinden kaynaklanan arızalar yüzünden bozulabilmektedir. Techizatın arıza durumunu tespit edebilmek, arızayı gidermek için gerekli işlemleri zamanında yapabilmek ve arıza öncesinde techizatın sürekliliğini korumak için bakımlar yapılmaktadır.

Elden çıkarılacak teçhizatlar için lisans kontrolleri yapılır, herhangi bir hasar varsa kontrol edilir.

20. Ortam Değiştirme

Kullanıcılara iş gereksinimlerine göre çalışma ortamı sağlanmıştır. Ortam değişimi gerektiğinde, istek Bilgi İşlem Bölümüne bildirilir. Bilgi işlem bölümü yeni ortam kontrollerini yaptıktan sonra değişime izin verir.

Kullanılmayan ortamlar yapılan kontroller sonrası Bilgi İşlem Bölümü tarafından ortadan kaldırılır.

21. Mobil İletişim

Kurumsal yapı dahilinde kablosuz ağ ve GSM bağlantıları mevcuttur. GSM bağlantıları 1nci kademe aramaların yapılması için kullanılır. Wi-Fi Bağlantı şirketin kurumsal müşterilerinin bağlı bulunduğu hattan bağımsız, Gateprotect Firewall ile güçlendirilmiş olarak çalışır. Şirket Network'u dışındaki bilgisayarlar, bu bağlantıyı kullanarak, internet ortamına çıkış yapar. Firmada WPA şifreleme kullanır. Bu şifre 90 günlük periyotlarda değiştirilir.

22. SLA Süreleri

Kurumsal yapı dâhilinde SLA takip yöntemi kullanılır. Bu süreler Ticket sistemi üzerinden takip edilir. Olayın Yapıya etksine göre kademelendirilir.

1-3 Kişi – Donanım - Low Level – 6 Saat

1-3 Kişi – Yazılım – 1 Saat

1-20 Kişi – Donanım – Normal Level – 2 Saat

1-20 Kişi – Yazılım – Normal Level – 30 Dakika

20-...Kişi - Donanım - Anında

20-...Kişi – Yazılım - Anında

Sistem Acknowledge işlemleri IT Uzmanınca yapılır ve ilgili personel'e aktarım işlemleri yapılır. SLA bitim süresinden önce ilgili birim yöneticilerine aktarım yapılır.

23. Uyum

Tüm Şirket çalışanları, ilgili yasalar, yönetmelikler ve sözleşmelerden doğan güvenlik gereksinimlerine, fikri mülkiyet haklarına, lisans anlaşmalarına ve Şirket tarafından belirlenen güvenlik gereksinimlerine uymakla yükümlüdürler. Yöneticiler sorumluluk alanlarındaki tüm süreçlerin işletilmesinde güvenlik politikalarına ve standartlara uyumu temin eder. Tüm Şirket çalışanları, Şirket verilerinin gizlilik derecelerine uygun şekilde kullanımı konusunda sorumludurlar.

Şirket'in bilgi güvenliği politikalarına uyumun denetlenmesi için Bilgi Güvenliği Yönetim Süreci kapsamında bilgi güvenliği gözden geçirme faaliyetleri gerçekleştirilir.

24. Bilgi Güvenliği politikasının uygulama sorumluluğu

Tüm çalışanların Bilgi Güvenliği Politikası'ndan haberdar olması sağlanır. Politikanın son hali tüm personele duyurulur ve personelin sürekli olarak erişebileceği ortak bir alanda yayımlanır. Personel kendisini ilgilendiren genel hükümlere uymak zorundadır. Personelin kendisini ilgilendiren genel hükümlere uyup uymadığının kontrol edilmesi sorumluluğu personelin idari amirindedir. Bilgi güvenliği politikalarına uyum düzenli olarak izlenir.

25. Yürürlük

Bilgi güvenliğine ilişkin bu düzenleme, üst yönetimin onay tarihi itibariyle yürürlüğe girer.

Şirket'in bilgi güvenliğine ilişkin tüm uygulama ve iş akışları politika hükümleriyle uyumlu şekilde oluşturulur/güncellenir.