BİLGİ GÜVENLİĞİ POLİTİKASI

MART-2020

BGYS POLİTİKASI

BGYS politikası, Hangisi İnternet ve Bilgi Teknolojileri A.Ş. bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır. Bu politikada tüm bölümleri ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır.

1. AMAÇ

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat kurum açısından en önemli varlıklardan biridir. Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımızın genel özeti bu politikada verilmektedir. Uygulama detay bilgileri için sistem dokümantasyonuna, ilgili prosedürlere, rehberlere, planlara ve raporlara bakılmalıdır. Bu politika bilgi güvenliği politikası ve detaylı kullanım politikalarını da kapsayan bir üst dokümandır. Yönetim tarafından onaylanmış ve yayınlanmıştır. Yönetim tarafından düzenli olarak gözden geçirilmektedir.

2. KAPSAM

“Bilgi Güvenliği Yönetim Sistemleri Politikası” dokümanında yer alan kriterler; bilgi İşlem altyapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

“Bilgi Güvenliği Yönetim Sistemleri Politikası” dokümanında yer alan kriterler; şirket bilgi sistemleri ve üzerinde işlenen, iletilen, depolanan ve yedek olarak saklanan tüm varlıkları kapsamaktadır. Politika aynı zamanda, şirket bilgi sistemleri altyapısını kullanmakta olan tüm personeli, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

3. KISALTMALAR VE TANIMLAR

a. **BGYS:** Bilgi Güvenliği Yönetim Sistemi

b. **Bilgi Güvenliği:** Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkar edememe ve güvenilirlik gibi diğer özellikleri de kapsar.

c. **Bilgi Güvenliği ihlal Olayı:** iş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

d. **Bilgi Güvenliği Yönetim Sistemi (BGYS) :** Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi; kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir.

e. **Bilgi Güvenliği Riski:** Açıklıklardan fayda sağlamak suretiyle kuruluşa zarar verebilecek varlık ya da varlık gruplarının potansiyel tehdididir. Bir olayın ve sonucunun olasılığının kombinasyon koşulları olarak ölçülür.

f. **PUKÖ:** Planla, Uygula, Kontrol Et, Önlem Al.

BİLGİ GÜVENLİĞİ HEDEFLERİ VE PRENSİPLERİ

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir. Her bir varlık için risk seviyesini kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir. Risk yönetimi ve kontrollerin uygulanması sürekli bir faaliyettir ve kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılması hedeflenmektedir.

4. SORUMLULUK

Bu dokümanın hazırlanması, en az yılda 1 kez veya gerekli görülmesi durumunda gözden geçirilmesi ve güncel tutulmasından Şirket Bilgi Güvenliği yetkilisi sorumludur. Bu politikanın onaylanmasından Yönetim sorumludur.

• **Yönetim :** Bilgi Güvenliği Politikası'nın onaylanması ve kendisine düzenli sunulan bilgi güvenliği raporlarını değerlendirmekten, gerekli önleyici ve tespit edici aksiyonları almaktan sorumludur.

• **Şirket Yöneticileri:** Bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda tüm yöneticiler gerekli kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlereyönelik

olarak yeterli kaynağı tahsis eder. Periyodik olarak bilgi güvenliğine ilişkin denetimleri gerçekleştirilmesine destek olarak, potansiyel risk taşıyan ve başarısız noktaları tespit eder.

• **BT Birimleri:** Bilgi Güvenliği Politikası'nın personele duyurulmasından ve iç ağda yayınlanmasından, bilgi güvenliği olaylarını Yönetim'e ve iLab'e zamanında ve eksiksiz raporlamaktan sorumludur.

• **Şirket Çalışanları:** Tüm Şirket personeli, gerek bu Politika'da gerekse Şirket'in destekleyici diğer politika ve prosedürlerinde belirtilen bilgi güvenliğine yönelik Şirket yaklaşımına uygun bir şekilde hareket etmek ve çalışmalarında bunları uygulamaktan sorumludur. Tüm çalışanlar, erişimleri dahilinde olan özel bilgi ve süreçlere ilişkin tam sorumluluk almak adına "Bilgi Güvenliği Taahhütnamesi"ni imzalar.

• **İnsan Kaynakları :** Bilgi güvenliği farkındalık eğitimlerinin (e-learning) yeni işe başlayan tüm çalışanlara oryantasyon sürecinde verilmesinden, bu eğitimlerin tüm çalışanlara en az yılda bir defa düzenli şekilde verilmesinden, gerekli ekiplere gizlilik anlaşmalarının eksiksiz imzalatılmasından ve özlükte muhafazasından, işe giriş, çalışma ve işten ayrılma aşamalarında her türlü bilgi güvenliği akışının (referans kontrol, diploma uygunluk kontrolü, gizlilik anlaşmaları, kullanıcı kaydetme ve silme akışında zamanında aksiyon aldırma, vs.) tastamam ve zamanında işletilmesinden, "Bilgi Güvenliği Taahhütnamesi" ile işe giriş, çalışma ve işten ayrılma aşamalarında çalışandan alınması gereken tüm taahhütname ve beyanların imzalatılması, arşivlenmesi, Bilgi güvenliği eğitimlerinin yürütülmesi vs. çalışanlara dair her türlü bilgi güvenliği ihlaline sebebiyet verecek süreçlerin önleyici ve tespit edici usullerde doğru yönetilmesinden sorumludur.

• **Üçüncü Şahıslar:** Tüm üçüncü şahıs firma çalışanları Bilgi Güvenliği Politikası'nı kabul etmiş sayılmaktadır.

5. BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU

Hangisi İnternet ve Bilgi Teknolojileri A.Ş. bünyesinde TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerini yürütmek üzere BGYS KOMİSYONU kurulmuştur.

BGYS Komisyonu Başkanı Görev, Yetki ve Sorumlulukları:

- Bilgi Güvenliği konularının altyapısını oluşturacak projeler hazırlanmasını sağlamak.
- Çalışmaların yürütülebilmesi için gerekli komisyonları, çalışma gruplarını oluşturmak ve görev tanımlarını yapmak.
- BGYS Komisyonuna başkanlık etmek.
- Hangisi İnternet ve Bilgi Teknolojileri A.Ş. bünyesinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standartlar seviyesinde bir hizmet kalitesini yakalamak amacıyla TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı, TS ISO/IEC 20000 Bilgi Teknolojileri Hizmet Standardı, Kurumsal Bilgi Güvenliği Mimarisi gibi konuların gerekliliklerinin yerine getirilmesi için gerekli çalışmaları yapmak,
- BGYS Biriminden, BGYS Komisyonunandan gelen istek ve talepleri değerlendirmek projelerin dayandırıldığı standartlar çerçevesinde onay vermek,
- Projelerde referans alınan standartların temel gereksinimlerden dolayı Bilgi Güvenliği Yönetim Sistemi gerekliliklerini oluşturmak ve yönetmek,
- Yönetim Sistemi dökümantasyonlarının hazırlanmasına rehberlik etmek ve hazırlanan dokümanları onaylamak.
- Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak,
- Çalışmaların yürütülebilmesi için Hangisi İnternet ve Bilgi Hizmetleri A.Ş. ile yüklenici firmalara yönelik gerekli tüm resmi yazışmaların yapılmasını, izinlerin alınmasını sağlamak,
- Projelerin yürütülebilmesi için gerekli olan yönetim Gözden Geçirme, İç Denetim, Farkındalık Eğitimleri gibi faaliyetlerin gerçekleşmesini sağlamak,
- Yapılan çalışmalar doğrultusunda yapılacak olan belgelendirme dış denetimlerini (Belgelendirme ve ara denetimler) organize etmek,
- Projelerin daha verimli şekilde yürütülebilmesi için BGYS Birim personelinin kişisel gelişimleri için gerekli görülen eğitimleri düzenlemek ya da dış taraflarda düzenlenmiş eğitimlere gönderilmesini sağlamak konu ile ilgili tüm yasal izin ve finansal kaynağın sağlanmasını organize etmek,

BGYS YGG (BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNETİM GÖZDEN GEÇİRME) TOPLANTILARI

BGYS biriminin ve üst yönetimin bilgi güvenliğinin uygunluğunu, verimliliğini, risk yönetiminin işlevselliğini, tetkit sonuçlarını, düzeltici ve önleyici faaliyetleriele aldığı yılda en az bir defa düzenlenen bir toplantıdır. Bu toplantıda yönetim risk kabul kriterlerini ve kaynak ihtiyaçlarını değerlendirir. Çalışmaların, risk değerlendirme ve işleme faaliyetlerinin verimliliğini inceler. Bu toplantılarda standarda göre girdi ve çıktılar Toplantı Tutanağı Formu kullanılarak kayıt altına alınmaktadır.

6. BİLGİ HASSASİYETİ VE RİSKLER

6.1. Bilgi Varlıklarımız

Hangisi İnternet ve Bilgi Teknolojileri A.Ş. bünyesinde tüm fiziki alanlardaki birimlerde üretilen bilgiler bilgi varlıklarımızı oluşturmaktadır.

Masaüstü bilgisayarlar, laptoplar, CD/DVD, USB ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan ya da iletim ortamında (internet, e-mail, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

6.2. Veri Sınıflandırması

BİLGİ SINIFLANDIRMA KILAVUZU		SAKLANMA YERİ
Gizli	**En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır.**	**Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar ve kişisel bilgisayarlar**
İç Kullanım	**Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3.taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır.**	**Departmanın kilitli dolapları,** **Kişisel bilgisayarlar**
Kişisel	**Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kurum işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, laptop veya dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişebilirlik ön plandadır.**	**Çalışma masalarının kilitli çekmeceleri**
Kuruma Açık	**Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.**	**Departmanın kilitli orta dolapları**
Halka Açık	**Bu bilgiler Hangisi İnternet ve Bilgi Teknolojileri A.Ş. ye bağlı tüm tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.**	**Dolaplar ve dolapların dışlarında**

Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmaktadır. Bu sınıflandırmaya göre halka açık dokümanlar web sitesinde yayınlanan ve işlem için üçüncü taraflara verilen kağıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

7. Bilgi Güvenliği Politikası ve Kılavuzu

Hangisi İnternet ve Bilgi Teknolojleri A.Ş. tarafından yayımlanan Bilgi Güvenlği politikaları Yönergesi ve kılavuzu çerçevesinde, Bilgi Sistemleri tarafından yayınlanan bu dokümanda genel bilgi güvenliği kuralları tanımlanmıştır. Her çalışan bu dokümanda belirtilen kurallara uymakla sorumludur.

8. Bilgi Güvenliği Sözleşmeleri

Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını tahhür ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (Bilgisayar kullansın/kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.

9. Bilgi Güvenliği Eğitimleri

Hangisi İnternet ve Bilgi Teknolojileri A.Ş. bünyesi çalışanları için 2020 yılı içerisinde hizmet içi eğitim planlarına Bilgi Güvenliği Farkındalık Eğitimleri dahil edilmiştir. Bilgi Güvenliği Farkındalık Eğitiminden Bilgi Güvenliği Temsilcisi sorumludur. Ayrıca web sayfası üzerinden yazılı olarak bilgilendirme dokümanları (.doc, .pdf, veya .pptx formatında) yayınlanacaktır.

10. İnsan Kaynakları ve Zafiyetleri Yönetimi

- Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
- Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.
- Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
- İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kağıt kesme makinasında imha edilmelidir.
- Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
- Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
- Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
- Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

- Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.
- Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.
- Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Sistem Yönetimine haber verilmelidir.

10.1. İşe Başlayış Prosedürü

- İşe başlayan her personele (kadrolu ve hizmet alımı dahil) bilgi güvenliği ve sosyal mühendislik zafiyetleri konularında eğitim verilmelidir. Bu eğitimler uyum eğitimlerine dahil edilmelidir.
- Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (Bilgisayar kullansın/kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.
- Kullanacağı bilgi sistemlerine yönelik kullanıcı adı ve şifreleri tanımlanmalıdır.
- Tüm personele kurum kimlik kartı çıkartılmalıdır.
- Tüm personele tanıtıcı yaka kimlik kartı çıkartılmalıdır.

10.2. İşten Ayrılış Prosedürü

- Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.
- Kullandığı bilgi sistemlerine yönelik kullanıcı adı ve şifreleri sistem yöneticisi tarafından pasif hale getirilmelidir.
- Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
- Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
- Görevden ayrılan personel işten ayrılma onay formunu doldurarak bağlı bulunduğu kurumun insan kaynakları birimine teslim etmelidir.
- İlgili form doldurulmadan personelin kurum ile ilişiği kesilmez.
- Kurumdan ayrılan personele ait “İşten ayrılma onay formu” resmi yazı ile “Bilgi Güvenliği Yetkilisi” ne gönderilmelidir.

11. Parola Güvenliği Politikası

- Güvenliğin oluşturulacağı birim için kullanılan programlarda uygulanan parola standardı belirlenmeli, bu parola sistemi aşağıdaki unsurları içerecek standarda getirilmelidir.
- Bilgi Güvenliği Yetkilisinin devreye girmesi ile parola standardı belirlenerek uygulanmaya başlanmalı, geliştirilerek aşağıdaki yapıya çekilmesi konusunda plan yapılmalıdır.
- Parola en az 8 karakterden oluşmalıdır.
- Harflerin yanı sıra, rakam ve "? @, !, #, %, +, -, *, %" gibi özel karakterler içermelidir.
- Büyük ve küçük harfler bir arada kullanılmalıdır.
- Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.
- Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır.(Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız gibi).
- Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.
- Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.
- Basit bir cümle ya da ifade içerisindeki belirli kelimeler özel karakter veya rakamlarla değiştirilerek güçlü bir parola elde edilebilir.

‘B’ yerine 8	‘Z’ yerine 2	**Örneğin** Balıkçıl-Kazak 8a11kç11-Ka2ak Solaryum! 501aryum!
‘I, İ, L, l’ yerine 1	‘O’ yerine 0	
‘S’ yerine 5, ‘G’ yerine 6	‘g’ yerine 9	
‘T’ , ‘t’ yerine ‘+’	‘Ş’, ‘ş’ yerine $	**Örneğin** "Dün Kar Yağmış" : Dün*Yağm1$ "Şeker gibi bir soru sordu" : $eker~1?Sordu "Tek eksiğim bir güldü" : 1ğim1:)dü "Yüzeysel bir soru eşittir eksi puan": %eysel1?=-puan
“kar”, “yıldız” yerine ‘*’	“dolar”, “para” yerine ‘$’	
“Soru” yerine ‘?’	“gibi” yerine '~’	
“gül” yerine ‘:)’	“eksi” yerine ‘-‘	
“bir”, “tek” yerine ‘1’	“yüz”, “yüzde” yerine ‘%’	

12. İhlal Bildirim ve Yönetimi

- Bilginin gizlilik, bütünlük ve kullanılabilirlik 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.
- Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
- Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.
- İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
- Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.
- 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 edilir.
- Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınır.

13. İnternet ve Elektronik Posta Güvenliği

- Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.
- İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.
- Kurumun e-posta sunucusu, kurum içi başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.
- Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.
- İnternet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-posta adresi bu mesajlarda kullanılamaz. Ancak iş gereği üye olunması yararlı internet haber grupları için yöneticisinin onayı alınarak Kurumun sağladığı resmi e-posta adresi kullanılabilir.
- Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.
- E-posta gönderiminde konu alanı boş bir e-posta mesajı göndermemelidir.
- Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.
- E-postaya eklenecek dosya uzantıları “.exe”, “.vbs” veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (.zip veya .rar formatında) mesaja eklenmelidir.

- Bakanlık ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.
- Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.
- Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.
- Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Sistem Yönetimine haber verilmelidir.
- Spam, zincir, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verilmemelidir.
- Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
- Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur.
- Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.
- Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.
- Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.
- Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Sistem Yönetimine haber verilmelidir.
- Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Sistem Yönetimine haber vermelidir.

14. Mal ve Hizmet Alımları Güvenliği

1- Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir.

2- Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

- Bilgi güvenliği politikası,
- Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,
- Gerekli fiziki koruma için kontrol ve mekanizmalar,
- Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,

- Varlıklarda oluşan herhangi bir değişimin tespiti için prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan kayıp veya modifikasyon,
- Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,
- Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,
- Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,
- Kullanıcı ve yönetici eğitimlerinin metodu, prosedürü ve güvenliği,
- Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,
- Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,Açık bir raporlama yapısı ve anlaşılan raporlama formatı,
- Değişim yönetimi sürecinin açıkça belirlenmesi,
- Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,
- İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,
- Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,
- Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,
- Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,
- Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,
- Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,
- Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,
- Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,
- Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,
- Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,
- Sorun çözümü için bir yükseltme sürecinin kurulması,
- Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik de dahil olmak üzere hizmet sürekliliği gerekleri,
- Anlaşmayla ilgili tarafların yükümlülükleri,
- Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak)
- Fikri mülkiyet hakları (IPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,

- Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri
- Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,
- Taraflardan birinin anlaşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır.
- Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların yeniden müzakere edilmesi.
- Varlık listeleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

3- Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar önemli ölçüde değişebilir. Bu nedenle; anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde yapılmalıdır. Gerektiğinde güvenlik yönetim planındaki gerekli kontroller ve prosedürler genişletilebilir.

4- Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.

5- Genellikle anlaşmaların esasları kuruluşlar tarafından geliştirilmiştir. Bazı durumlarda anlaşmaların üçüncü taraflarca geliştirilmesi ve kuruluşa empoze edilmesi durumu olabilir. Kuruluşlar, kendi yapılarına üçüncü taraflarca empoze edilecek anlaşmalarda kendi güvenliklerinin gereksiz yere etkilenmesini engeller.

15. Sosyal Mühendislik Zaafiyetleri Ve Sosyal Medya Güvenliği Politikası

15.1. Sosyal Mühendislik Zafiyetleri

- Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Başka bir tanım ise; İnsanoğlunun zaaflarını kullanarak istediğiniz bilgiyi, veriyi elde etme sanatına sosyal mühendislik denir. Sosyal mühendisler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanların zaaflarından faydalanıp, en çok etkileme ve ikna yöntemlerini kullanırlar.
- Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.
- Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
- Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.
- Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgileriniz paylaşılmamalıdır.
- Şifre kişiye özel bilgidir. Sistem yöneticiniz dâhil telefonda veya e-posta ile şifrenizi paylaşmamalısınız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
- Oluşturulan dosyaya erişecek kişiler ve hakları *"bilmesi gereken"* prensibine göre belirlenmelidir.

- Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.
- Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.
- Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.
- Kazaa, emule, we transfer gibi dosya paylaşım yazılımları kullanılmamalıdır.

15.2. Sosyal Medya Güvenilirliği

- Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
- Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
- Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.

16. YÜRÜRLÜK

Bu politika 22.03.2020 tarihi itibari ile yürürlüğe girmiştir.