KİLİS 7 ARALIK ÜNİVERSİTESİ
ISO 27001:2022
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ
FARKINDALIK EĞİTİMİ
2026

❖ BİLGİ NEDİR ?

Veri ; Sayısal ve mantıksal her bir değere (rakam, harf, sembol) yani İşlenmemiş ham bilgiye denir. (Ör: Tuncay, Bursa, 1978)

Bilgi ; herhangi bir konu ile ilgili verilerin bir araya gelmesi ile oluşan açıklayıcı ifadeler bütününe yani verinin işlenmiş haline denir. (Ör: Tuncay 1978'de Bursa'da doğdu.)

❖ BİLGİ HANGİ BİÇİMLERDE BULUNABİLİR ?

Bilgi birçok biçimde bulunabilir. Kağıt üzerine basılmış veya yazılmış olabilir, elektronik ortamda yaratılmış ve saklanıyor olabilir, çalışan personel tarafından edinilmiş olabilir. Bilgi konuşma sırasında söylenebilir.

Bilgi E-posta yoluyla, taşınabilir ortam işleme cihazları ile (usb flash bellek, harddisk v.b) veya elektronik imkânlar kullanılarak gönderilebilir ve saklanabilir.

❖ BİLGİ HANGİ ORTAMLARDA BULUNUR ?

1. FİZİKSEL ORTAMLAR

- KAĞIT
- YAZI TAHTASI
- DOSYALAR / KLASÖRLER
- DOLAPLAR

2. ELEKTRONİK ORTAMLAR

- BİLGİSAYARLAR, SUNUCULAR, VERİ DEPOLAMA ÜNİTELERİ
- YAZILIMLAR, VERİ TABANLARI
- MOBİL CİHAZLAR
- E-POSTA HESAPLARI
- TAŞINABİLİR ORTAMLAR (USB BELLEKLER , HARDDİSKLER)
- CD-DVD ORTAMLARI

❖ **BİLGİ HANGİ ORTAMLARDA BULUNUR ?**

3. İNSAN

- **ÇALIŞANLAR TARAFINDAN EDİNİLMİŞ VE BARINDIRILIYOR OLABİLİR.**

4. SOSYAL ORTAMLAR

- **TELEFON GÖRÜŞMELERİ**
- **MUHABETLER**

BİLGİ HANGİ ORTAMDA OLURSA OLSUN MUTLAKA KORUNACAKTIR !!!

ISO 27001
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

❖ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) NEDİR ?

Bilgi güvenliğini kurmak (Bilginin Gizlilik, Bütünlük ve Erişilebilirlik kayıplarından korunmasını temin etmek) gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.

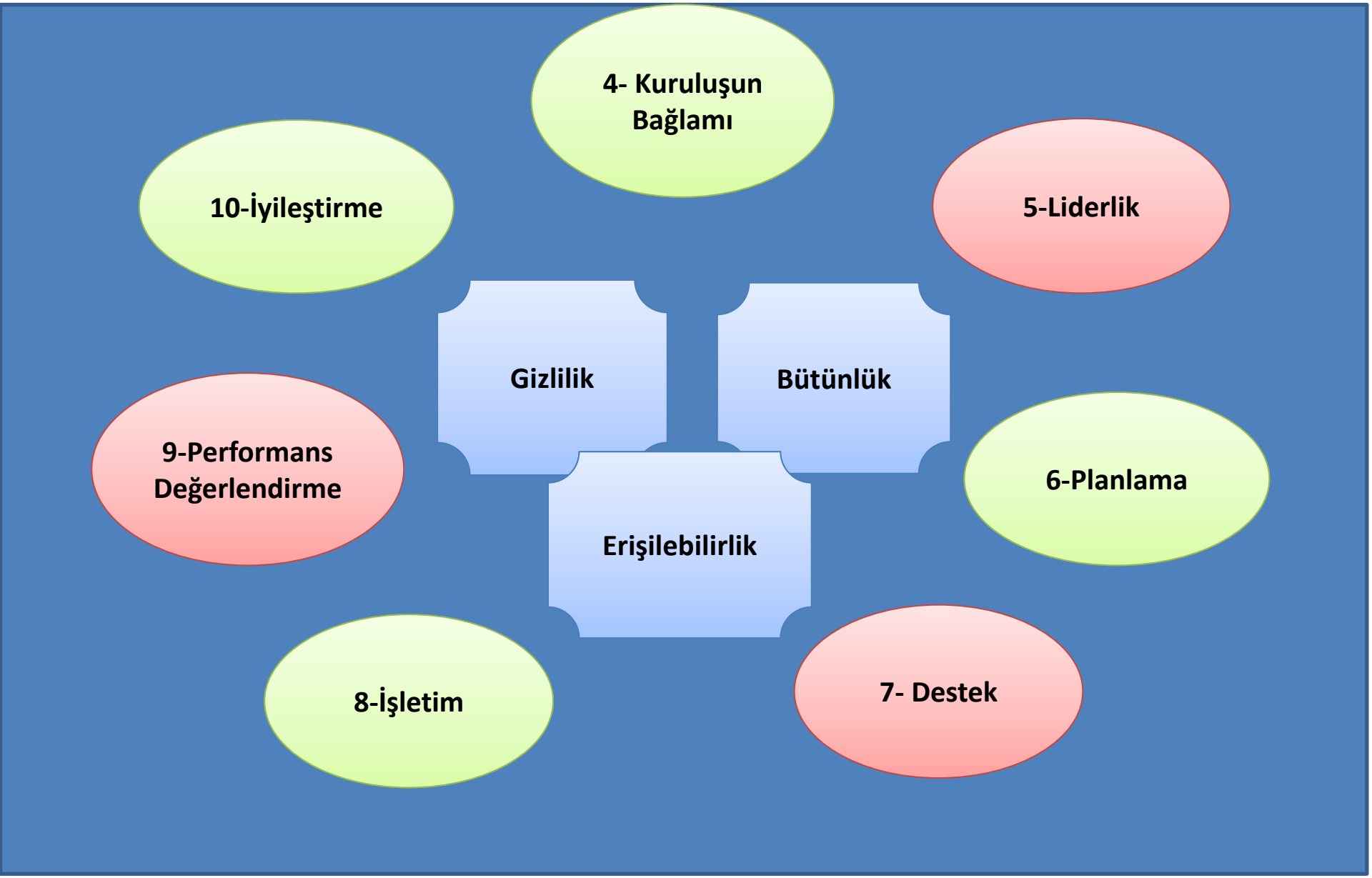
❖ BİLGİNİN KORUNACAK NİTELİKLERİ NELERDİR ?

Gizlilik; Bilginin, istenmeyen biçimde yetkisiz kişilerin eline geçmesinin önlenmesi, yetkisiz kişiler veya uygulamalar tarafından kullanılamaması, bilgilere sadece erişim yetkisine sahip kişilerce erişilebilmesinin garanti altına alınmasıdır.

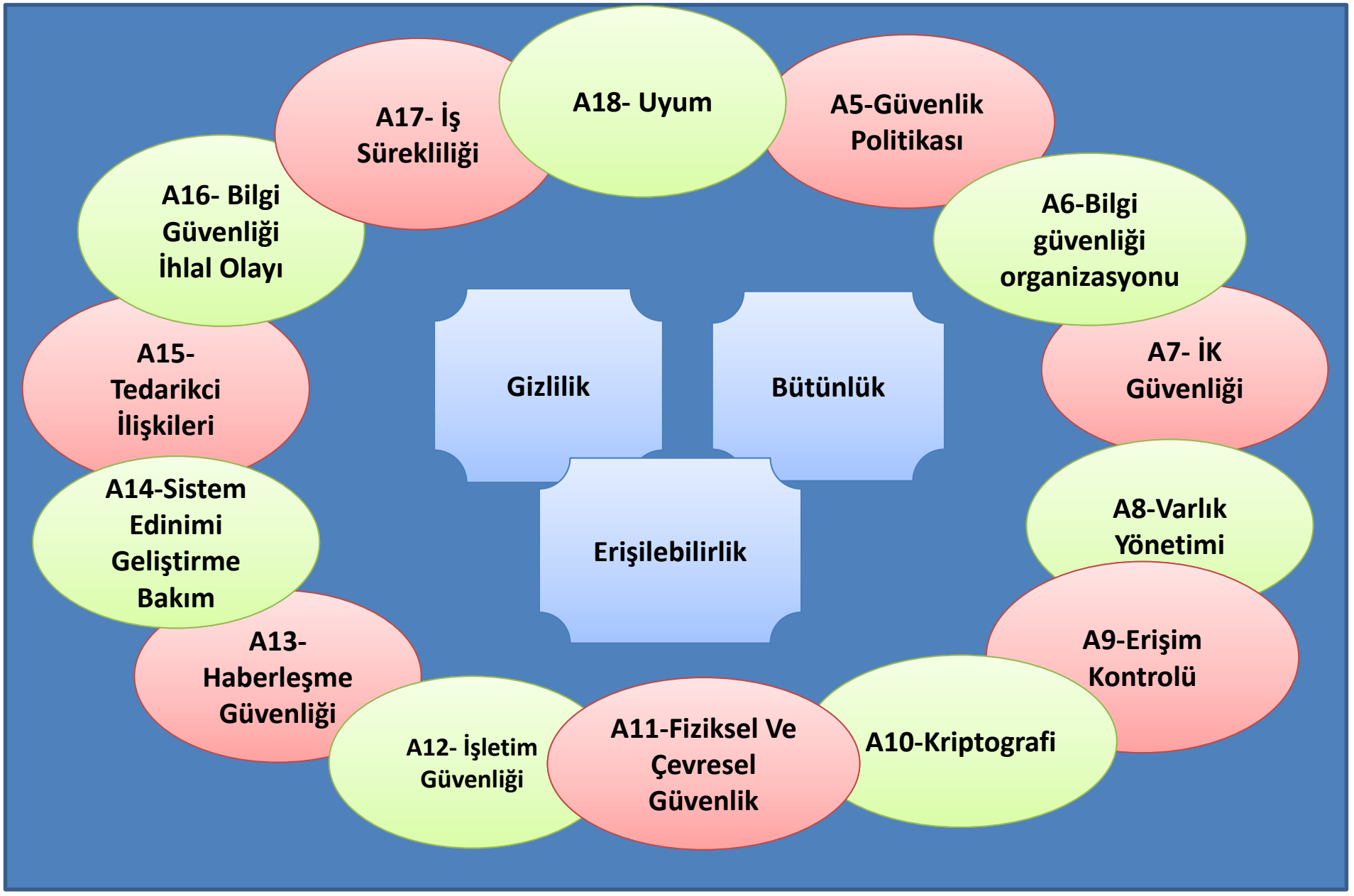
Bütünlük; Bilginin yetkisiz kişilerce değiştirilmemesi, silinmemesi ve bozulmamasıdır.

Ulaşılabilirlik, Kullanılabilirlik; Bilginin ilgili yada yetkili kişilerce sürekli erişilebilir ve amaca uygun olarak kullanılabilir olmasıdır.

27001:2013 Standart Maddeler



27001:2013 Ek-A Kontroller



BİLGİ GÜVENLİĞİ POLİTİKAMIZ

Üniversitemiz

- Bilgi güvenliği Yönetim Sistemi standart şartları ve gereksinimlerine uygunluk sağlanacaktır.
- BGYS kapsamı dâhilindeki, kurumsal ve kişisel bilgilerin ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.
- T.C. yasaları, yönetmelikler, genelgeler, müşteri sözleşmeleri ve işin gerektirdiği yasal mevzuat ile belirlenmiş gereksinimler karşılanacak, bunlar ile uyumlu çalışma sağlanacaktır.
- Kapsam dâhilinde tüm bilgi varlıklarının bilerek veya bilmeyerek yetkisiz kullanımı, değiştirilmesi, açıklanması ve hasara uğratılması önlenecektir.

BİLGİ GÜVENLİĞİ POLİTİKAMIZ

- Bilgi varlıkları üzerindeki risklerin değerlendirmesi yapılarak tespit edilen risklerin kabul edilebilir düzeylere indirilmesi sağlanacaktır.
- Personelin bilgi güvenliği farkındalığını arttıracak ve sistemin işleyişine katkıda bulunmasını teşvik edecek eğitimler düzenli olarak kurum çalışanlarına, yeni işe giren çalışanlara ve ilgili durumlarda tedarikçi çalışanlarına sağlanacaktır.
- Bilgi güvenliği olaylarına ait gerçek ya da şüpheli tüm ihlâller rapor edilecek; tekrar etmesini engelleyici önlemler alınacaktır.
- İş sürekliliği sağlanarak, bilgiye sürekli olarak erişimin sağlanması ve bilginin etkin, doğru, hızlı ve erişim yetkileri gözetilerek güvenli bir biçimde kullanılması sağlanacaktır.
- Bilgi Güvenliği Yönetim Sisteminin uygulanması, sürdürülmesi ve iyileştirilmesi için gerekli kaynaklar sağlanacaktır.

BİLGİ GÜVENLİĞİ EKİPLERİMİZ

BİLGİ GÜVENLİĞİ YÖNETİCİSİ : Hatice DEMİRCİ

BİLGİ GÜVENLİĞİ KURULU

Mehmet Nuh UÇAR	Başkan
Hatice DEMİRCİ	BGYS Üyesi
Ayşe BAYTOK CANBAZOĞLU	Üye
Özkan ZEYBEK	Üye
Murat BİÇER	Üye
Esma ÖZDEMİR	Üye
Yakup DAL	Üye
Veysi BAYINDIR	Üye
Dr. Öğr. Üyesi Zeynep Büşra KORKMAZ	Üye

BİLGİ GÜVENLİĞİ EKİPLERİMİZ

BİLGİ GÜVENLİĞİ ACİL MÜDAHALE EKİBİ

Mehmet Nuh UÇAR	Başkan
Hatice DEMİRCİ	BGYS Yöneticisi
Özkan ZEYBEK	Üye
Murat BİÇER	Üye
Yakup DAL	Üye
Veysel BOLAT	Üye
Ahmet ÜNVANLI	Üye
Mehmet ÖZDEMİR	Üye
Esma ÖZDEMİR	Üye
Recep GÜN	Üye
Furkan BENLİOĞLU	Üye
Musa BAĞÇECİ	7/24 nöbet esaslı güvenlik
Orhan ERTÜRK	7/24 nöbet esaslı güvenlik

BİLGİ GÜVENLİĞİ EKİPLERİMİZ

BİLGİ GÜVENLİĞİ DİSİPLİN KOMİTESİ

Prof. Dr. Mehmet Ali YILDIRIM	Rektör Yardımcısı
Necdet BOZGEYİK	Genel Sekreter
Addulkerim KALKAN	Personel Daire Başkanı
Mehmet Nuh UÇAR	Bilgi İşlem Daire Başkanı
Hatice DEMİRCİ	BGYS Yöneticisi
Öğr. Gör. Ali GENÇ	Kurumsal İletişim Koordinatörlüğü
Dr.Öğr.Üyesi Zeynep Büşra KORKMAZ	Hukuk Müşavirliği V.

BİLGİ GÜVENLİĞİ EKİPLERİMİZ

BİLGİ GÜVENLİĞİ İKLİM DEĞİŞİKLİĞİ (SÜRDÜRÜLEBİLİRLİK) KOMİTESİ

Mehmet Nuh UÇAR	Başkan
Hatice DEMİRCİ	BGYS Yöneticisi
Ayşe BAYTOK CANBAZOĞLU	Üye
Özkan ZEYBEK	Üye
Murat BİÇER	Üye

BGYS SORUMLULUKLARIMIZ

Tüm çalışanlarımız Bilgi güvenliği yönetim sistemi ile ilgili aşağıdaki görev ve sorumluluklara uymakla yükümlüdür.

- BGYS Politikasını bilmek ve gereklerini yerine getirmek,
- BGYS prosedürlerine ve talimatlarına uygun hareket etmek,
- **“Bilmesi gereken”** prensibine ve **“temiz masa temiz ekran”** prensibine göre hareket etmek.

BİLMESİ GEREKEN PRENSİBİ: Herhangi bir konu veya işi, ancak görev ve sorumlulukları gereği öğrenmekle, incelemekle, gereğini yerine getirmekle ve korumakla sorumlu bulunanların yetkisi düzeyinde bilgi sahibi olması.

TEMİZ MASA TEMİZ EKRAN POLİTİKAMIZ

- Kullanıcılar bilgisayarlarının başından ayrılmaları gerektiğinde “Ctrl + Alt + Del” veya “Windows + L” tuş birleşimlerini kullanarak oturumlarını kilitlemelidir.
- Mesai bitiminde tüm kullanıcılar bilgisayarlarını kapatmalıdır.
- Özel, gizlilik derecesine sahip bilgi içeren basılı veya elektronik dokümanlar ekranda veya ofis masalarında kontrolsüz olarak bırakılmayacaktır.
- Özel, Gizli derecesine sahip basılı dokümanlar, CD/DVD, USB Bellek vb. ortamlar kullanılmadıkları durumlarda kilitli dolaplar içerisinde saklanacak, anahtarları kontrolsüz alanlarda bırakılmayacaktır.
- Kullanıcılar şifre bilgilerini başkaları tarafından erişilebilecek alanlarda bulundurmayacaktır.
- Özel, Gizli veya üstü gizlilik derecesine sahip dokümanlar, yazıcılar veya faks cihazları üzerinde kontrolsüz olarak bırakılmayacaktır. Dokümanları toplama sorumluluğu dokümanı gönderendedir.

TEMİZ MASA TEMİZ EKRAN POLİTİKAMIZ

- Özel, Gizli veya üstü gizlilik derecesine sahip dokümanlar, CD,DVD , vb. ortamların imhası kağıt kırpma makinası ile yapılacaktır. USB Bellek, hard disk vb. cihazların imhası Bilgi İşlem bölümü personeli tarafından yapılacaktır. İmha işlemleri, tutanak ile kayıt altına alınarak Bilgi Güvenliği Yöneticisine teslim edilecektir.

- Toplantı sonrasında toplantı odalarındaki tüm evraklar toplanacak, tahta içeriği temizlenecek ve projeksiyon kapatılacaktır. Bu işlemlerin sorumluluğu toplantı sahibine aittir.

- Ofislerde ve toplantı odalarında bilgisayarlar kontrolsüz şekilde bırakılmayacaktır.

BİLGİ VARLIKLARIMIZ
(VARLIK ENVANTERİ)

BGYS kapsamı içerisinde yer alan varlıklarını aşağıdaki kategoriler altında belirlemiştir;

- **Bilgi varlıkları** **:** Kağıt ve Elektronik ortamda tutulan bilgi varlıklarıdır.
- **Yazılım varlıkları:** Üzerinde bilgi barındıran Yazılım varlıklarıdır.
- **Donanım varlıkları :** Üzerinde bilgi barındıran donanım cihazlarıdır. (Bilgisayar, USB Disk, Telefonlar v.b)
- **İnsan kaynakları :** İnsanlar tarafından edinilmiş bilgilerdir.
- **Tedarikçi Hizmetleri :** Bilgilerimize erişimi olan tedarikçi hizmetleridir.
- **Kurumsal itibar ve imaj :** Web sayfamızda tutulan bilgilerdir.

« Varlık sahibi, varlığın kullanımından ve korunmasından sorumludur »

BİLGİ VARLIKLARIMIZ
(VARLIK DEĞERLENDİRMESİ)

Varlık Envanteri oluşturulduktan sonra Varlıklarımızın değerini belirlemek için varlıklarımızın Gizlilik , Bütünlük ve Erişilebilirlik açısından kayıplarının değerlendirmesini yapıyoruz. Gizlilik değeri aynı zamanda bize varlığımızın Bilgi sınıfını da göstermiş oluyor. Değerlendirmemizi ;

Gizlilik : Üçüncü tarafın yada yetkisiz kişilerin eline geçerse firmaya olan etkisi,

Bütünlük : Bilgimizin bütünlüğü (olması gereken durumu) bozulursa, yetkisiz kişilerce yada yanlışlıkla değiştirilse firmaya olan etkisi,

Erişilebilirlik : Bilgimize erişmeye çalıştığımızda erişemezsek ne olur, sorularının yanıtlarını objektif olarak değerlendirme kriterlerine göre vererek 5 li sistemde değerlendiriyoruz.

VARLIK DEĞERİ= GİZLİLİK X BÜTÜNLÜK X ERİŞİLEBİLİRLİK

BİLGİ VARLIKLARIMIZ
(VARLIK DEĞERLENDİRMESİ)

BİLGİ SINIFLANDIRMASI

Halka Açık= 1 , Hizmet İçi = 2 , Özel = 3 , Gizli = 4 , Çok Gizli = 5

Varlık :	Sözleşmeler
Gizlilik:	3 — Gizlilik Derecesi : Özel
Bütünlük:	3
Erişilebilirlik:	4
Değerlendiren :	
Değerlendirme Tarihi:	16.11.2015 15:46:36

		Sözleşmeler		Finans			36	Varlık

Varlık Değeri

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM KURALLARIMIZ

E-POSTA KULLANIM KURALLARI

- E-posta sistemi sadece iş amaçlı olarak kullanılacaktır.
- Kullanıcılar kendi e-posta hesaplarından gönderilen e-posta içeriklerinden sorumludur.
- Özellikle hassas bilgi içeren e-postalar şirket içi ve şirket dışına gönderimlerinde gönderim kurallarına (bilgi sınıflandırması) uyulacaktır.
- E-posta sistemi kullanılarak kurum itibarını küçük düşürücü, dil, din, ırk, cinsiyet, siyasi görüş ayrımı yapan veya ahlak kurallarına aykırı e-posta içeriği göndermek yasaktır.
- E-posta sisteminden SPAM (reklam içerikli yada bir mesajın yüksek sayıda kopyasının) içerikli e-posta gönderimi yasaktır.
- Elektronik posta kutuları için kota uygulaması devrededir. Kullanıcılar kendileri için tanımlanan kota limitine yaklaştıklarında sistem tarafından otomatik olarak uyarılacaktır. Kullanıcılar eski olan tüm e-postalarını silmek ve/veya arşive taşımakla yükümlüdür.

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM KURALLARI

- Tüm kullanıcıların E-posta sunucu altyapısı kullanarak gerçekleştirdiği firma içi ve firma dışı e-posta yazışmaları şirket politikaları gereği arşivlenmektedir. Üst yönetim herhangi bir bilgilendirmeye ihtiyaç duymadan gerek gördüğü durumda tüm yazışmaları inceleyebilir.
- Tüm e-postalar SPAM ve zararlı yazılım kontrolünden geçirilmektedir, alınan tüm önlemlere rağmen kullanıcı şüpheli gördüğü Kaynağı bilinmeyen e- posta ekinde gelen dosyalar kesinlikle açmamalı ve derhal silmelidir. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler. Tanınmayan adreslerden gelen epostaları mutlaka açmadan siliniz. (Örnek Türkcell Fatura, PTT Fatura gibi veri şifreleme linkleri olan epostalar.) e-postayı açmadan silerek, Bilgi İşlem Bölümü' nü bilgilendirmelidir.
- SPAM veya zararlı içerik kontrolü sırasında önemli bilgi içeren e-postalar filtrelemeye takılabilir, kullanıcılar kendilerine gelecek e-postaların takibini gerçekleştirmek ve e-posta sorgulaması için Bilgi İşlem Bölümü' ne talepte bulunmakla yükümlüdür.

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM KURALLARI

- SPAM veya zararlı yazılım kontrolü en güncel yöntemler ile gerçekleştirilmektedir. Gönderen firma kaynaklı sorunlar sebebi ile Bilgi İşlem Bölümü sorumlu tutulamaz.
- Çalışanlar şirketin e-posta adresini iş amaçlı web siteleri dışındaki web sitelerine (alışveriş vb.) üye olmak için kullanmayacaktır.
- Görevden ayrılma vb. sebepler dolayısı ile personelin e-posta hesabının başka bir kullanıcıya yönlendirilmesi sadece ilgili bölüm yöneticisinin yazılı veya e-posta ile onayı sonrasında Bilgi İşlem Bölümü tarafından gerçekleştirilebilir.
- Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- E-posta gönderimlerinde konu kısmı boş bırakılmayacaktır.
- Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar Tarafından görülmesi ve okunmasını engellemekten sorumludurlar,
- E-posta gönderimlerinde e-posta içeriğinin gizlilik derecesine göre gerekli önlemlerin alınması çalışan sorumluluğundadır.

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM KURALLARI

- Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludurlar. Şifrelerinin kırıldığını fark ettikleri andan itibaren yetkililerle (Bilgi işlem ve/veya ilgili birim yöneticisi) temasa geçip durumu haber vermekle yükümlüdürler.
- Altı ay süre ile kullanılmayan e-posta kutuları Bilgi İşlem Birimi tarafından kaldırılır. Kurumdan ayrılan personel kurumsal e-posta sistemini kullanamaz.

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM KURALLARI

İNTERNET KULLANIM KURALLARI

- İnternet altyapısı sadece görev gereği gerekli içeriğe erişmek için kullanılacaktır.
- Kurumumuz tarafından sağlanan internet içeriği 5651 sayılı kanun gereklilikleri, firma etik değerleri, teknik altyapı göz önüne alınarak belirlenmektedir.
- Internet erişimi ile ilgili gerekli güvenlik tedbirleri Bilgi İşlem tarafından alınacaktır, fakat internet erişimi olan sistemlerde %100 güvenlik kesinlikle garanti edilememektedir.
- Kullanıcıların Internet üzerinden program indirmesi yasaktır. Bu konuda bölümlerden gelecek talepler Bilgi işlem bölümü tarafından değerlendirilerek uygun bulunması halinde gözetimli olarak bilgi işlem personeli tarafından gerçekleştirilecektir.
- İnternet erişimlerinde alınan güvenlik tedbirlerini atlatmaya yönelik girişimlerin gerçekleştirilmesi yasaktır.
- Taşınabilir bilgisayar kullanıcıları firma dışındaki internet erişimlerinde de bu maddeler içerisinde belirtilen kurallara uymakla yükümlüdür.

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM KURALLARI

- Servis Sağlayıcılar tarafından sağlanan internet erişimi kullanılarak internet üzerindeki diğer sistemlere servis durdurma vb. saldırılarda bulunulması yasaktır.
- Hassas (gizli) bilgilerin internet üzerindeki dosya paylaşım sunucuları, e-posta servisleri vb. altyapılar üzerinde saklanması ve transfer edilmesi yasaktır.
- Kullanıcıların internet üzerindeki tüm aktiviteleri yasa ve iş gereklilikleri gereği kayıt altına alınmaktadır.
- Şirketin internet alt yapısı kullanılarak şirket itibarını küçük düşürücü, dil, din, ırk, cinsiyet, siyasi görüş ayrımı yapan veya ahlak kurallarına aykırı e-posta içeriği göndermek yasaktır.
- Bilgi işlem bölümü her hangi bir tehdit tespit ettiği durumlarda kullanıcı bazında veya genel olarak internet erişimini kısıtlayabilir ve/veya engelleyebilir.

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM KURALLARI

VARLIKLARIN VE SİSTEMLERİN GENEL KULLANIM KURALLARI

- Taşınabilen bilgi işleyen cihazlar halka açık ortamlarda, araç içinde, toplantı odaları, konferans salonları gibi yerlerde kontrolsüz olarak bırakılmayacaktır.
- Taşınabilir cihazların fiziksel güvenliğinden varlık/risk sahibi sorumludur.
- Taşınabilir bilgi işleyen cihazların (Firma bilgisi içeren kişisel cihazlar dâhil (Akıllı telefon üzerinden kullanılan uygulamalar (E-posta vb.) çalınması kaybolması durumunda varlık/risk sahibi en kısa süre içerisinde Bilgi İşlem Bölümü' ne bilgi vermekle yükümlüdür.
- Çalışanlar şirket bilgilerini düzenli olarak dosya sunucusundaki kendi bölümüne ait kişisel alanlara yedeklemek ile yükümlüdür.
- Taşınabilir bilgisayarlar diskler üzerindeki arızaları ve veri kayıplarını önlemek için işletim sistemi "Kapalı veya Hazırda Beklet" modunda iken taşıma yapılacaktır.
- Taşınabilir bilgisayarlar işyerinde bırakılacak ise yangın tehdidine karşı şarjda bırakılmamalıdır.
- Bilgisayarlar (ofiste bırakıldığı sürece) mesai saatleri dışında mutlaka kapalı konumda muhafaza edilmelidir.

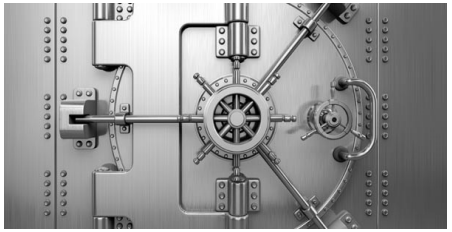
VARLIKLARIN KABUL EDİLEBİLİR KULLANIM KURALLARI

- Şirket tarafından çalışanlara tahsis edilen bilgisayarlar, diğer bilgi işleme ve saklama cihazları (Telefon, USB Bellek vb.) aile fertleri, arkadaş, dış firma vb. kişilerin kullanımına verilemez.
- Taşınabilir bilgi işleme aygıtları kullanılarak halka açık ve güvenliğinden emin olunmayan yerlerde kablolu veya kablosuz bağlantılar üzerinden hassas (gizli) şirket bilgileri ile ilgili işlem yapılamaz.
- Bütün Cep telefonu, PDA (Personel Dijital Asistan), tablet, taşınabilir bilgisayarlar kurumun ğı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, wifi vs.) özellikleri aktif halde olmamalıdır.
- Ağ güvenliğini (örnek, bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozacak (paket sniffing, paket spoofing, denial of service vs.) ortadan kaldıracak eylemlere girişmemelidir. Port veya ağ taraması yapılmamalıdır.

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM KURALLARI

- Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır, Şirket bilgilerini kurum dışından üçüncü şahıslara iletilmemelidir.
- Bilgisayarlarda Telif Hakkı yasası ile korunan (Film – Müzik – Mp3 – Mpg ve diğerleri) Bilgisayara yüklenmesi paylaşılması ve bilgisayarda barındırılması yasaktır. Yükleyenler kanuni yaptırımlar durumunda kendilerinin sorumlu olacaklarını kabul ve beyan ederler.
- Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Yükleyenler kanuni yaptırımlar durumunda kendilerinin sorumlu olacaklarını kabul ve beyan ederler.

BİLGİ SINIFLANDIRMASI VE ETİKETLEMESİ



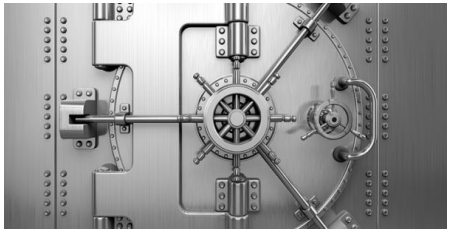
Bilgi varlıklarına ait Bilgi sınıflandırması aşağıdaki gibi yapmıştır;

- **Halka Açık** **:** İçeriğinin hiçbir kısıtlamaya ihtiyaç duyulmadan Halka açılması uygun olan bilgi varlıklarıdır.(Kurumsal web sayfası)

- **Hizmet İçi (Genel) :** Sadece fabrika içi kullanıma açık olabilecek bilgilerdir. İlgili bilginin gizliliğinin ihlal edilmesi minor sonuçlar doğurabilecek bilgi varlıklarıdır. (Telefon numarası, e-posta adresleri, fabrika içi düzenlemeler vb.)

- **Özel** **:** Sadece fabrika / bölüm içi kullanıma açık olan bilgi varlıklarıdır. Yetkisiz kişilerin kullanımına geçmesi durumunda şirket çıkarlarına zararlar verebilecek bilgi varlıklarıdır. Örn. Bölümlere özel bilgiler, Üretim ve kalite süreçleri, Bölümlerin süreçlerine ait bilgiler v.b

BİLGİ SINIFLANDIRMASI



- **Gizli** : Yetkisiz kişilerin kullanımına geçmesi durumunda şirket çıkarlarına büyük zararlar verebilecek (Örn: Müşteri kaybı, Satışların azalması, şahıs veya organizasyonun itibarına zarar verilmesi vb.) bilgi varlıklarıdır.

- **Çok Gizli** : Yetkisiz kişilerin kullanımına geçmesi durumunda şirket çıkarlarına yaşamsal zararlar verebilecek bilgi varlıklarıdır. Örn: Büyük oranda müşteri kaybı, satışlarda keskin ve önemli düşüş, önemli itibar kaybı vb.

BİLGİ ETİKETLEMESİ, TRANSFERİ, İMHASI VE KORUMA KURALLARI

BİLGİ ETİKETLEMESİ

Kullanılmayan hassas bilgi içeren dokümanların, sökülüp taşınabilen medyanın, ortamların (DVD, Usb, Disk ya da Bellek v.b) imhası kağıt kırpma makinası ya da ilgili ortamın yakılması, parçalanması ile yapılır. İmha işlemi tutanak ile kayıt altına alınır.

Ortam başka bir uygulama için kullanılacak ise içindeki bilgiler tekrar geriye dönülemeyecek şekilde yöntemler uygulanarak silinir.

RİSK DEĞERLENDİRMESİ

Varlık Envanteri ve Değerlendirilmesi aşamasından sonra bilgi varlıklarının kategorilerine göre üzerinde barındırdığı zaafiyetlerden dolayı maruz kalabileceği tehditler; Tehditin gerçekleşme ihtimali (Olma Olasılığı) ve Tehdit gerçekleşirse (Tehdidin etkisi) etkisinin değerlendirildiği Risk değerlendirmesi aşaması tüm bilgi varlıkları için gerçekleştirilir. Gerçekleştirme sonunda Risk değeri Kabul edilebilir Risk seviyesinin (243) üzerinde çıkan varlıkların risklerinin düşürülmesi için (kabul edilebilir seviyeye indirilmesi) Risk işleme faaliyetleri gerçekleştirilir.

RİSK = VARLIK DEĞERİ X OLASILIK X ETKİ (sonuç 243 ise kabul edilebilir risk)

Varlık :	Sözleşmeler
Süreç Adı :	
Zaafiyet :	Uygunsuz ortam şartlarına (Rutubet, toz , sıcaklık, nem, kir) karşı hassas olma, Yanabilir, Islanabilir olma, Yetersiz yada eksik fiziksel koruma tasarımı, kontrolü, Firma, tedarikçi çalışan farkındalık eksikliği
Tehdit :	Kullanılamaz, erişilemez hale gelme
Varlık Değeri :	36
Olma Olasılığı:	3
Tehdidin Etkisi:	3
Risk Değeri :	324

ŞİFRE KULLANIM KURALLARI

- Şifreler tüm bölüm çalışanları için en az 7 karakter olması gerekmektedir.
- Parola belirlenirken Büyük harf, küçük harf, rakam ve semboller kullanılacaktır. Ardışık harf ve rakamlar, bilinen isimler, tarihler parola belirlerken kullanılmayacaktır.
- Şifreler karmaşık içeriğe sahip olmaktadır.(En az 1 büyük harf, en az 1 sayı ve en az 1 sembol (*, ? , /, % vb.) kullanılmalıdır.)
- Şifreler en son belirlenen 3 şifre ile benzerlik göstermemelidir.
- Şifrelerin her 72 günde bir tekrar yenilenmesi istenecek, sistem tarafından kullanıcılar son 15 gün kala uyarılacaktır.
- Oturum açma ve şifre değişim işlemleri merkezi log yönetim uygulaması tarafından kayıt altına alınmaktadır.
- Kullanıcılara kullanıcı hesabı açıldığında gizli geçici parola verilir. Geçici parolalar kişiye özel, tek kullanımlık, tahmin edilmesi zor ve tekildir.
- Bilgi sistemlerinde kullanılan bilgisayarların üretici firmaları tarafından verilen varsayılan sistem parolaları mutlak surette değiştirilir.

ŞİFRE KULLANIM KURALLARI

KULLANICI SORUMLULUKLARI

- Kullanıcıların parolaları gizli ve benzersiz olmalıdır ve yukarıda tanımlanan şifre politikalarına uygun olarak oluşturulmalıdır.
- Parola kolay hatırlanabilir, başkaları tarafından kolay tahmin edilebilir olmamalıdır. Tahmin edilemeyecek şekilde oluşturulmalıdır
- Kullanıcılara kullanıcı hesabı açıldığında gizli geçici parola verilir ve kullanıcılar ilk kullanımlarında bu parolayı değiştirmek zorundadırlar.
- **Kullanıcılar parolalarını başkaları ile paylaşmamaktadır. Paylaşanlar hakkında disiplin işlemi uygulanır.**
- Kullanıcılar şifre bilgilerini başkaları tarafından erişilebilecek alanlarda bulundurmayacak, saklamayacaktır.
- Kullanıcıların şifrelerini unutması durumunda sistem yöneticisi tarafından eski parolası sıfırlanarak ilk oturum açma esnasında kullanıcıya yeni parola oluşturtulur.

ERİŞİM YÖNETİMİ VE YETKİLENDİRME KURALLARI

ERİŞİM YETKİLENDİRME KURALLARI

- Kullanıcı adları mutlaka tekildir.
- Tüm kullanıcılar şahsi kullanımları için kendine ait tek bir kullanıcı tanımına sahiptir.
- Kullanıcının kimliğini doğrulamak için uygun bir doğrulama tekniği seçilmiştir.
- Teknik destek personeli, operatörler dâhil her tür kullanıcıya kontroller uygulanmaktadır.
- Kullanıcı tanımları sorumlu personelin faaliyetlerini izlemek için kullanılmaktadır. Tüm kullanıcı faaliyetleri kayıt altına alınmaktadır.
- Rutin kullanıcı faaliyetleri ayrıcalıklı hesaplar üzerinden yapılmamaktadır.
- USB Bellek, Harici Disk vb. Taşınabilir Veri depolama aygıtlarının kullanımı için istisnai durumlar hariç yetki verilmemektedir.
- E-posta adresi olmayan personel için talep **Yetkilendirme Talep Formu** ile gerçekleştirilmektedir.

ERİŞİM YÖNETİMİ VE YETKİLENDİRME KURALLARI

- Internet erişim talepleri **Yetkilendirme Talep Formu** kullanılarak gerçekleştirilir.
- Kullanıcıların faaliyetlerinin izlenmesinin gerekli olmadığı durumlarda (sadece okuma erişimi gibi) genel kullanıcı tanımları kullanılabilmektedir.
- Ayrıcalıklı erişim hakları düzenli iş faaliyetleri için kullanılan kullanıcı kimliğinden farklı bir kullanıcı kimliği ile yapılmakta ve düzenli olarak takip edilmektedir. **Yetkilendirme Talep Formu** onaylanmadan ayrıcalıklı erişim hakları verilmemektedir.
- Kuvvetli yetkilendirme ve kimlik doğrulamasının gerektiği durumlarda sadece parola ile yetinilmeyip veriye erişimin 2. metodla şifrelenmesi, akıllı kartlar kontroller de kullanılmaktadır.
- Ayrıcalıklı yetkilerin tanımlanması kontrollü ve sınırlı olarak yapılmaktadır.
- Parola kullanımı sistemler tarafından kontrol edilir.
- Tüm erişim hakları talepleri (Dosya erişim, İnternet kullanım, E-Mail Kullanım, Telefon kullanım vb. **Yetkilendirme Talep Formu** ile yapılacaktır.

FİKRİ MÜLKİYET HAKLARI

Kuruluşumuzun fikri mülkiyet hakkı gerektiren tüm varlıkları tespit edilmiş (yazılımlar, donanımlar ve diğerleri) lisans veya kullanım hakları ödenmekte ve kayıtları muhafaza edilmektedir.

- Kuruluşumuzda lisanssız yazılım kullanmak ve kurmak yasaklanmıştır, lisanssız yazılım kullananlar ve kuranlar hakkında yasal ve disiplin işlemi yapılır.
- Kuruluşumuzda Lisans çerçevesinde izin verilen kullanıcı sayısının aşılmamasını ve yalnızca yetkili yazılım ve lisanslı ürünlerin yüklenmiş olmasını sağlamak için uygun kontroller devreye alınmıştır.
- Kullanıcıların bilgisayarları üzerinde var olan Local admin hakları alınarak izinsiz yazılım yüklemesi yapılması engellenmiştir.
- Taşınabilir ortam cihazlarının kullanımı sınırlandırılmış ve yetkilendirilerek izinsiz, kontrolsüz yazılım kullanımı ya da kopyalanması engellenmiştir.
- Fikri mülkiyet hakkı gerektiren bilgi varlıkları tespit edilmiş, yılda en az bir kez gözden geçirilmektedir.

GİZLİLİK SÖZLEŞMESİ

Kuruluşumuzun tüm faaliyetlerinde çalışan firma ve tedarikçi personellerine ait hassas (gizli) bilgilerin korunması amacıyla **"Personel Gizlilik Sözleşmesi"** imzalatılmaktadır.

Kuruluşumuzun bilgilerine erişimi olan hizmet tedarikçilerine, kurumumuza ait ait hassas (gizli) bilgilerin korunması amacıyla **" Üçüncü Taraflarla Gizlilik Sözleşmesi"** imzalatılmaktadır.

Personel Gizlilik Sözleşmesi yükümlülüklerine uyulmaması durumunda, gerçekleşen eylemin yoğunluğuna, kaynaklara veya verilen zararın boyutuna, tekrarına göre aşağıdaki yaptırımlar uygulanır;

- Çalışanı sözlü veya yazılı olarak uyarma,
- Çalışanın iş akdine son verilmesi,
- Çalışana tahsis edilmiş bilişim kaynaklarının kullanımını sınırlama,
- Yasalara göre suç teşkil edecek kullanımların ya da bu taahhütname hükümlerine aykırı davranışların tespiti halinde ilgililer hakkında gerekli yasal girişimde bulunma.

GİZLİLİK SÖZLEŞMESİ

Üçüncü Taraf Gizlilik Sözleşmesinde; Taraflardan her biri bu anlaşma tahtındaki ve özellikle bu anlaşmaya göre elde edilen Gizli Bilgilerin açıklanmamasına ilişkin yükümlülüklerinden herhangi birini ifa etmemesi durumunda aşağıda belirtilen maddelerden yükümlü olacaktır.

- Meydana gelebilecek zarar ve ziyanı Türk Ceza Kanunu ve Türk Ticaret Kanunu hükümlülüklerince hukuki ve cezai olarak karşılamakla yükümlü olacak ve bu bilgilerin açıklandığının veya kullanıldığının ortaya çıkması halinde alan taraf daha başka açıklama yapılmasını veya kullanımı önlemek için gayret sarf edecektir.

« Gizlilik Sözleşmeleri; İş akdinin sona ermesinden, üçüncü taraf sözleşmesinin sona ermesinden sonrada geçerli olacaktır»

FİZİKSEL VE ÇEVRESEL GÜVENLİK



Fiziki güvenlik (koruma); Evrak, bilgi, belge, malzeme, bina ve tesislerin yetkisiz kişilerce casusluk, sabotaj, hırsızlık, hasar ve zarar verme gibi eylemlerine karşı korunmasını sağlamak amacıyla alınacak fiziki önlemlerdir. Fiziki güvenlik önlemleri, birbirini bütünleyen bir güvenlik sistemidir.

Fiziki güvenliğin sağlanması için aşağıdaki kontroller uygulanmaktadır;

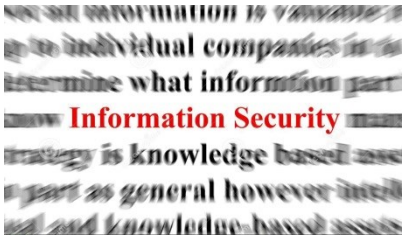
- Personel giriş ve çıkışları ana giriş kapısından yapılması,
- Ziyaretçilerin ziyaret maksadı ve/veya kiminle görüşeceği, kimlik bilgileri ve giriş - çıkış tarih ve saatleri bilgilerinin güvenlik birimi tarafından kayıt altına alınması,
- Ziyaretçilere giriş kartı verilmesi ve ziyaret süresince görünür şekilde taşımalarının istenmesi,
- 7/24 güvenlik görevlisi-görevlileri tarafından çevresel ve giriş güvenliğinin sağlanması,
- Tesise dışarıdan gelebilecek saldırı tehditlerine karşılık olarak kritik bölgelerde önlemlerin artırılması, güvenlik güçleri ile koordinasyon ve işbirliği sağlanması hususlarının sürekli olarak göz önünde bulundurulması,

FİZİKSEL VE ÇEVRESEL GÜVENLİK



- Güvenli alanlara sadece yetkili personeller için giriş yetkilerinin tanımlanması ve giriş kontrolü için Kartlı ve/veya şifreli kontrol mekanizmaları kullanılması,
- Kontrollü alanlara girişte personel sadece kendine tahsis edilmiş kart vb. giriş kontrol mekanizmalarını kullanmak zorundadır,
- Güvenli bölgelere, yetkili personel veya yetki verilen diğer şahısların girmesi sağlanarak kayıt altına alınır,
- Gelen müşteriler veya misafirler Girişte güvenlik görevlisi veya kabul yeri görevlisi tarafından karşılanır. Güvenlik görevlisi ziyaret edilen kişinin ziyaretçiyi karşılamasını sağlar,
- Tüm çalışanlar, üçüncü taraflar ve sözleşme sahipleri görünebilir bir şekilde kimlik kartı taşır,
- İzinsiz fotoğraf makinesi, ses, video, cep telefonu gibi kayıt cihazlarının sokulması veya fotoğraf çekilmesi, ses kaydı yapılması yasaklanmıştır,

BİLGİ GÜVENLİĞİ İHLAL OLAYLARI



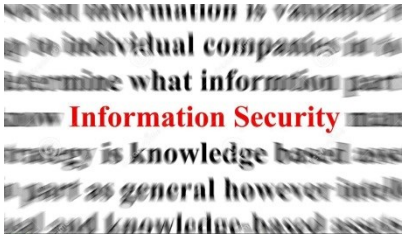
Bilgi güvenliği ihlal olayı

İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

Bilgi güvenliği ihlal olayı tipleri

Gizli bilgilerin, evrakların ifşası
Politikalara aykırı davranma (Bilgi transferi, Varlıkların kullanımı, Şifre Politikası, Temiz masa Temiz ekran politikası v.b)
Virus, Zararlı Yazılım Faaliyetleri
Hırsızlık, Dolandırıcılık
Yetkisiz Erişim
Sabotaj / Sistemi bozma
Telif hakları İhlali
Kasti zarar verme
Bilgi Kaybı – Dosya Silinmesi
Uygunsuz İnternet ve E-Posta kullanımı v.b

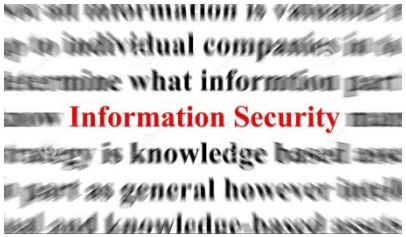
BİLGİ GÜVENLİĞİ İHLAL OLAYLARI – SORUMLULUKLAR



- Firma çalışanları ve tedarikçi personelleri herhangi bir Bilgi Güvenliği İhlal Olayı meydana geldiğinde vakit kaybetmeden **Bilgi Güvenliği İhlal Olayı Formunu doldurarak** durumu uygun iletişim kanallarını kullanarak (telefon ve e-mail yoluyla BGYS Yöneticine veya ilgili birim yöneticisine) durumu bildirmek zorundadır.

- Güvenlik ihlaline neden olan firma çalışanları , üçüncü taraf ve çalışanları ile olaya tanık olan ve bildirmeyen personeller hakkında **Disiplin Talimatı** esaslarına göre disiplin cezaları uygulanır.

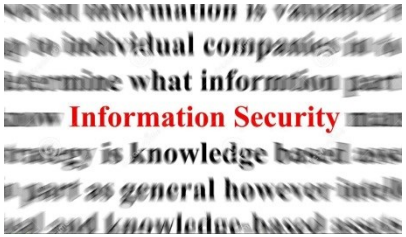
BİLGİ GÜVENLİĞİ İHLAL OLAYLARI – YAPTIRIMLAR



Bilgi güvenliği ihlal olayı gerçekleştiren çalışanlar hakkında, gerçekleştirilen eylemin etkileri değerlendirilerek (Yasal Etkisi, Finansal Etkisi, Müşteri Etkisi, Kurumsal İtibar ve İmaj Etkisi, İş Sürekliliği Etkisi) düzenlenecek bilgi güvenliği ihlal olayı değerlendirme raporuna göre Disiplin kurulu tarafından Disiplin talimatına göre aşağıdaki yaptırımlar uygulanır;

- Çalışanı sözlü veya yazılı olarak uyarma,
- Para Cezası
- Çalışanın iş akdine son verilmesi,
- Çalışana tahsis edilmiş bilişim kaynaklarının kullanımını sınırlama,
- Yasalara göre suç teşkil edecek bilgi güvenliği ihlal olayları hakkında çalışan hakkında gerekli yasal girişimde bulunma.

YASAL VE SÖZLEŞMEYE TABİ GEREKSİNİMLERE UYUM



Kurumumuz için İlgili tüm yasal, meşru, düzenleyici, sözleşmeden doğan gereksinimler ve bu gereksinimlerinin karşılanmasına yönelik yaklaşımlar tanımlanmış ve güncel tutulacaktır. Bu konuda birim yöneticilerinin görev ve sorumluluğu aşağıda tanımlanmıştır;

- Birim yöneticileri kendi birimine ait süreçleri ile ilgili mevzuatın tespit edilmesinden ve güncel bulundurulmasından sorumludur. Mevzuatlar tespit edilirken şirketin iş kollarına ve faaliyetlerine bağlı olarak diğer ülkelerdeki uyulmasını gereken yasal mevzuatlarda dikkate alınacaktır.

UYUM RAPORU

Videoları aşağıdaki oynatma tuşuna basarak izleyebilirsiniz.

Videoları aşağıdaki oynatma tuşuna basarak izleyebilirsiniz.

Videoları aşağıdaki oynatma tuşuna basarak izleyebilirsiniz.

Videoları aşağıdaki oynatma tuşuna basarak izleyebilirsiniz.

Videoları aşağıdaki oynatma tuşuna basarak izleyebilirsiniz.

Videoları aşağıdaki oynatma tuşuna basarak izleyebilirsiniz.

Katılımınız için Teşekkür Ederim

Bilgi Güvenliği Yöneticisi