EGE VİTRİFİYE

# ISO 27001 Bilgi Güvenliği Yönetim Sistemi Farkındalık Sunumu

## Bilgi Nedir ?

Süreçlerin devamlılığı için gerekli olan ve bu nedenle değeri olan, dolayısı ile uygun şekilde korunması gereken bir varlıktır.

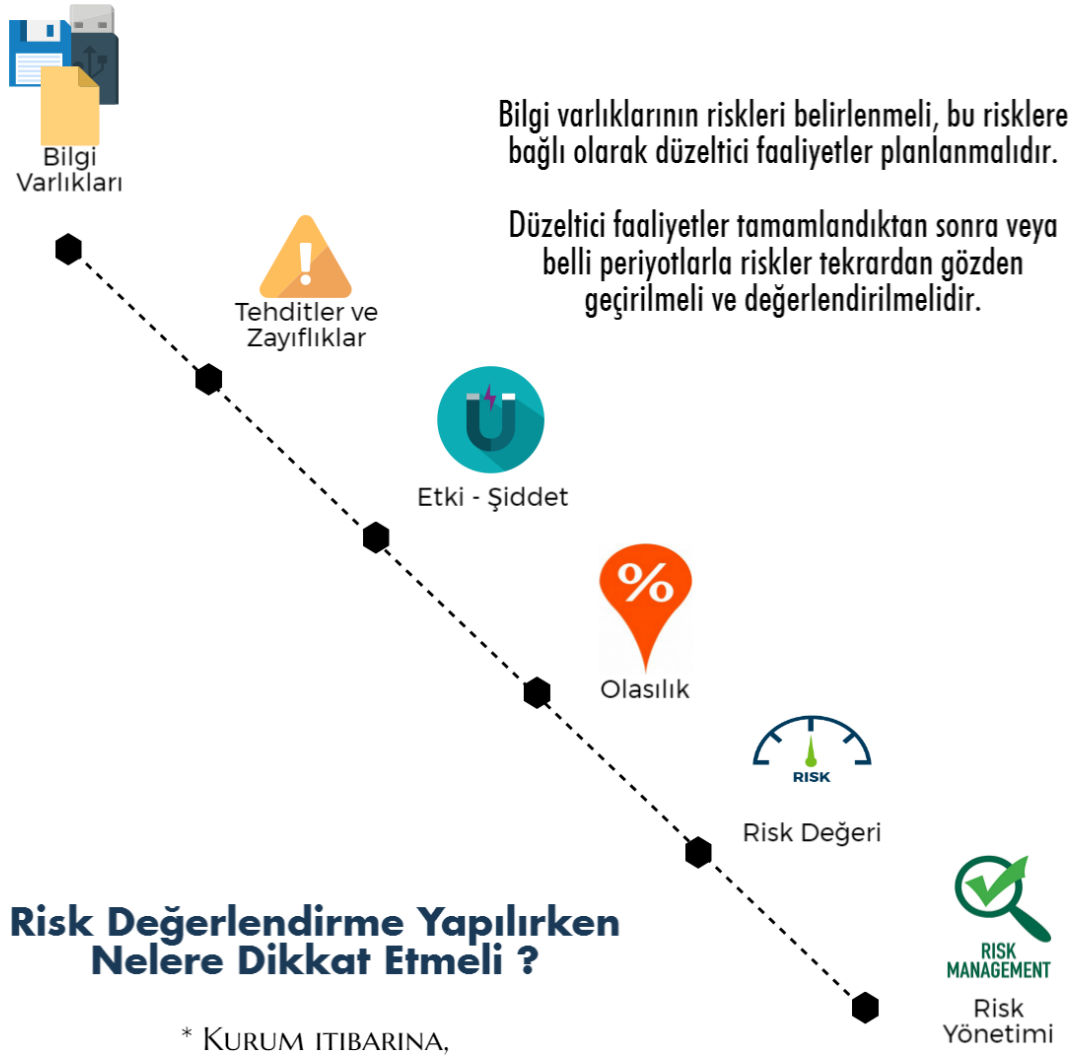
# Bilgi Formatı Nasıldır ?

Kağıt üzerinde yazılı ve basılı olabilir...
Elektronik ortamda saklanmış olabilir...
Karşılıklı konuşmalarda veya toplantılarda sözlü ifadeler şeklinde olabilir...
Sesli ve görsel medya ortamında olabilir...
Posta ve elektronik ortamda gönderilebilir formatta olabilir...
Kişilerin bilgi dağarcıklarında olabilir...

# Bilgi Güvenliği

Bilgi Güvenliği Nedir?

Herhangi bir ortam(elektronik, basılı vb.) üzerinde bulunan bilgilerin yetkisiz erişim, yetkisiz değiştirilme, yetkisiz imhaya karşı korunmasına yönelik tedbirlerdir.




Bilgi varlıklarının riskleri belirlenmeli, bu risklere bağlı olarak düzeltici faaliyetler planlanmalıdır.

Düzeltici faaliyetler tamamlandıktan sonra veya belli periyotlarla riskler tekrardan gözden geçirilmeli ve değerlendirilmelidir.

## Risk Değerlendirme Yapılırken Nelere Dikkat Etmeli ?

* Kurum itibarına,
* Müşteri gizlilik kriterlerine,
* Üretkenliğe,
* Yasal boyutlara,
* Finansal ve diğer etkilere.

# Bilginin güvenlik özellikleri nelerdir ?

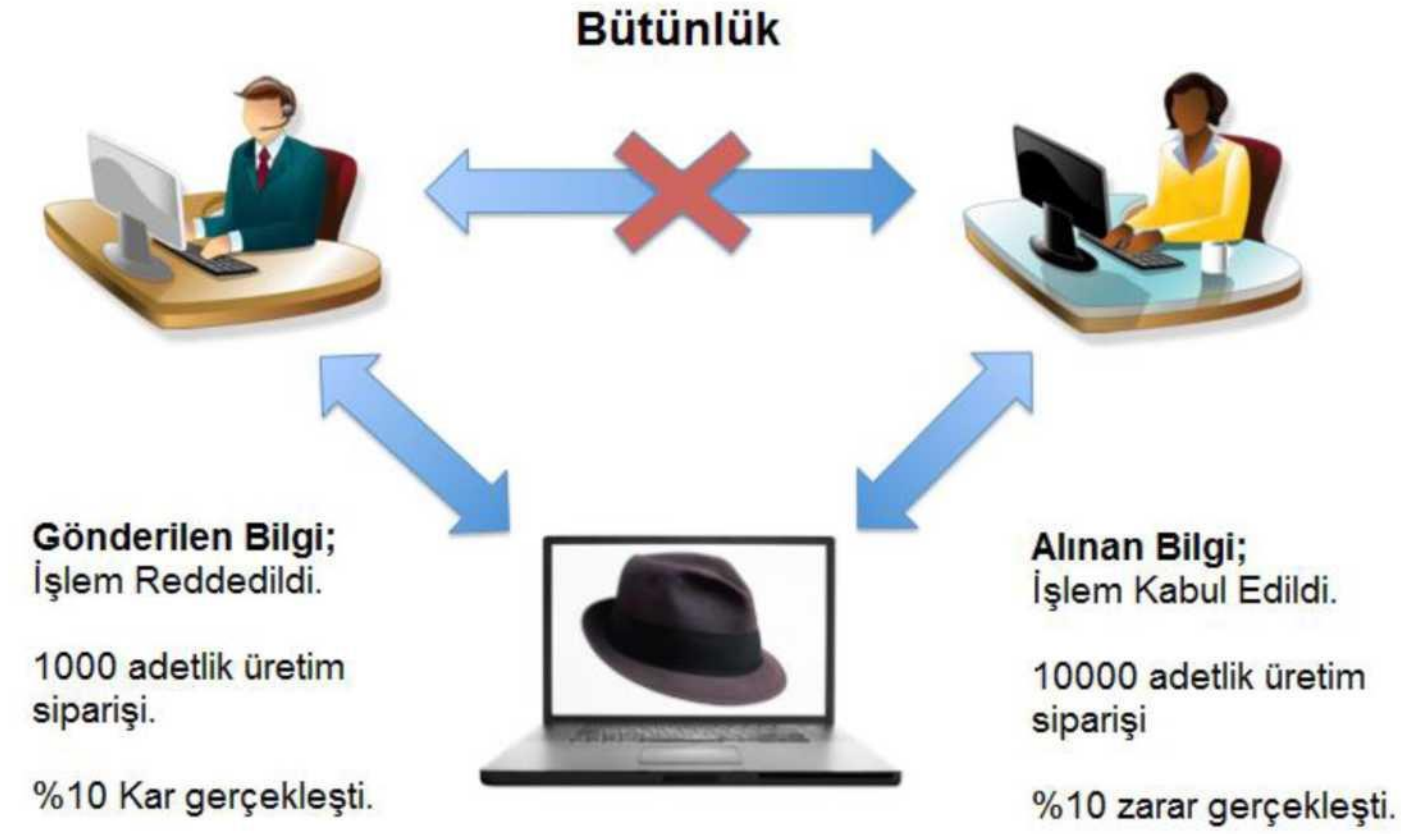
**Gizlilik:** Bilgiye yetkisiz kişilerce erişilmesinin ve bilginin sızdırılmasının önlenmesidir.

**Bütünlük:** Bilginin doğruluğunun ve tamlığının korunmasıdır.

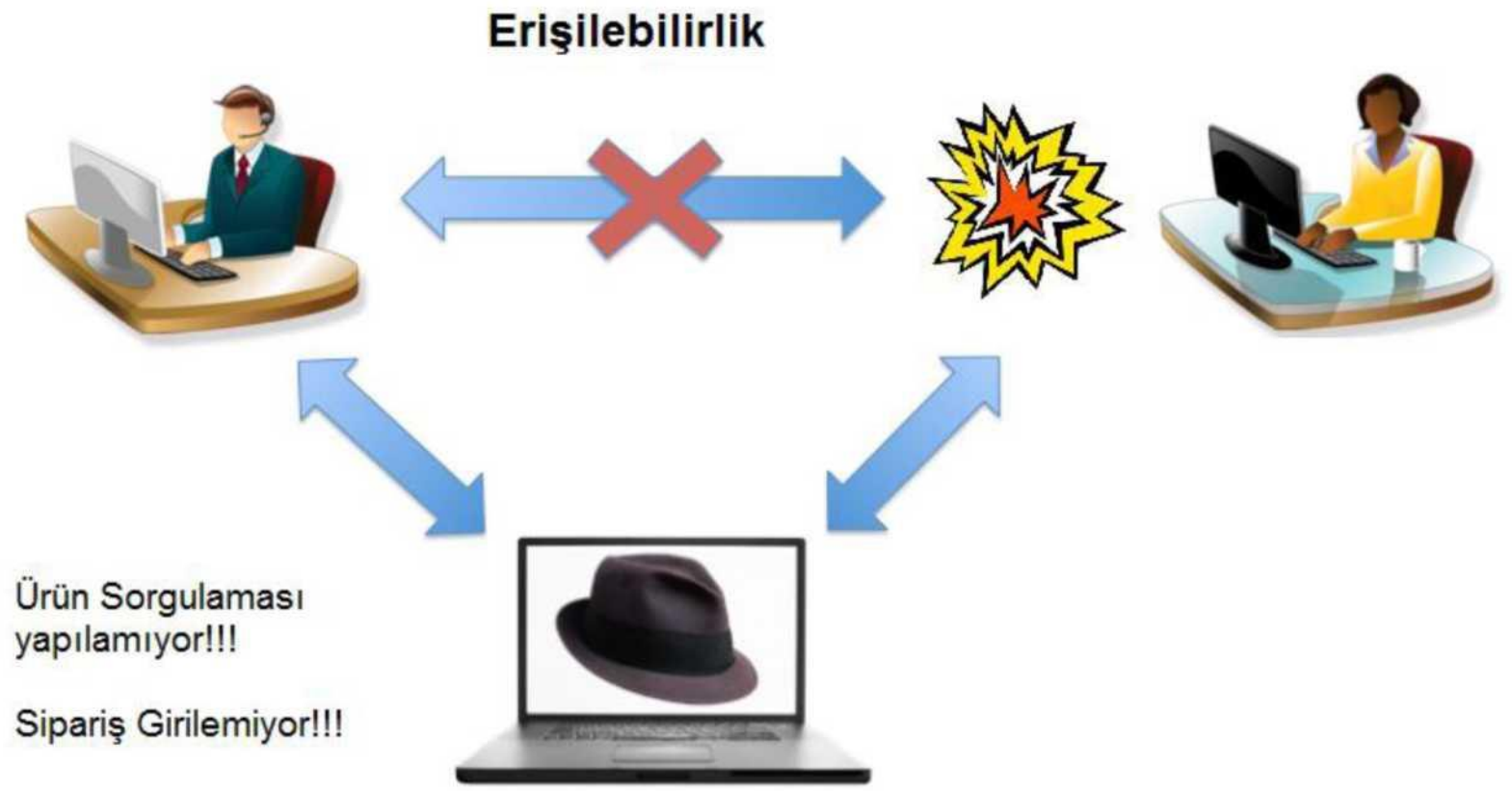

**Erişebilirlik:** Bilginin ihtiyaç duyulduğunda erişilebilir olmasıdır.

# Bilgi Güvenliği (Gizlilik — Confidentiality)

## Bilgi Güvenliği (Bütünlük — Integrıty)



# Bilgi Güvenliği (Erişilebilirlik - Availability)



## Veri Sızıntılarının Anatomisi

### Veri Sızıntılarının Nedenleri

- Kurum İçindeki İyi Niyetli Çalışanlar
- Kuruma dışarıdan yöneltilebilecek saldırılar
- Kurum içindeki kötü niyetli çalışanlar

Bilgi Güvenliği sistemlerinde en zayıf halka kullanıcılar (İnsan) 'dır.

- **Kurum İçindeki İyi Niyetli Çalışanlar**
  - Çalınan Kaybolan PC / NB
  - E-posta, CD/DVD, USB Bellek vb.
  - 3. Şahıs veri kaybı
  - İş süreçleri
- **Hedeflenmiş Saldırılar**
  - Şifre saldırıları
  - DOS & DDOS
  - Zararlı Yazılımlar
  - SQL Enjeksiyonu
- **Kötü Niyetli Çalışanlar**
  - Bilgi Hırsızlığı / Ticareti
  - İşine son verilen çalışanlar
  - Kurum Verileri ile Kariyer

**Bilgi Güvenliği**

## 2. Bilgi Güvenliğinin Önemi

### Bilgi Güvenliği ile Korunan Değerler;

Kurumsal İtibar

Yatırım/Para

Ticari Devamlılık

**Bilgi Güvenliği**

**Bilgi Güvenliğine nasıl destek oluruz ?**

Şirketinizin ve müşterileriniz tarafından sizinle paylaşılan bilgi varlıklarını yetkisiz kişilerin erişimine karşı koruyunuz.

Yazılı onay almadan Ege Vitrifiye bilgi varlıklarını 3. şahıslar ile paylaşmayınız.

Kurumunuzda yaşadığınız bilgi güvenliği ihlallerini en kısa süre içerisinde Ege Vitrifiye Bilgi Sistemleri Departmanına bildiriniz.

# Bilgi Güvenliğine Nasıl Destek Oluruz?

## Kişisel bilgileriniz güvende mi?

**Akıllı Telefon vb. taşınabilir cihazlarınızdaki bilgileri koruyun...**

- Şifre veya PIN kullanın
- Kişisel verilerinizi kriptolayın
- Güvenli olduğundan emin olmadığınız kablosuz ağ'lara bağlanmayın.
- Verilerinizi düzenli olarak yedekleyin.
- Cihazı elden çıkarmadan önce kişisel verilerinizi temizlevin.

## Mobil Cihaz Güvenliği

**Mobil cihazınızı da bilgisayariniz gibi koruyun.**

- Karmaşık Şifreler kullanın otomatik kilitlemeyi aktif edin.
- Kişisel bilgilerinizi kriptolayın.
- En güncel işletim sistemini kullanın.
- Oltalama saldırılarına karşı dikkatli olun... Güvenilirliğinden emin olmadığınız kaynaklardan gelen eposta, dosya, SMS mesajlarını açmayın.
- Zararlı yazılım önleme programları kullanın.

# Bilgi Güvenliğine Nasıl Destek Oluruz?

## Gerçekten o dosyayı indirmeli misiniz ?

Güvenilirliğinden emin olmadığınız dosyaları veya programları bilgisayarınıza indirmek çok tehlikeli olabilir. Bilgisayarınızda bilgisayar korsanlarının erişebileceği Arka Kapılar açabilir, bilginiz dışında klavye hareketlerini ve ekran görüntülerini kaydederek siber suçlulara gönderebilir.

Güvenliğinden emin olmadığınız linklere asla tıklamayın, bilgisayarınıza emin olmadığınız program ve dosyaları indirmeyin.

## Bilgisayarıma zararlı yazılım bulaşması önemli değil, üzerinde hiç bir gizli bilgim yok ki...

**Zararlı yazılım bulaşmış bilgisayar kullanılarak;**

- SPAM mailler gönderilebilir
- Ağdaki diğer sunucu/bilgisayarlara servis durdurma saldırıları yapılabilir.
- Eposta, Çevrimiçi bankacılık vb. şifreler ele geçirilebilir.
- Yasal olmayan şekilde müzik, video vb. dosya dağıtımları yapılabilir.
- Ağdaki diğer sistemlerin şifreleri ele geçirilebilir.

**Bilgisayarınızı koruyun:**

- Güvenliğinden emin olmadığınız link ve ek dosyalara tıklamayın.
- Güvensiz kaynaklardan dosya veya program yüklemeyin.
- Güncel ve güvenlik duvarı özelliği olan zararlı yazılım önleme programları kullanın.
- İşletim sistemi ve programların güncellemelerini mutlaka yükleyin.


# PHISHING (OLTAYA TAKILMA) NEDIR ?

Genellikle çeşitli banka ve finans kurumları tarafından gönderilmiş gibi görünen, acil ve çok önemli konular içeriyormuş gibi duran sahte e-postalardır.

Bu e-postalarda verilen linkler aracılığı ile kart bilgileri, kart şifreleri, internet şubesi şifreleri ve kişisel bilgiler istenmektedir.

## Ne YAPMALIYIZ ?

* Size gönderilen e-posta'nın kimden geldiğinden ve doğruluğundan mutlaka emin olun.

* Online işlemlerinizi gerçekleştirirken, işlem yaptığınız sayfanın güvenli olup olmadığını mutlaka kontrol edin!.

İnternet tarayıcınızın üst kısmında bulunan adres bar'da bulunan adresin "https" olup olmadığını kontrol edin. "https"'in son kısmında yer alan "s" harfi bu sayfanın güvenli ve çeşitli şifreleme metod'ları ile işlem yaptırdığını belirtir.

# Trojan Maillere Örnekler;

**From:** TurkishCargo [mailto:gj@bbsyd.dk]
**Sent:** Tuesday, November 15, 2016 1:21 PM
**To:** <@egeseramik.com>
**Subject:** KL96869626 72TR kargonuz 14.11.2016 adresinize teslim edilememistir

TURKİSH
KARGO

Sayın Müşteri

**KL96869626 72TR** barkod kodlu kargonuz **14.11.2016** adresinize teslim edilememiştir. Lütfen adresinizi güncelleyerek kargonuzu teslim alınız.

Teslim adresi değişmek için Turk Cargo Verileri Düzenleme Formu dikkatle doldurunuz.

Adres Değişikliği Bildirimi

**Önemli**

Kargonuzu 7 çalışma günü içinde almanız gerekmektedır. Herhangi bir ekstra gün için TURKISH CARGO sizden Bir gün için 30YTL para cezası sizden alınacak.

İleriye dönük açıklamalar, tarihsel verileri temel almamakla birlikte, daha çok Turkish Cargo'nin veya Turkish Cargo Limited ve bağlı şirketlerinin gelecekteki sonuçlara, performansa, muhtemel müşterilere, fırsatlara ve etkinliklere ilişkin güncel beklentilerini ve tahminlerini yansıtır.

Söz konusu risk, belirsizlik ve diğer faktörler Turkish Cargo'nin veya Turkish Cargo Limited ve bağlı şirketlerinin en güncel Faaliyet Raporlarında ve ilgili menkul kıymetler mevzuatı kapsamında yaptığı bildirimlerde açıklanmıştır.

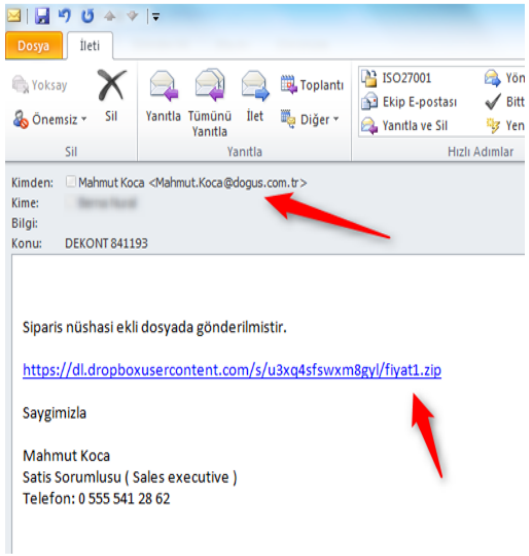
Turkish Cargo'nin ve Turkish Cargo Limited ve bağlı şirketlerinin ilgili mevzuat uyarınca yapılması öngörülenlerin dışında herhangi bir açıklama yapma zorunluluğu bulunmayıp, basın bültenleri veya resmi makamlara sunulması gerekli diğer şirket bildirimleri de dahil zaman yönünden hassas nitelik taşıyan bilgileri güncelleme, düzeltme, değiştirme veya bunlara ekleme yapma konusunda hiçbir sorumluluk üstlenmemektedir.

A Brand of Turkish Airlines Turkish Airlines. All Rights Reserved

# Trojan Maillere Örnekler;

**Subject:** Mail ile trojan atakları hk.
**Importance:** High

Aşağıda örnekleri bulunan trojan saldırıları başlamıştır. Her biri farklı sahte eposta adreslerinden gönderilen epostalar ile sahte sitelere yönlendirilerek bu siteden bir link aracılığı ile zip uzantılı dosya indirilmesi istenmekte ve virüs bulaşması sağlanmaktadır. Konu ile ilgili olarak dikkatli olunması gerekmektedir. Bilgilerinize sunarım.



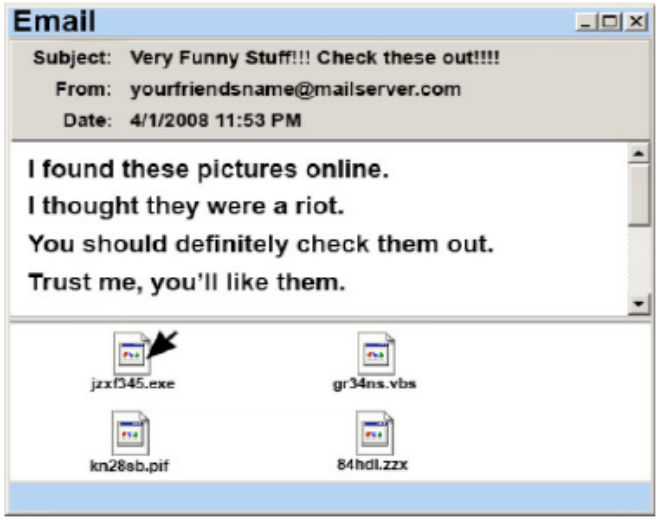


**Halil ULUSAKARYA**
**Ege Seramik Sistem Destek / System Support**

Ege Seramik Sanayi ve Ticaret A.Ş.
Ankara Karayolu 26.km. Kemalpaşa 35170 İzmir / Türkiye
T:(0232) 878 17 00 D:198 F:(0232) 878 12 54 M:(0232) 878 12 54
egeseramik.com

# Bilgi Güvenliğine Nasıl Destek Oluruz?

## E-posta eklerini açmadan önce tekrar düşünün...




**Şüpheli ise, dosyaları açmayın.**

**Dikkatli Olun...**

- Tanımadığınız adreslerden gelen epostalar
- Anlamsız dosya isimleri olan ek dosyalar
- Şüpheli dosya uzantısı olan ekler.
  ( *.exe, *.vbs, *.pif, *.zzx)

# Bilgi Güvenliğine Nasıl Destek Oluruz?

**Siber Güvenlik Hepimizin Sorumluluğundadır.**

**Şirket bilgilerimizi korumalıyız.**

- ✓ Şifrelerinizi hiç kimse ile paylaşmayın.
- ✓ Şüpheli gördüğünüz durumları hemen Bilgi İşlem bölümüne bildirin.
- ✓ Ortak klasörlerde gizli / kişisel bilgileri saklamayın.
- ✓ Şirket verilerini düzenli olarak Kişisel klasörlerinize yedekleyin.
- ✓ Hassas veri içeren şirket bilgilerinin epostə, USB Bellek vb. ile gönderimleri sırasında dosyaları şifreleyin.
- ✓ Gizli / Hassas Şirket bilgileri konusunda bilgi paylaşmayın.

**Hassas bilgi içeren dosyaları şifreleyin.**


**Şüpheli gördüğünüz durumları Bilgi İşlem bölümüne haber veriniz.**


**Bilgisayarınızı kullanmadığınızda oturumu kilitleyin.**

**Şirket bilgilerini kontrolsüz olarak ofiste / araçta vb. bırakmayın.**

## Bilgi Güvenliğine Nasıl Destek Oluruz?


## Bilgi Güvenliğine Nasıl Destek Oluruz?


## Bilgi Güvenliğine Nasıl Destek Oluruz?


## Bilgi Güvenliğine Nasıl Destek Oluruz?

# Şifre Güvenliği

**Bilgisayar ve uygulama şifrelerinizi hiç kimse ile paylaşmayın...**

Şifrelerinizin başka kişiler tarafından bilinmesi durumunda;

- E-postalarınız okunabilir !
- Sizin adınıza e-posta gönderimi yapılabilir!
- Dosyalarınıza erişilebilir !
- Dosyalarınız silinebilir !
- Uygulamalarda sizin adınıza işlemler gerçekleştirilebilir!

Not: Bilgi İşlem altyapısında kullanıcı aktivitileri kayıt altına alınmaktadır. Sorumluluk ilgili kullanıcı hesabında olacaktır.

Şifrelerinizi başkaları tarafından erişilebilecek alanlarda saklamayın.

# Şifre Güvenliği

**Şifreleriniz de parmak iziniz gibi benzersiz olmalıdır.**


**Masadan kalkarken bilgisayarlar <u>kesinlikle</u> kilitlenmelidir.**
**( CTRL + ALT + DEL – Kilitle veya Windows tuşu + L )**

**Ayrıca masada veya bilgisayar ekranlarında kullanıcı adı – şifre <u>yazılmamalıdır.</u>**

**Bilgi Güvenliğine Nasıl Destek Oluruz?**

# Şifreler;

Tahmini kolay ve anlamlı olmamalıdır !
(ör: “Anne kızlık soyadım”)

Herhangi bir yere yazılmamalıdır !

# ŞİFRELER GÜÇLÜ OLMALIDIR

EGE VİTRİFİYE

Uzun Olmalı

Karmaşık Olmalı

Değiştirilme Sıklığına Uyulmalı

# GÜÇLÜ BİR ŞİFRE NASIL BELİRLENİR ?

* En az 6 karakter uzunluğunda olmalı,

* Büyük harf, küçük harf, sayı ve alfabetik olmayan karakter (örn. !, $, #, %) içermeli,

* Kullanıcının hesap adını veya kullanıcının tam adını içermemeli,

* 30 günde bir şifreler değiştirilmelidir.

EGE VİTRİFİYE

# GİZLİ BİLGİ İÇEREN BELGELER FAX VE YAZICI ÜZERİNDE BIRAKILMAMALIDIR.

This block is for comparisons.

Try breaking the differences into bullet points to keep it concise.

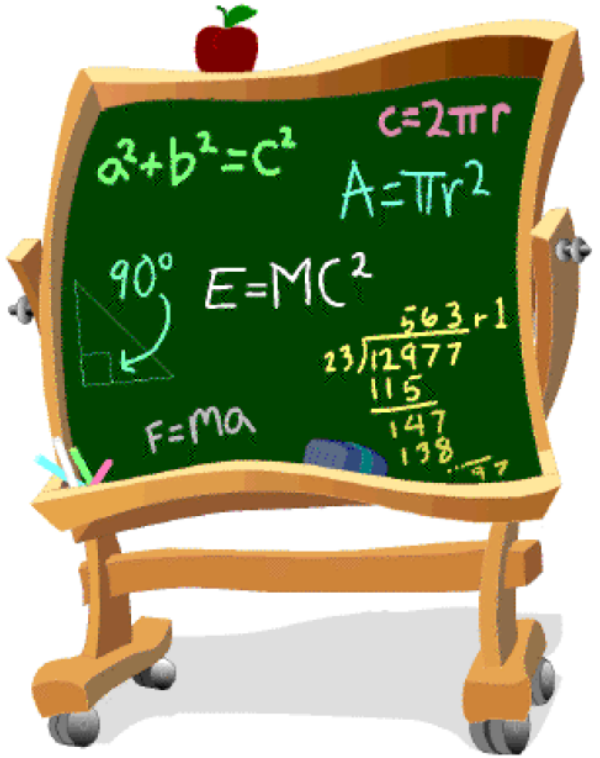
It's best if your text doesn't go beyond 4 lines. Less is more!

**Bilgi Güvenliği**

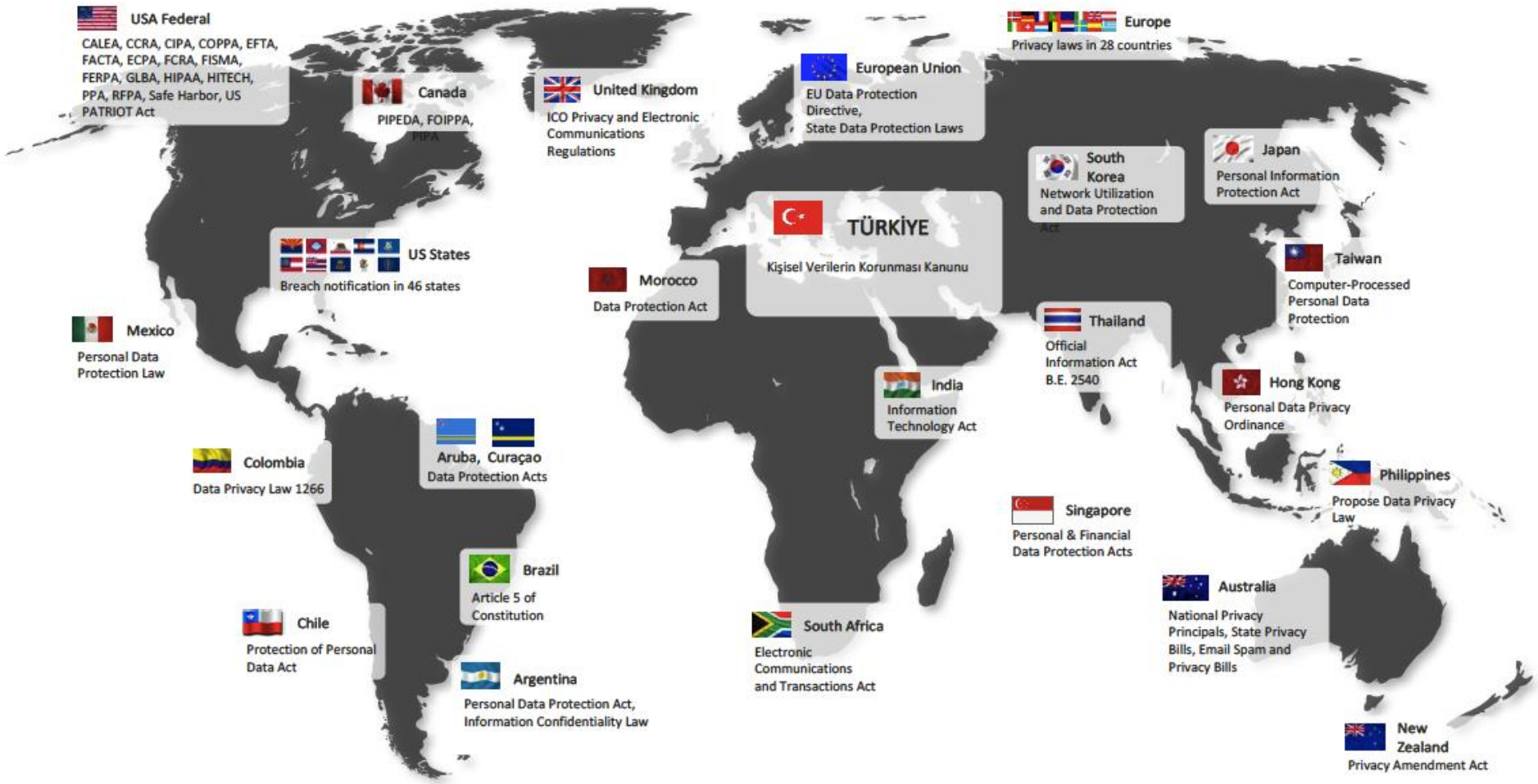
Gizli bilgi içeren belge ve araçlar geri dönüşü sağlanamayak şekilde imha edilmelidir.

**Bilgi Güvenliği**

Toplantı odalarında döküman bırakılmamalı, tahta silinmelidir.



# KİŞİSEL VERİLERİN KORUNMASI



## Kişisel Veri Nedir ?


KİŞİSEL VERİ, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.

# Kişisel Veriler Nelerdir ?

# Özel Nitelikli Kişisel Veri Nedir?

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN, ilgilinin **açık rızası** olmaksızın işlenmesi **yasaktır**.

# Kişiler

Kişisel verilerin korunması hukukunda taraflar

**İLGİLİ KİŞİ**

Kişisel verisi işlenen gerçek kişidir.

**VERİ İŞLEYEN**

Veri sorumlusunun **verdiği yetki**ye dayanarak **onun adına** kişisel verileri işleyen gerçek veya tüzel kişidir.

**VERİ SORUMLUSU**

Kişisel verilerin **işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu** olan gerçek veya tüzel kişidir.

Kişisel verileri hukuka aykırı kaydetmek: 1-3 yıl

Nitelikli kişisel verileri hukuka aykırı kaydetmek: 1,5-4,5 yıl

Kişisel verileri başkasına vermek, yaymak veya ele geçirmek: 2-4 yıl

Kanunla belirlenen süreler geçmiş olmasına rağmen verileri yok etmeme: 1-2 yıl

Ceza muhakemesi Kanunu'na göre silinmesi gerekenler: 1,5-3 yıl

## İDARİ HAPİS CEZASI

**ISO/IEC 27001:2013**

# ISO 27001 BGYS'nin Faydaları

- ✓ Kuruluşlar, bilgi varlıklarını belirler ve bilgi değerlerinin farkına varır.
- ✓ Bilgi varlıklarını koruma metotlarını belirleyerek korumaya başlar.
- ✓ Olası bir güvenlik ihlâlinin etkilerini minimize ederek İş Sürekliliği sağlar.
- ✓ Müşterilerin, tedarikçilerin ve çalışanların güvenini kazanır.
- ✓ Ulusal ve uluslararası pazarda yüksek prestij sağlar.

**ISO/IEC 27001:2013**

# ISO 27001 BGYS'nin Faydaları

- ✓ BGYS ön şartı, beklentisi, sözleşme şartı olan pek çok kuruluş ile iş yapmanızı sağlar.
- ✓ IT sisteminizin güvenli olduğunu tüm taraflara açıklamanızı sağlar.
- ✓ Sitem zaaflarını ve güvenlikle ilgili tehlike risklerini azaltır.
- ✓ Mevzuata uyumluluğunuzu yetkili makamlara kanıtlamanıza yardımcı olur.

# EGE VİTRİFİYE BİLGİ GÜVENLİĞİ POLİTİKASI

Ege Vitrifiye Bilgi Güvenliği Politikasına
Web Sitemiz üzerinden erişebilirsiniz.


www.egevitrifiye.com