1. AMAÇ

Ege Üniversitesi (E.Ü.) Diş Hekimliği Fakültesine başvuruda bulunan kişilere ve personelimize ait kişisel bilgilerin güvenliğinin sağlanması amaçlı verilerin doğru olarak toplanması, depolanması ve kullanılmasın sağlamak, risklere karşı güvenlik önlemlerimizi almak kurumsal riskler kadar kullanıcı kaynaklı risklerinde en aza indirgenmesini sağlamaktır.

2. KAPSAM

E.Ü. Diş Hekimliği Fakültesine başvuruda bulunan kişiler, dış kurumlardan staj için gelen öğrenciler, personele ait kişisel bilgileri ve kurumsal faaliyet bilgilerinin güvenliğiyle ilgili hususları kapsar.

3. KISALTMALAR

HBYS	**:**	Hasta Bilgi Yönetim Sistemi
CD	**:**	Compact Disk
DVD	**:**	Digital Versatile Disc (Çok Amaçlı Sayısal Disk)
USB	**:**	"Universal Serial Bus (Evrensel Seri Veri yolu)
SGK	**:**	Sosyal Güvenlik kurumu
İP	**:**	Internet Protocol Address
NTP	**:**	Network Time Protocol (Ağ Zamanlama Protokolü)
VPN	**:**	Virtual Private Network (Sanal Özel Ağ)
IPsec	**:**	IP Security
TLS	**:**	Transport Layer Security
SSH	**:**	Secure Shell

4. TANIMLAR:

Varlık: kurum içi değeri olan her türlü unsur (insan, donanım, yazılım, bilgi, vs.)

Gizlilik: Bilgiye sadece erişme izni olan yetkili kişiler ya da sistemlerin erişimini sağlamaktır.

Bütünlük: Bilginin tutarlılığı sağlamak amacıyla bilginin yetkisiz kişi ya da işlemler tarafından değiştirilmemesini sağlamaktır.

Erişilebilirlik: Bilgiye doğru zamanda erişimin ve erişim sürekliliğinin sağlanmasıdır.

Bilgi Güvenliği İhlal Olayı: Bilgi Güvenlik Politikalarının ve prosedürlerinin dışında işlem tesis edilmesi ile iş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek yada bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayıdır.

Bilgi Sistemleri: Donanım, yazılım, bilgisayar ağları ve insan unsurlarından oluşan, veri ve bilgileri toplayan, kaydeden, işleyen, dönüştüren ve yayan sistemler bütününü ifade eder.

Spam: Kullanıcının isteği dışında gelen e-postadır.

Phishing: Güncelleme veya program indirme sitelerinin taklit edilerek yazılımının yükletilmesinin sağlanması.

Yer Sağlayıcı, internet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir.

İNSAN KAYNAKLARI ZAFİYETİ YÖNETİMİ

Fakültemizde görev yapan tüm personellerin kurumda işe başlarken ve kurumdan ayrılış yaparken yapması gereken işlemler aşağıda sırasıyla belirtilmiştir. Bu işlemlerin tamamlanmadan işe başlanmaması ve kurumdan ayrılış yapılmaması kişinin çalışacağı/çalıştığı Birim Sorumlusunun takibinde olacaktır. Kuruma Başlayış ve Kurumdan Ayrılış Formlarında yer alan birimlerin uzmanları veya birim sorumluları bu prosedür de belirtilen işlemleri yaptıktan sonra formlarda bulunan tarih, imza ve imza yetkilisinin adı soyadı kutularını doldurarak imzalamakla yükümlüdür.

Kuruma Başlayış İçin Yapılacaklar

- Kurumda göreve başlayan personelin, personel birimi tarafından Sağlık Personeli Takip Sistemine giriş yapılır. Kişi oryantasyon eğitimi için başlayış yazısıyla birlikte Kalite Yönetim Birimine başvurur.
- Kişinin kurumsal kimlik kartı Rektörlük tarafından temin edilir. Ayrıca döner sermaye birimine başlayış yazısıyla birlikte başvurur
- Kişi başlayış yazısıyla birlikte Bilgi İşlem Birimine giderek Tablo 1'deki görev tanımı uygun HBYS erişim ve yetkilendirme tablosuna göre kullanıcı adı ve şifre yaratılarak yetkilendirilir. Görev tanımı dışında yetki talebi olması durumunda İntranet üzerinden Bilgi İşlem İstek Formu doldurularak istekte bulunur. Yönetim tarafından uygun görülmesi durumunda yetki değişikliği yapılır.
- Kişi, başlayış yazısıyla birlikte Dekanlığa üst yazı ile ihtiyaç duyduğu araç ve gereçler için talepte bulunur.

SOSYAL MÜHENDİSLİK ZAFİYETLERİ

Sosyal Mühendislik zafiyetlerine yönelik işlemler fakültemizin **"Sosyal Mühendislik Zafiyetleri ve Sosyal Medya Güvenliği Talimatı**"na göre yönetilmektedir.

- Kullanıcı sosyal medya tarafından yapmış olduğu her paylaşımdan kendisi sorumludur. Paylaştığı bilgileri seçerken ve paylaşımda bulunurken Fakültemizin Bilgi Güvenliği Politikasına uygun hareket etmelidir.
- Kullanıcı, taşıdığı ve işlediğiniz verilerin öneminin bilincinde olmalıdır. Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket etmelidir.
- Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.
- Özellikle telefonda e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgiler paylaşılmamalıdır.
- Şifre kişiye özel bilgidir. Sistem yöneticisi dahil telefonda veya e-posta ile şifre paylaşılmamalıdır.
- Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
- Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
- Sosyal medyada içeriği bilinmeyen linklere giriş yapılmamalıdır.

HBYS ERİŞİM ve YETKİLENDİRME TABLOSU		
	Görev Tanımı	**HBYS Erişim ve Yetkilendirme Modülleri**
1	Yöneticiler, Bilgi İşlem Personeli	Muhasebe Modülü Faturalama Arıza Takip Modülü Diş Klinik Modülü Hasta Kayıt Modülü Vezne Modülü Ayniyat ve Ambar Modülleri PACS Modülü İnsan Kaynakları Modülü Protez Takip Modülü Randevu Modülü Satın Alma Talep Formu Yönetici Takip Ekranları
2	Diş Hekimleri	PACS Modülü Arıza Takip Modülü Diş Klinik Modülü Randevu Modülü Malzeme Talep Formu
3	İdari Personel	Muhasebe Modülü Arıza Takip Modülü Ayniyat ve Ambar Modülleri İnsan Kaynakları Modülü Satın Alma Talep Formu Malzeme Talep Formu
4	Diş Klinik Yard. Personeli	Arıza Takip Modülü Randevu Modülü Hasta Kayıt Modülü Malzeme Talep Formu
5	Teknik Personel	Arıza Takip Modülü Satın Alma Talep Formu Malzeme Talep Formu
6	Diş Teknisyeni	Protez Takip Modülü Arıza Takip Modülü Malzeme Talep Formu
7	Özel Protez Lab. Tems.	Protez Takip Modülü Arıza Takip Modülü
8	Temizlik Personeli	Arıza Takip Modülü
9	Özel Güvenlik Personeli	Arıza Takip Modülü (Beyaz kod modülü)

BİLGİ VARLIKLARIMIZ

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

Bgys.ege.edu.tr Adresinde varlıklarımız kayıt altında tutulmaktadır

Varlık Sınıflandırması

BİLGİ SINIFLANDIRMA KILAVUZU		**Saklanma Yeri Dolap**
GİZLİ	En kritik bilgilerdir, sadece üst 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 işisel bilgisayarlar
İÇ KULLANIM	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır.	Departmanın kilitli dolapları, kişisel bilgisayarlar
KİŞİSEL	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. Erişilebilirlik ön plandadır.	Çalışma masasının kilitli çekmeceleri
KURUMA AÇIK	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın kilitli ortak dolapları
HALKA AÇIK	Bu bilgiler üniversitemiz network birimi ve tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Her türlü fiziki ortam, erişime açık elektronik ortamı

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

ERİŞİM KONTROLÜ

Erişim Kontrol Politikası

- Erişim kontrolünün amacı, bilgi ve bilgi işleme tesislerine yapılacak olan erişimlerin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesine imkân verecek bir sistemin tesis edilmesidir.
- Herhangi bir gizliliği olmayan, herkesin erişimine açık olan (tasnif dışı gizlilik dereceli) bilgiler için özel bir erişim kontrol tedbiri alınmasına gerek yoktur. Bu tür bilgiler, kurumların İnternet sitelerinin vatandaşlara açık bölümlerine konulabilir. Bina ve tesislerde duyuru panosu vb. ortamlarda yayımlanabilir.
- Bilgiye verilen gizlilik derecesi yükseldikçe, uygulanacak olan erişim kontrol politikalarının sıkılaştırılması (zorlaştırılması) gerekir.
- Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir.
- Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.
- "Görevlerin ayrılığı" prensibi uyarınca; kritik iş süreçlerinin gerçekleştirilmesi için birden fazla kullanıcı görevlendirilir. Bilgiye erişim için aşamalı yetkilendirme yapılarak, bir kişinin kendi başına tüm bilgi varlıklarına erişimi engellenir. Teknik nedenlerle görev ayrımı yapılamayan süreçlerin (örneğin etki alanı yöneticisi, veri tabanı yöneticisi vb.) kontrolü için ilave tedbirler alınır.
- "Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.
- Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Yapılacak risk değerlendirmesine göre daha kritik sistemler için farklı kimlik doğrulama yöntemleri (akıllı kart, tek kullanımlık parola, parmak izi / retina / avuç içi tarama vb.) kullanılabilir.
- Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur.
- Üniversitemiz network ağı dışındaki ağlar güvensiz ağ olarak kabul edilir. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için yetkili girişi ve ip güvenliği ile birlikte sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.
- Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. Veri tabanı yönetim sistemi sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.
- Bilgi varlıklarına fiziksel olarak yapılacak erişimler için gerekli önlemler alınır.
- Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için Kişisel Verileri Koruma Kurulu'nun 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir. SGK'ya 3 bildirim yapılır. Bildirimlerin ip üzerinden yetkili bilgisayarlar tarafından girişi sağlanır.

KULLANICI ERİŞİMLERİNİN YÖNETİMİ

- Kullanıcı erişimlerinin yönetimi, sistem ve hizmetlere yetkisiz olarak yapılacak erişimleri engellemek, sadece yetkili kullanıcıların erişimlerini temin etmek için yapılır.

- Tüm sistem ve hizmetler için kullanıcı erişimi ile ilgili hususlar Erişim Kontrol Politikası içinde belirtilir. İlgili tüm kullanıcılara resmen duyurulur.

- Hizmet veya sistemlerin sahiplerince erişim hakları periyodik olarak incelenir. Bilmesi gereken prensibi uyarınca, gereksiz olarak verilmiş yetkilerin kaldırılması sağlanır.

- İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en fazla altı aylık aralıklarla yapılır.

- Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında gözden geçirilir.

- Ayrıcalıklı hesapların tahsisi ve kullanımı ile ilgili incelemeler, üç ayı aşmayacak şekilde daha sık yapılır.

- 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır.

- Ayrıcalıklı erişim hakkı verilen kullanıcı sayısı (etki alanı yöneticisi, veri tabanı yöneticisi vb.) asgari düzeyde tutulur. HBYS program sınırlaması ile kontrol altındadır.

RİSK YÖNETİMİ

- Bilgi yönetim sistemine yönelik fiziksel tehlikeler, yazılım ve donanımla ilgili sorunlar, bilgi güvenliği bilgi mahremiyeti kişisel verilerin korunması kullanıcı hataları gibi konularda risk değerlendirmesi yapılır
- Tespit edilen riskler doğrultusunda iyileştirme çalışmaları başlatılır.
- Risk değerlendirmesi en geç altı ayda bir olur. Düzenli yapılır

PAROLA GÜVENLİĞİ

Parola Güvenliği ile ilgili işlemler fakültemizin "Parola Güvenliği Talimatı"na göre yönetilmektedir.

- Domain sisteminde her personel için ayrı "adı soyadı" formatında küçük harflerle kullanıcı tanımlanır. Şifrelerin en az sekiz (8) karakter olması, en az bir büyük harf, bir sayı veya kompleks karakter(*,+,%- vb.) içermesi, kullanıcı adıyla aynı olmaması yapılan ayarlama ile zorunlu hale getirilmiştir.

- Sistem tarafından yapılan ayarla, domain deki şifrelerin her 180 günde bir değiştirilmesi zorunlu kılınmıştır. 15 gün önceden kullanıcılar bilgisayarlarına giriş yaparken, gerekli ikaz, sistem tarafından otomatik olarak ekranlarında görünmektedir.

- Kullanıcı ilk verilen geçici şifreyle sisteme giriş yaptığında, yeni bir şifre belirlemesi sistem tarafından otomatik olarak istenmektedir.

- Sistemin ilk girişte belirlemesini istediği yeni şifrenin tanımlanmasını, uygunluğu ve korunması ilgili personelin sorumluluğundadır. Şifreler hatırlanmak maksadı ile herhangi bir kağıt ortamına yazılmaz.

- Şifrelerin unutulması durumunda, kullanıcı şifresi yenilenmesi için personel ilgili Sistem Yöneticisine bizzat başvurmalıdır. Daha sonra değiştirilmek üzere kullanıcı için yeni bir geçici şifre oluşturulur.

- Sistem sunucularında ve ağ cihazlarında kullanıcı tanımı yapılırken, şifreler boş bırakılmamalıdır. Şifrelerin karakter boyutu ve karşılığı konusundaki kısaltmalar, ilgili işletim sisteminin özellikleri ile sınırlıdır.

UZAKTAN ÇALIŞMA VE ERİŞİM

- Uzaktan çalışma, 4857 sayılı İş Kanununun 14'üncü maddesine göre; "çalışanların, işveren tarafından oluşturulan iş organizasyonu kapsamında, iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iş ilişkisi" olarak tanımlanmaktadır.
- Uzaktan çalışma; Üniversitemiz çalışanları ile yükleniciler, tedarikçiler, iş ortakları çalışanları gibi Üniversitemiz ile geçici olarak iş ilişkisi olan kişiler tarafından Bilgi Sistemleri Uzaktan Bağlantı Erişim Talep Formu doldurularak yapılabilir.
- Uzaktan çalışma işlemi, yapısı itibarı ile güvensiz olarak kabul edilir ve bilgi güvenliğini sağlamak için yetkili giriş parola vb. ek önlemler alınması gerekir.
- Uzaktan çalışma ile ilgili kontrol tedbirleri belirlenirken aşağıda sıralanan dört temel tehdit unsuru/modeli dikkate alınır.

- Uzak çalışma ortamlarının fiziki güvenliğindeki yetersizlikler,
- Uzak bağlantının güvenli olmayan ağ ortamları (çoğunlukla internet) üzerinden yapılması,Kurum güvenlik politikaları uygulanmamış güvenilir olmayan cihazların iç ağa bağlanması.

İÇ AĞDAKİ KAYNAKLARA DIŞARIDAN ERİŞİM

- Farklı yöntemler kullanılarak uzak bağlantı yapılması mümkündür. Uzaktan erişim için ihtiyacın kendine özgü şartları ve riskleri değerlendirilerek en uygun yöntem belirlenir.
- Uzaktan erişim yöntemi olarak tünelleme, uzak masaüstü erişim veya doğrudan uygulama erişimi yöntemlerinin biri veya birkaçı birlikte kullanılabilir.

- Tünelleme yöntemi, uzaktan çalışmada kullanılan bilgisayar ile iç ağın kriptolojik yöntemler kullanılmak suretiyle oluşturulan güvenli bir tünel vasıtasıyla birbirine bağlanmasıdır. Tünelleme işlemi, ağırlıklı olarak sanal özel ağ (VPN: Virtual Private Network) teknolojileri vasıtasıyla yapılır. VPN işlemi IP güvenliği (IPsec: IP Security), taşıma katmanı güvenliği (TLS: Transport Layer Security) veya güvenli kabuk (SSH: Secure Shell) protokolleri kullanılmak suretiyle yapılabilir.

- Uzak masaüstü erişim çözümleri, uzaktan çalışan kullanıcıların kurumun iç ağında yer alan bir sunucu veya istemci bilgisayarın karşısındaymış gibi kullanılmasını sağlar. Bu yöntemde, uzak kullanıcılar bağlanılan bilgisayarın klavye ve fare kontrollerini uzaktan yapar hale gelirler.

- Uzaktan erişim ile ilgili yöntem belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir:

- Üniversitemizde genel bir politika olarak uzak masaüstü işlemleri VPN bağlantısı üzerinden yapılır. VPN bağlantısı yapılmadan doğrudan uzak masaüstü bağlantısı yapılmasına hiçbir şekilde izin verilmez.

- Özel nitelikli verilerin işlendiği, muhafaza edildiği elektronik ortamlara uzaktan erişim yapılırken, en az iki kademeli kimlik doğrulama sistemi kullanılması yasal bir zorunluluktur. Diğer sistemler için de çok faktörlü kimlik doğrulama yapılması tercih edilir.

- VPN işlemi üniversite Network grubuna ait güvenlik duvarı üzerinden yapılır.
- Erişim kontrollerinin uygulanabilmesi maksadıyla, hedef bilgisayarlara sabit IP adresi verilir. Yapılacak erişim; erişim yapacak kişi, hedef bilgisayar IP adresi ve kullanılacak port/uygulama bazında sınırlandırılır. VPN bağlantılarına ilişkin iz kayıtları tutulur ve söz konusu iz kayıtları en az iki yıl süre ile saklanır.
- Uzak bağlantı yapılacak uygulamalara/kaynaklara erişimin daha kontrollü olarak yapılması gerekiyorsa, bağlantılar bu amaçla ayrılan bir terminal/vekil sunucu üzerinden de yapılabilir.
- Uzak bağlantı yapacak istemci bilgisayarların IP adresleri/blokları biliniyorsa, hedef bilgisayara sadece belirtilen IP adreslerinden erişim yapılması için gerekli ayarlar yapılır.
- Uzak erişim için yapılan bağlantıda boşta kalma süresi (herhangi bir işlem yapılmadığı takdirde connection time out süresi) 10 dakikadır.
- Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;
- Bağlantı VPN üzerinden yapılır.
- Bağlantı yapan kişinin, hedef bilgisayarda oturum açma iznine sahip bir kullanıcı olması gerekir.
- Hedef bilgisayara kullanıcı adı ve parola girilerek oturum açılır. Anonim girişlere izin verilmez.
- Hedef bilgisayarda uzak bağlantı için kullanılan servis/arayüz vasıtasıyla, bilgisayara erişecek kullanıcılar "kullanıcı adı ve/veya IP adresi" bazında sınırlandırılır. Bu yöntemle sadece yetki verilen kullanıcıların/bilgisayarların uzaktan erişim yapması sağlanır.
- Bağlantı yapan kullanıcının hedef bilgisayardaki oturum açma, oturum kapatma gibi kullanıcı hareketleri kayıt altına alınır ve söz konusu iz kayıtları en az 2 ay süre ile saklanır.
- Hedef bilgisayar üzerinden bir başka sunucuya bağlantı yapılacak ise ilgili kullanıcının söz konusu sunucuda yaptığı işlemlere ait iz kayıtları da kayıt altına alınır.
- Uzak bağlantı yazılımı olarak mümkün ise "Microsoft Uzak Bağlantı Programı" kullanılır.

AĞ İLETİŞİM GÜVENLİĞİ

- Yeni teknolojileri, uygulamaları tehdit veya açıklıkları takip etmek için dernek, forum siteleri, e-Posta grupları gibi özel ilgi grupları belirlenir ve bilgi işlem personeli tarafından takip edilir.
- Güvenlik cihazları ve ağ yönetiminde ayrıcalıklı erişim hakkı verilen kullanıcıların sisteme erişimi onay mekanizmasından geçerek tamamlanır. Erişim talepleri, resmi yazı veya kurumsal e-Posta ile bildirilir. Ayrıcalıklı erişim hakkı elde eden personelin yer ve görev değişikliği olması durumunda erişimleri düzenleyen birime bilgi verilmesi sağlanır.
- Güvenlik ve ağ cihazlarında yönetici olarak erişim yetkisine sahip olan kullanıcı hesaplarındaki değişiklikler kontrol edilir. Sistemler üzerinde ortak erişim yetkisi olan hesaplar açılmaz.
- Sahibi bilinmeyen hesaplar kaldırılır.
- Güvenlik ve ağ cihazlarına yapılacak uzaktan erişim yetkisi verilen kullanıcılara bağlantı zamanı ve süresi ile ilgili kısıtlamalar getirilir. Kurumdaki görevi gereği kullanıcıların bağlantı süreleri farklı olabilir.
- Güvenlik duvarları, ana omurga cihazları gibi kritik sistemlere yapılacak erişimler için yerel kullanıcılar yerine ikincil bir kimlik doğrulamasının kullanılması tavsiye edilir.

- Güvenlik ve ağ cihazlarının gösterildiği "ağ mimarisi krokisi" hazırlanır. Hazırlanan kroki, sadece ilgili personelin görebileceği bir şekilde saklanır. Güvenlik ve ağ mimarisinde değişiklik yapıldığı zaman kroki de güncellenir.
- Güvenlik ve ağ cihazlarının kurulumunu, yapılandırmasını ve sistemde karşılaşılan hataları gidermek için izlenilen yöntemleri anlatan kılavuz dokümanları hazırlanır. Bu kılavuzlardan bilgi havuzu oluşturulur.
- Yedekleme politikası uyarınca güvenlik ve ağ cihazlarının konfigürasyon yedekleri düzenli aralıklarla alınır. Yedekler 2 (iki) farklı lokasyonda saklanır.
- Sistemi etkileyecek bir çalışma yapılması gerekiyorsa mesai saati dışında yapılır. Bu çalışmadan etkilenecek kurum/firma ya da kişilere bilgi verilir.
- Kablosuz ağlara giriş yapan tüm kullanıcılar 'eduroam' sistemine kaydedilir ve bu bilgiler belirlenen süreler boyunca saklanır.
- Telnet gibi güvensiz bağlantılara izin verilmez. SSH protokolünü kullanan bağlantılarda SSH Ver2 kullanılır.
- İhtiyaç olmayan tüm portlar kapatılır. Dışarıdan tarama yapıldığında portların durumunun açık olarak görülmemesi için gerekli tedbirler alınır. Kurum web sayfaları, laboratuvar sonuç sorgulama sayfası gibi uygulamalarca kullanılan 80 ve 443 dışındaki portlar kullanıma kapatılır.
- Güvenlik duvarı ve ağ cihazları için kontrol listeleri (ACL, güvenlik ürünleri erişim kısıtlaması vb.) tanımlanır.(Üniversitemiz network güvenlik duvarı tarafında kontrolü sağlanır.)
- Güvenlik ve ağ cihazlarının fiziksel güvenliğini sağlamak için gerekli tedbirler alınır.
- Güvenlik ve ağ cihazlarının yazılım güvenliğini sağlamaya yönelik tedbirler alınır. Cihazlar ilk kurulduğunda varsayılan olarak atanmış olan kullanıcı adı ve parolalar değiştirilir. Parolalar güçlü parola ilkeleri esaslarına göre oluşturur.
- Güvenlik ve ağ cihazları üzerindeki gereksiz ve kullanılmayan tüm servisler kaldırılır.
- Cihazlara, saldırılara karşı korumak için 5 (beş) yanlış deneme sonrasında oturum belirli bir süre kilitlenecek şekilde ayarlama yapılır.
- Doğru yapılandırılmış zaman damgası için cihazlar NTP sunucu ile senkronize olarak çalıştırılır.
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Kanunu uyarınca tutulması gereken trafik bilgileri (iz kayıtları) kayıt altına alınır.

- Saldırganların yerel ağda kendilerini ağ geçidi olarak tanımlayarak trafiği kendi üzerinden geçirerek bilgilere erişim sağlamasını önlemek için ağda kullanılan anahtarlarda "DHCP snooping" ve "arp inspection" özelliği aktif edilir.
- Dış ağdan sunucular üzerindeki servislere, sunucu yönetim protokolleri (RDP, SSH) ile erişim engellenir.
- Sunucular, sadece belirli portlardan erişim sağlanacak şekilde yapılandırılır.
- Kurum bünyesinde barındırılan ve hizmet veren uygulamalara HTTPS üzerinden bağlanılır.
- Güncel atak metotlarından korunmak için saldırı tespit ve önleme sistemleri, ağ hizmetlerine erişim

ilkelerinin belirlenmesi için Üniversitemiz güvenlik politikası gereği Güvenlik Duvarı kullanılır.

- Kurumsal kaynakların etkin olarak kullanılması, 5651 sayılı kanundan kaynaklanan uyum zorunlulukları, veri güvenliğinin sağlanması, zararlı içerik ve yazılımlardan korunma vb. maksatlarla internet erişimi kısıtlamaları yapılabilir.

Kısıtlama ile ilgili politikalar belirlenirken aşağıdaki hususlar dikkate alınır:

- Virüs, Spyware, Malware, Trojen, Spam, Solucan, Hacking (korsan), Fishing (oltalama) saldırıları içerdiği tespit edilen güvenlik seviyesi düşük internet sitelerine erişimler kapatılır.
- Alkol, sigara, uyuşturucu, silah vb. sağlığa zararlı ürünlerin reklam ve satış sitelerinin erişimleri engellenir.
- Erotik içerikli siteler, çocuk istismarı, bahis ve kumar siteleri, oyun siteleri erişime kapatılır.
- Kurumun internet bant genişliğini olumsuz etkileyen uygulama ve sitelerin (Torrent, P2P, Streaming Media, Download vb.) erişimleri engellenir.
- Basın yayın organlarını takip ederek idareye raporlamakla sorumlu personel haricindeki tüm personelin dizi, film ve televizyon erişimleri kapatılır.
- Kuruma ait sosyal medya hesaplarını yönetmekle sorumlu personel dışındaki tüm personelin Facebook, Twitter, Instagram vb. uygulamalara erişimleri engellenir veya bant genişliği sınırlaması yapılır. Youtube, Vimeo, Dailymotion gibi platformlarda erişimlerle ilgili olarak sadece ihtiyaç duyan personele izin verilir veya bu platformlara erişimlere bant genişliği sınırlaması yapılır.

ANTİVİRÜS YÖNETİMİ

- Tüm bilgisayarlar lisanslı antivirüs yazılımı ile korunur. Antivirüs yazılımının virüs veritabanı güncel tutulur.
- Antivirüs veritabanı güncelleme işlemi antivirüs sunucusu üzerinden haftanın yedi günü yapılır.
- Antivirüs yazılımının antivirüs sunucusu üzerinden yönetilmektedir.
- Sunucu üzerinden periyodik güncellemeler, virüs taraması, zayıf noktalar (farklı programların açıkları) antivirüs yazılımının sürümü, durum bilgisi ve birçok yararlı bilgi sunucu üzerinden raporlanır.
- Antivirüs yazılımının yönetilmesi ve doğru politikayla çalışmasını bağlı olduğu antivirüs sunucusu uygular. Bunun için yönetilen bilgisayara antivirüs yazılımı haricinde agent (ajan) yazılımının da yüklenmesi gerekmektedir.
- Güncelleme sırasında kapalı olan bilgisayarlar sunucu üzerinde listelenir ve açıldığı anda güncelleme gönderilip doğrulanır.
- Antivirüs sunucusunu yöneten personel ağda yönetilen tüm bilgisayarların antivirüs yazılımının ne durumda olduğunu görür ve ona göre müdahalelerde bulunur.
- Antivirüs Sunucusu üzerinde sunucular, bilgisayarlar ve diğer cihazlar için gruplar oluşturulur ve her bir gruba ayrı politika uygulanır. Örnek olarak sunucularda port ve internet kısıtlaması çok daha genişken bilgisayarlar gurubundakiler daha sıkıdır.

- Antivirüs yazılımları herhangi bir ağ saldırısı durumunda sunucuya bu durumu raporlar ve kaynağını 60 saniye boyunca keser. Kaynağın hangi ip ve port üzerinden geldiği sunucu üzerinden izlenir ve müdahalede bulunur.
- Antivirüs yazılımları sunucu üzerinden yönetiliyorsa lisans anahtarları sunucu üzerinden tüm bilgisayarlara gönderilir.
- Antivirüs yazılımları bazı durumlarda otomasyon (HBYS, pacs, tıbbi cihaz yazılımları vs) yoğun ağ trafiğini saldırı olarak görüp engelleyebilir. Bu durum antivirüs yazılımına sunucu üzerinden ilgili yazılımın güvenli olduğunu gösteren "güvenilir uygulama" olarak tanımlamak gerekir.
- Antivirüs yazılımları her zaman güncel ve sunucuyla haberleşebilir durumda olmalıdır.
- Yüklü olan antivirüs programı devre dışı bırakılmamalıdır, sistemden kaldırılmamalıdır.

İZ KAYITLARI (LOG) YÖNETİMİ

- Kurum bünyesindeki kullanıcı faaliyetleri, bilişim sistemlerine yönelik saldırı ya da hatalar, saldırının tespit edildiği anda saldırıya ait detayları gösteren iz kayıtları oluşturulur ve belirli kurallar dâhilinde toplanır.
- İz kayıtlarının tutulması ve yönetilmesi (iz kayıtlarının üretilmesi, aktarılması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi gibi süreçler) sadece erişim yetkisi verilen bir birim/kişiler tarafından yapılır.
- Farklı sistemler tarafından üretilen iz kayıtları; güvenlik denetimi sağlamak, iz kayıtlarını daha etkin ve verimli olarak saklamak, yedeklemek ve raporlayabilmek amacıyla merkezi bir sunucuda toplanır.
- İz kaydı (log) alınması gereken fiziksel ortam kayıtları; kritik bilişim sistemleri odaları giriş-çıkış kayıtları ve kamera kayıtları, çalışma ortamları giriş-çıkış kayıtları ve kamera kayıtlarından oluşur. Kamera kayıtları 2 (iki) ay, kritik sistem odaları ve çalışma ortamları giriş-çıkış kayıtları 2 (iki) yıl süreyle tutulur.
- İz kayıtlarının saklanma süresi belirlenirken; yasal zorunluluklar, iz kayıtlarından sağlanacak fayda, saklama maliyeti ve ilgili iz kaydının kritikliği göz önünde bulundurulur. Başka bir yasal zorunluluk yoksa elektronik olarak üretilen tüm iz kayıtları en az 2 (iki) yıl süre ile saklanacak şekilde önlem alınır.
- Kritik olaylara ilişkin iz kayıtlarının merkezi sunucuya eş zamanlı olarak (olay oluştuğu zaman) gönderilmesi sağlanır.
- Kritik sistemlerde oluşan iz kayıtları eş zamanlı olarak merkezi iz kayıtları sunucusuna aktarılır. Merkezi sunucuya aktarılan kayıtların silinmesi ve değiştirilmesinin engellenmesi için gerekli teknik ve idari tedbirler alınır.
- Kayıt üreten ortamların teknolojisine uygun olarak kimlik doğrulama ve yetkilendirme sistemleri hayata geçirilir.
- Teknik olarak mümkün olması durumunda, iz kayıtları gizlilik ve hassasiyet seviyelerine göre sınıflandırılarak, ilgili kullanıcıların sadece verilen yetkiler çerçevesinde iz kayıtlarına bakmaları sağlanır.
- Bütün sistemlerin zamanlarının aynı olması için Ağ Zaman Protokolü (NTP-Network Time Protocol) sunucusu kurularak kayıt üreten farklı sistemlerin zamanları bu sunucu ile senkronize edilir.
- İz kayıtları periyodik olarak yedeklenir ve yedeklerin uygun şekilde muhafaza edilmesi sağlanır.
- Merkezi iz kaydı sunucusu sadece yeni iz kayıtlarının saklanması için fonksiyonlar içerir. Bu sunucuda iz kayıtlarının silinmesi/değiştirilmesi amaçlı erişimlere izin verilmez.

İz kayıtları tutulan belli başlı sistemler:

- Çalışma ortamları ve sistem/sunucu odalarına yapılan giriş-çıkışlara (kartlı geçiş sistemi, parmak izi okuyucuları vb. sistemler tarafından üretilen iz kayıtları),
- Sanal ortam kayıtları,
- Bilişim sistemleri tarafından üretilen kayıtlar, SBYS'ler,
- Güvenlik duvarları iz kayıtları,
- Antivirüs yazılımları,
- Saldırı tespit/önleme sistemleri,
- Yönlendiriciler ve anahtarlama cihazları,
- Sunucular,
- Diğer iş uygulamaları (kritik kurumsal projeler),
- Veri tabanları,
- VPN iz kayıtları

Tutulması gereken asgari iz kayıtları;

- Kaydı oluşturan sistem,
- Kaydın oluşturulma zamanı (tarih, saat, zaman dilimi),
- Kaydı oluşturan olay,
- Kaydın ilişkili olduğu kişi (IP/Port bilgisi, MAC adresi, işlemi yapan tekil kullanıcı adı veya sistemin adı).

SUNUCU VE SİSTEM ODASI GÜVENLİĞİ

Sunucu ve sistem odasının işleyişi **Sunucu Odalarının Güvenliği ve Kullanma Talimatı'**na göre yapılmaktadır.

- Hizmet sunumunun sürekliliğinin sağlanması için kesintisiz ve sürekli çalışan elektronik ve donanımsal altyapı ihtiyacı bulunmaktadır. Donanım, elektronik altyapı ya da çevresel faktörlerden kaynaklanabilecek sorunlar hizmetlerin sunumuna birçok açıdan zarar verebilir ve olumsuz etkilerin giderilmesi gerek maliyet gerek zaman açısından çok zor olabilir. Bu nedenle, hizmet sunumunda yer alan tüm aktif ve pasif donanımın; sadece sunuculara tahsis edilmiş, yetkisiz personelin girişinin engellendiği, sıcaklık ve nemin kontrol edildiği, elektrik kaynağının stabilize edildiği, özel şekilde iklimlendirilmiş ve güvenliği sağlanmış sunucu/sistem odasında konumlandırılması gerekir. Sistem odalarındaki donanımların hizmet sürekliliğinin sağlanması için yedekli bir güç kaynağı sistemi, yedekli haberleşme bağlantıları, sıcaklık, nem gibi çevre değişkenlerinin kontrolü için iklimlendirme cihazları ve güvenlik cihazları yer alır.
    - Sunucuya ait güncel bilgiler bgys.ege.edu.tr adresinde kayıt altına alınmıştır
    - Bir sistem odasının en temel özellikleri;
        - 7×24 kesintisiz çalışabilirlik,
        - Güç yönetimi ve ağ bağlantılarında farklı kanallardan yedeklilik,
        - Ağ güvenliği, fiziksel erişimlerde yetkilendirme ve görüntülü gözetleme,

- Çevre şartlarının kontrol altında tutulması,
- Yangına karşı duman algılama gibi erken uyarı sistemleridir.

- Sistem odasının kesintisiz çalışmasına; sıcaklığın normal aralığın dışına çıkması, yangın, su baskını, deprem, yetkisiz kişilerin sistem odasına girmesi, odadaki herhangi bir cihazın arızalanması engel olabilir. Tüm bu olumsuz durumların yaşanmasının önlenmesi ve hizmetlerin sağlıklı çalışabilmesi için standartlara uygun bir sistem odası oluşturulması ve ana bilgisayar, sunucu ve diğer hizmet sürecindeki bileşenlerin güvenli olarak bu alanlarda konumlandırılması gerekir.

Sistem odası ile ilgili aşağıdaki ölçütlere dikkat edilmesi gerekir;

Sistem Odasının Yeri: Çevresel faktörlerden en az etkilenecek bir yer tercih edilmelidir. Binanın nem ve sıcaklık oluşturabilecek kalorifer ve su tesisatlarından uzak, eğer mümkünse orta katlarda ya da 2. katında konumlandırılmalıdır. Sistem odasının yeri iklimlendirme açısından da değerlendirilerek, sistem odasından bina çıkışındaki klimanın dış ünitesine giden borunun mesafesi düşünülerek seçilmelidir. Mümkün olduğunca sistem odasında cam pencere ve duvarlar olmamalıdır.

Sistem odasının bulunduğu binada yıldırımlara karşı paratoner kurulmalı ve kablolaması sistem odasından uzakta olmalıdır. Manyetik alan oluşturabilecek enerji ve elektrik hatlarından izole olmalı, telefon santrali ve benzeri dış unsurlar kesinlikle sistem odasına alınmamalıdır, kullanılması gerekiyorsa kafes yapmak gibi ek güvenlik önlemi alınmalıdır.

Sistem Odasının İnşaat Özellikleri: Kesintisiz güç kaynakları ve elektrik dağıtım panoları; aktif cihazlar ve sunucuların yerleştirildiği alandan ayrı bir bölüm olarak tasarlanabilir. Odanın dış duvarları, mümkünse yangına ve sızdırmazlığa karşı gaz beton tuğla veya iki tarafı alçı ile kaplanmış -50º ile +650º arasındaki sıcaklıklara dayanıklı bir malzeme olan taş yünü ile örülmelidir. İç duvarlar pasif yangın koruması sağlayacak epoksi boya ile kaplanmalıdır. Sistem odalarındaki kablo yoğunluğu ve diğer iletim hatları yükseltilmiş taban, asma tavan ve/veya asma kablo tavalarının içinden geçirilerek sistem odası içerisinde oluşabilecek karmaşa önlenmelidir.

Giriş - Çıkış Kontrolü: Sistem odasına giriş ve çıkışlar kart okuyucu, avuç içi damar okuyucu veya şifreli giriş ile kontrol altına alınmalı ve giriş/çıkışlara ait iz kayıtları tutulmalıdır. IP kamera ile izleme sistemi kurulmalı, odanın durumu, giriş çıkışları ve yapılan işlemler kameralarla kayıt altına alınmalıdır.

Sıcaklık Kontrolü: Birçok işlemci için üreticisi tarafından belirtilen en yüksek sıcaklık derecesi ortalama 70 °C'dir. Bu ısıya ulaşan sunucular, üzerlerindeki sensörler aracılığıyla kendilerini kapatırlar. Hizmet sürekliliği için ortam sıcaklığının 18 °C ile 22 °C arası olması kabul edilir. Sistem odasına e-Posta, SMS ya da telefon çağrısı aracılığıyla bilgilendirme yapan sıcaklık sensörleri konumlandırılmalıdır.

Yangın Kontrolü: Sistem odasının dışında çıkabilecek yangınlara karşı, odanın dış kısımları su püskürtmeli yangın sistemi ile koruma altına alınmalıdır. Sistem odasının kapısı yangına dayanıklı, ısıyı ve dumanı diğer tarafa geçirmeyen, standartlara uygun özel üretim bir kapı olmalıdır. Duman algılama detektörü ile yangın söndürme sistemi konumlandırılmalıdır. Elektrik yangınlarına müdahalede, bilgisayar kabinlerinin zarar görmesini engellemek için karbondioksitli veya halon gazlı (FM200 vb.) ve basınç kontrollü yangın söndürme sistemi kullanılmalıdır. Herhangi bir yangın tehlikesi durumunda sistem odasının elektriği kesilerek yangına müdahale edilmelidir.

Su Baskını Kontrolü: Su basmasına karşı kabinler yerden 15-20 cm yükseltilmiş olmalı ve su dedektörü konumlandırılmalıdır.

Enerji Kontrolü: Enerjinin sürekliliği ve yedekliliği, iletimi, izlenmesi ve topraklama hassasiyetle üzerinde durulması gereken konulardır. Sistem odasındaki cihazların çektiği enerjinin kapasitesine uygun olarak ve büyüme kapasitesi de göz önüne alınarak, elektrik kesintisi ya da şebekedeki dalgalanmaları önleyecek regülatörlü bir UPS ve sistemlerin kritiklik durumuna göre jeneratör kurulumu yapılmalıdır.

Enerjinin iletimi için doğru kablo tipi ve kalınlığı seçilmeli, enerji kabloları kablo kanalı ile korunmalıdır. Kablo ısınması ya da sigorta atması ve benzeri sonuçların engellenmesi için tüm cihazların kullandığı enerji miktarı sayısal değer olarak izlenmelidir. Sistem odası kuruluş aşamasında topraklama yapılmalıdır.

Deprem Kontrolü: Kabinler yere veya duvara sabitlenmeli, kabinler arası yerleşim deprem ve havalandırma şartlarına uygun tasarlanmış olmalı, deprem yönetmeliği şartları sağlanmalıdır.

Kablolama Kontrolü: Data ve elektrik kablolama için TSE standartlarına uygun malzemeden imal edilmiş kablo kanalları kullanılmalıdır. Tüm kanallar bölmeli olmalıdır. Kuvvetli akım ve zayıf akım kabloları ayrı ayrı bölmelerden geçirilmelidir. Kablolar kablo kanalı ile (haşereler de düşünülerek) korunmalıdır. Kabin içi kablolarda kablo toplayıcı aparatlar kullanılması ve ağ kablolarının etiketlenmesi gerektiğinde kolay müdahale için zaman kazandıracaktır.

Kabin Düzeni: Kabinlere cihazlar yerleştirilirken yerel ağ ve DMZ bölgesine hizmet eden sunucuları ve anahtarlama cihazlarını (switchleri) ayrı konumlandırmak, veri depolama, yedekleme, ağ bağlantısı ve güvenlik cihazlarını kolay erişilebilir bir kabine yerleştirmek planlı büyüme için kolaylık sağlayacaktır.

İzleme: Cihazların hata ya da alarmlarını manuel olarak kontrol etmek yerine Basit Ağ Yönetim Protokolü (SNMP) destekli cihazları bir izleme yazılımı üzerinden kontrol etmek için arıza durumunda e-Posta ve/veya SMS yoluyla bilgilendirme yapacak bir sistem oluşturulmalıdır. Bu iş için mevcut sunucuların üreticisinin izleme için özel ürünlerini kullanmak bir yöntem olabilir ya da bakım anlaşması ve garanti kapsamındaki cihazlar için donanım arızası durumunda otomatik çağrı açılması ve arızalı parçanın değişim sürecinin otomatik olarak başlatılması sağlanabilir.

YEDEKLEME YÖNETİMİ

Kurum Yedekleme Politikası

- Verilerin yedeklenmesi iş sürekliliğinin en temel prensipleri arasında yer alır. Donanım arızaları, yazılım hataları, kullanıcıdan kaynaklanan sorunlar ya da doğal tehditler gibi nedenlerle veri kayıpları yaşanabilir. Başarılı bir yedekleme işlemi ve yedeklenen verinin ihtiyaç anında veri kaybı olmadan kurtarılabilmesi veri yedekleme sistemlerinin en temel iki bileşenidir.
- Yedeklerin kurumun gereksinimleri dikkate alınarak hazırlanmış olması, yönetimin konuya bakış açısını yansıtan bir yedekleme politikası doğrultusunda alınıp güvenliğinin sağlanması, saklanması ve belirli sıklıkta geri dönüş testlerinin yapılması veri kaybı riskini minimum seviyeye indirecektir. Yedekleme sisteminin kurulumu; yedeklenecek veri miktarı, yedekleme sıklığı, yedeklenen verinin zaman içerisinde değişme oranı, kabul edilebilir maksimum veri kaybı gibi parametrelere bağlıdır.
- Her kurumun kendine özgü yasal veya sözleşmeden doğan gereksinimleri ile verinin saklanma ve korunma gerekliliklerini karşılayacak şekilde bir politika oluşturması gerekir.
- Yedekleme politikası; olası bir felaket durumu ya da sistem hatası sonrası gerekli tüm verilerin geri getirilebilmesini sağlayacak şekilde yedekleme kuralları tanımlanmış, etkin, yönetilebilir ve izlenebilir bir yedekleme sistemi kurulması ve işletilmesine imkân verecek şekilde hazırlanmalıdır.
- Yedekleme politikasının yerine getirilmesi için bir yedekleme planı ortaya koyulmalıdır. Yedekleme planı; Yedekleme sıklığı, hangi saklama ortamında ne kadar süre tutulacağı, hangi yedekleme türü ile yedekleneceği, kabul edilebilir geri dönüş süresi ve kabul edilebilir veri kaybı süresi bilgilerini içermelidir.

Yedekleme Planlarının Oluşturulması

- Kurumun sistem gereklilikleri göz önüne alınarak; Sunucular, Sanal Sunucular, Veri Tabanları, Etki Alanı Denetleyicisi, Güvenlik ve Ağ Cihazları gibi veri içeren platformların yedeklenmesi planlanmalıdır.
- Yedeklenecek veriler bilgi işleme süreci içerisinde değişiklik gösterebileceğinden yedekleme listesi oluşturularak en az yılda 2 (iki) kez gözden geçirilmeli ve güncellenmelidir.
- Başarılı bir yedekleme sistemi için kategorize edilmiş ve önceliklendirilmiş verilerin yedekleme planları oluşturulur.

- Yedekleme planları asgari olarak; yedeklenecek bileşenin adı (host name), ulaşım yolu (ip adresi), yedekleme tipi ve sıklığı, yedek geri dönüş testi raporları gibi bilgileri içerir.
- Yedekleme planına göre yedeklerin düzenli aralıklarla alınması ve sürekli olarak gözden geçirilmesi gerekir.

Yedekleme Çalışmaları

- Kritik veriler yedeklenirken iki farklı şekilde yedeklenmek üzere bir yedekleme sistemi oluşturulmalıdır. Bunlardan ilki; canlı çalışma ortamında eş zamanlı olarak kümelenmiş disk sisteminin farklı disk bölümlerine; ikincisi ise, çevrimdışı olarak varsa yedekleme sunucusu yoksa şifrelenmiş olarak harici depolama ortamlarında yedeklenmesidir.
- Kritik olmayan veriler yedeklenirken, verilerin bir kopyası mevcut sunucular üzerinde, diğer bir kopyası çevrimdışı olarak yedekleme sunucusu veya harici depolama ortamlarında tutulur.
- Yedekleme politikası ve planları doğrultusunda yapılan yedekleme işlemleri düzenli olarak kontrol edilmelidir.
- Özel nitelikli kişisel veri kategorisinde bulunan sağlık kayıtlarının yer aldığı yedekleme ortamları şifrelenir.
- Yedekleme medyalarının acil durumlarda kullanılması gerekebileceğinden güvenilir ürünlerden seçilmeli ve düzenli periyotlarda test edilmelidir.
- Yedekleme medyalarının bulundurulduğu ortamların fiziksel uygunluğu ve güvenliği sağlanmalı ve herhangi bir felaket anında etkilenmeyecek şekilde bilgi işlem odalarından farklı odalarda veya binalarda saklanmalıdır.
- Yedekleme işlemi, günde 2 defa yapılır (yedekleme işlemi için sistemin yoğun olmadığı zamanlar seçilir).Yedekleme; tam yedeğin dışa aktarılması, anlık veri tabanı log dosyalarının 10 gün süre ile saklanması ve anlık veri tabanı replikasyonu (uzak lokasyona) şeklinde yapılmaktadır.
- Yedekleme dosyaları HBYS'nin çalıştığı sunucu haricindeki bir ortama alınır.
- Yedekleme; harici bellek, taşınabilir kayıt ortamları veya ağ üzerinde çalışan yedek sunucu gibi bir ortamda saklanır.
- Alınan yedekleme ortamı, fiziksel olarak HBYS'nin üzerinde çalıştığı alanlardan farklı bir alanda/ farklı birimde saklanır.
- Veriler offline ortamlarda süresiz olarak dekan/dekan yrd/başhekim tarafından saklanır.
- Yedeklemeler aracılığı ile yılda bir kez veri kurtarma testi uygulanır.
- Yedeklemeden geri dönüşüm sağlanıp sağlanmadığı ve veri kaybının olup olmadığı kontrol edilir.
- Test tutanakla kayıt altına alınır.
- Gerektiğinde iyileştirme çalışmaları başlatılır.

Geri Dönüş Testler

- Yedeklenen verilerin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için yılda en az 1 (bir) kez geri dönüş testlerinin yapılması gerekir.
- Yedekten geri yükleme testlerinin, başarısız olması nedeniyle veri kaybı olabileceği durumu göz önüne alınarak, canlı ortamda değil gerçek ortamın aynısı olan test ortamında yapılması gerekmektedir.

TAŞINABİLİR ORTAM YÖNETİMİ VE ORTAMIN YOK EDİLMESİ

Taşınabilir Ortam Yönetimi

- Kaybolma, kolayca çoğaltma vb. nedenlerden dolayı özellikle elektronik medya (CD/DVD, USB girişli hafif taşınabilir bellekler, taşınabilir diskler, hafıza kartları, teyp kartuşları vb.) ve basılı evraklar (yazılar, dosya klasörleri, etüdler, çizimler, krokiler, proje evrakları vb.) olmak üzere taşınabilir ortamlarda saklanan her türlü bilginin korunması ve yetkisiz kişilerin eline geçmemesi için özel önlemler alınır.
- Elektronik medya kullanımı ile ilgili olarak aşağıdaki hususlar göz önünde bulundurulur.
- Kuruma ait veriler, kişilere ait medyalar üzerinde saklanamaz. Verilerin bir taşınabilir ortama aktarılması ihtiyacı kaçınılmaz ise bu maksatla kuruma ait medyalar kullanılır.
- Görev devir teslimlerinde veya işten ayrılışlarda, kişilere teslim edilmiş olan medyaların iade edilmesi istenir veya ne şekilde sarf edildiği bilgisi sorgulanır.
- ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL veriler, taşınabilir ortamda saklanamaz. Özellikle bu tür ortamlarda saklama zorunluluğu var ise şifreli olarak saklanır.
- Bir bilgi sadece taşınabilir medya ortamında saklanıyorsa, bozulma/kaybolma gibi ihtimallere karşı bir başka medya ortamında da yedeklenmesi tavsiye edilir. Veriler çok kıymetli ise yedeklenen medya ortamı, doğal afet vb. tehditlere karşı önlem olmak üzere fiziksel olarak farklı bir yerde muhafaza edilir.
- Yeni medya teknolojilerinin ortaya çıkması nedeniyle üç yıldan uzun süredir eski teknolojilerin kullanıldığı bir medya ortamında saklanan verilerin daha yeni bir medya ortamına taşınması tavsiye edilir.
- Gizlilik derecesi taşıyan kurumsal verilerin saklandığı medya ortamları, kişisel (şahsın kendisine ait) bilgisayarlarda kullanılamaz. Bu tip veriler kişisel bilgisayarlarda işlenemez.
- Tüm ortamlar üretici talimatında belirtildiği şekilde toz, nem vb. çevresel şartlardan etkilenmeyecek şekilde güvenli bir ortamda saklanır.
- Elektronik medya da dâhil tüm taşınabilir ortamlar, kullanılmadığı zamanlarda içinde bulunan verilerin gizlilik derecesi dikkate alınarak fiziki güvenlik tedbirleri alınmış kasa, dolap, çekmece gibi ortamlarda saklanır.

Ortamın Yok Edilmesi

- Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik veya fiziki nedenlerle kullanılmasında yarar görülmeyerek hizmet dışı bırakılmasına karar verilen ve kayıt silme işlemleri tamamlanan bilgi sistem cihazlarına ait veri depolama üniteleri, içerisinde gizlilik dereceli bilgi bulundurma ihtimali nedeniyle usulüne uygun olarak imha edilir veya güvenli silme işlemi yapılır.
- Sökülen sabit disklerden daha önce ilgili teknik birimler tarafından "onarımı mümkün değil" şeklinde rapor verilenler ile sağlam olmakla birlikte "yeniden kullanımı düşünülmeyen" cihazlar fiziksel yok etme yöntemi ile imha edilir.
- Fiziksel yok etme; optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.
- Disk imha işlemleri, bizzat disklerin sahipleri veya taşınır mal sorumlularının nezaretinde yapılır. Kâğıt ve mikro fiş ortamlarındaki veriler, kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünerek imha edilir.
- Yeniden kullanılması planlanan disklere, içlerinde yer alan bilgilerin yetkisiz kişilerin eline geçmesini engellemek maksadıyla 'güvenli sil' (üzerine yazma) işlemi yapılır.
- Güvenli silme işlemi, manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu iş için uygun bir yazılım (DBAN, Kill Disk, Eraser, Disk Wipe, HDShredder gibi) veya donanım kullanılır.

- Arızalanan ya da bakıma gönderilen cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce veri saklama ortamının sökülerek saklanması sağlanır.

LİSANSLAMA VE FİKRİ MÜLKİYET HAKLARI

- Fikri mülkiyet insan zekâsının, entellektüel birikiminin, zihinsel yaratıcılığının ortaya çıkarmış olduğu müzikten, edebiyata, endüstriyel tasarımlardan bilimsel buluşlara kadar uzanan geniş bir yelpaze içinde yer alan ürünleri kapsar. Bu ürünler düşünce safhasında kaldığı ve üreticisi dışındakilerle paylaşılmadığı sürece korumaya konu olmazlar. Ancak bu düşüncelerin ve ürünlerin, uygun şekilde kayıt altına alınmalarını takiben diğer kişilerle paylaşılmaları ve özellikle bu ürünlerin kazanç amacıyla ticarete konu olmaları söz konusu olduğu zaman korunmaları gerekir.
- Fikri mülkiyet, sınai mülkiyet hakları ve telif hakları olmak üzere iki ana başlık altında incelenir.
- Sınai mülkiyet hakları; teknolojik buluşlar, patentler, mal ve hizmetlerin ticari markaları, modeller, endüstriyel tasarımları ve coğrafi işaretleri kapsar. Bu haklar 6769 Sayılı Sınai Mülkiyet Kanunu ile korunur. Tescil işlemleri, Türk Patent ve Marka Kurumu tarafından koordine edilir.
- Telif hakları; edebiyat, müzik, sanat ürünleri ve görsel-işitsel ürünler, filmler, bilgisayar program ve yazılımlarını ortaya çıkaran kişilerin bu ürünler üzerindeki haklarını içerir. Bu haklar 5846 sayılı Fikir ve Sanat Eserleri Kanunu ile korunur. Konu ile ilgili faaliyetler, T.C. Kültür ve Turizm Bakanlığı Telif Hakları Genel Müdürlüğü tarafından yürütülür.
- Üniversitemizde ve bağlı birimlerince yapılan her türlü iş ve işlemlerde, fikri mülkiyet haklarına saygılı davranılır. Bu hakların korunması için gerekli tedbirler alınır.
- Lisanslı yazılım kullanımı ile ilgili hususlarda Başbakanlık'ın 2008/17 sayılı Genelgesinde belirtilen esaslara dikkat edilir. Genelge ile lisanslı yazılım kullanımı ile ilgili işlerde "birinci derecede" sorumluluğun "ilgili kamu kurum ve kuruluşunda bilgi işlem ünitesi veya bu işten sorumlu birimde çalışanlara" verilmiş olduğu dikkate alınır.
- Çeşitli maksatlar için tedarik edilen yazılımlar, kurumların taşınır kayıt birimleri tarafından envantere alınmak suretiyle kayıt altına alınır.
- Yazılımlara ait lisans belgeleri, yazılımın üreticisi firma tarafından sağlanan lisans takip/indirme sayfasına erişim şifresi, varsa CD/DVD ve benzeri materyal, USB vb. anahtarlar, ilgili projenin yürütüldüğü birimde muhafaza edilir. izinsiz olarak kopyalanması vb.) yazılım kullanılamaz.
- Herhangi bir proje veya faaliyet kapsamında yeni bir yazılım tedarik edilmesi ihtiyacı olduğunda, tedarik faaliyetine başlanmadan Bilgi İşlem Birimi ve Taşınır Kayıt Birimi ile koordinasyon kurulur.
- Üniversitemize ait hiçbir cihazda, üreticisi tarafından açıklanmış lisanslama politikasına aykırı bir şekilde (lisanslama/kullanım anahtarının kırılması, yazılımın izinsiz olarak kopyalanması vb.) yazılım kullanılamaz.
- Lisans çerçevesinde izin verilen kullanıcı sayısının aşılmaması için gerekli tedbirler alınır.
- Çeşitli isimler altında (open source, freeware, shareware) ücretsiz olarak dağıtılan yazılımlar, zararlı öğeler barındırma ihtimaline karşı test edilmeden kuruma ait bilgisayarlara kurulmaz.
- Üniversitemiz çalışanlarınca, görev tanımlarının bir parçası olarak resmi bir hizmetin ifası için kurum kaynakları kullanılmak suretiyle üretilen (her türlü bilgi, belge, rapor, doküman, grafik, kitapçık, sunum, tasarım, proje, yazılım vb.) fikri mülkiyete konu olabilecek varlıkların mülkiyeti, Üniversitemize aittir. Fakültemiz söz konusu varlıkları, ilgili mevzuat uyarınca kendi adına tescil ettirebilir. Kişiler, söz konusu varlıklar üzerine kişisel bir hak iddia edemezler. Aksi kararlaştırılmadıkça, tedarik sözleşmeleri kapsamında yüklenici firmalar tarafından yapılan/yaptırılan tasarım, geliştirme ve/veya eklemelere ilişkin ortaya çıkan fikri mülkiyet hakları aittir. Bu kapsamda, yükleniciler tarafından geliştirilen (tasarım, yazılım, yazılım kodu, algoritma vb.) fikri mülkiyete konu olabilecek varlıklar, sözleşme süresi sonunda idare tarafından teslim alınır. Yükleniciler ve/veya çalışanları, söz konusu varlıklar üzerinde kişisel/kurumsal bir hak iddia edemezler.

- Yüklenici firmalar, sözleşmeler kapsamında Üniversitemiz için yaptıkları iş ve işlemlerde üçüncü taraflara ait herhangi bir fikri mülkiyet hakkını ihlal edemezler. Bu husus sözleşmelere konulmak suretiyle garanti altına alınır.
- Telif hakları kapsamında korunan kitaplar, makaleler, raporlar ve diğer belgeler hiçbir şekilde kopyalanamaz, çoğaltılmaz ve dağıtılamaz.

FİZİKSEL VE ÇEVRESEL GÜVENLİK

Fiziksel ve çevresel güvenlik, işyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikelere karşı korunmasıdır. Günümüzde bilgiler, büyük oranda bilgi sistemleri vasıtasıyla işlenmekte ve sayısal ortamlarda saklanmaktadır. Bu nedenle bilgi güvenliği ile ilgili tedbirlerin önemli bir kısmını, bilgi sistemleri ve ağlarının korunmasına yönelik siber güvenlik önlemleri oluşturmaktadır. Bununla birlikte, fiziksel ortamda saklanan bilgiler ile elektronik ortamda saklanan verilerin muhafaza edildiği bilişim sistemleri ve ağlarının güvenliği için, fiziksel ve çevresel önlemlerin alınması kaçınılmazdır.

Güvenli Alanlar

- Fiziksel ve çevresel güvenlik tedbirlerinin belirlenmesi ve uygulamaya alınmasının ön koşulu, hassas veya kritik bilgi ve bilgi işleme tesislerini barındıran güvenli alanların tespit edilmesi ve bu alanların güvenlik sınırlarının tanımlanmasıdır.
- Güvenlik sınırları belirlenirken kademeli bir yaklaşım kullanılır. Gerekiyorsa iç içe güvenli alanlar oluşturularak, daha hassas ve kritik bilgilerin işlendiği alanlara erişim için birden fazla fiziksel sınırdan geçilmesi zorunlu hale getirilir.
- Güvenlik sınırları belirlenirken kişilerin kontrolsüz olarak giriş çıkış yapabilecekleri herhangi bir boşluk bulunmamasına dikkat edilir. Bu tür boşlukların kapatılması/korunması için ilave tedbir alınır.
- Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunur.
- Göreceli olarak daha az hassas varlıkların yer aldığı dış güvenlik sınırında alınan güvenlik tedbirleri ile kritik varlıkların yer aldığı iç güvenlik sınırlarındaki tedbirler farklılaştırılır.
- Güvenli alanlar, fiziksel güvenlik engelleri ile çevrili, kilitlenebilir bir ofis ya da birkaç oda olabilir. Birden fazla kuruluşun aynı bina içerisinde olduğu durumlarda fiziksel erişim güvenliğine özel dikkat gösterilir.
- Fiziksel koruma, bir ya da daha fazla fiziksel engel konularak gerçekleştirilir. Birden fazla fiziksel engel kullanımı (kartlı geçiş sistemleri, turnikeler, kayar kapılar, kilitli odalar vb.) ilave koruma sağlayarak tek bir engelin başarısızlığı durumunda güvenliğin tehlikeye girmesini önler.
- Giriş kontrolleri, korunacak tesis veya varlığa göre değişir.
- Sağlık hizmet sunumu yapan tesislerde en dışta yer alan güvenlik sınırlarının geçiş noktaları, sadece gözle veya elektronik tarama araçları ile korunur. Burada amaç, vatandaşların gereksiz giriş kontrolleri ile uğraşmadan en kısa yoldan sağlık hizmetine eriştirilmesidir. Bununla birlikte sürekli gözetim yapılarak şüpheli durumlarda, güvenlik personeli vasıtası ile gerekli üdahalelerde bulunulur. Bölgesel koşullar dikkate alınarak ilave güvenlik tedbirleri alınabilir.
- Kapsamı ve yöntemi idareler tarafından belirlenecek şekilde ziyaretçilerin giriş ve çıkışlarının tarih ve saatleri kayıt altına alınır. Daha önce erişimi onaylanmadığı sürece tüm ziyaretçiler denetlenir.Kapsamı ve yöntemi idareler tarafından belirlenecek şekilde ziyaretçilerin giriş ve çıkışlarının tarih ve saatleri kayıt altına alınır. Daha önce erişimi onaylanmadığı sürece tüm ziyaretçiler denetlenir.
- Ziyaretçilere sadece belirli, yetkilendirildikleri amaçlar için erişim verilir. Ziyaretçilerin kimliği uygun bir yöntem ile doğrulanır.
- Sunucu odaları, güvenlik kontrol merkezleri, arşiv odaları vb. hassas bilgilerin işlendiği veya saklandığı alanlar kolayca ulaşılamayacak yerlere kurulur. Bu gibi yerlere giriş için iki faktörlü kimlik doğrulama mekanizmaları kullanılır.

- Kapsam ve yöntemi idarelerce belirlenmek suretiyle tüm personel ve ziyaretçilerin güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartları hazırlanır ve kullanılır.
- Dış taraf destek personeline güvenli alanlara veya gizli bilgi işleme tesislerine erişim izni, sadece gerekli olduğu durumlar için geçici süre ile verilir. Bu tür erişimlerde, mümkün olduğu kadar erişim kısıtlaması yapılır ve takip edilir.
- Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilir.
- Güvenli alanlara erişim hakları düzenli olarak gözden geçirilir. Gereksiz erişim izinleri iptal edilir veya yetki kısıtlaması yapılır.
- Sahipsiz güvenli alanlar fiziksel olarak kilitlenir ve periyodik olarak gözden geçirilir.
- Yetki verilmediği sürece, güvenli alanlarda fotoğraf, video, ses ve diğer kayıt cihazları ve mobil cihazlardaki kameralara izin verilmez.
- Yetkisiz kişilerin teslimat ve yükleme işlemleri için güvenli alanlara giriş yapmasını engellemek üzere, güvenli alan dışında olacak şekilde teslimat ve yükleme alanları oluşturulur.
- Postacı, kurye personeli, dağıtıcı gibi kişilerin tesis içlerine kontrolsüz olarak girmesi engellenir. Teslimat ile ilgili kurallar oluşturulur. Teslimat işlemlerinin kurum içinde belirlenecek noktalarda yapılması için tedbir alınır.
- Personel güvenliği ve sağlığı için ilgili yönetmelikler uygulanır.
- Yangın, sel, deprem, patlama ve diğer doğal afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınır ve uygulanır.Giriş/çıkış yapılan yerler ve ortak kullanım alanları güvenlik kameraları ile kayıt altına alınır.

EKİPMAN GÜVENLİĞİ

Belli Başlı Temiz Masa Kuralları

- Masalarda ya da çalışma ortamlarında korumasız bırakılmış bilgiler yetkisiz kişilerin erişimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle bütünlüğünün bozulmalarına ya da yok olmalarına sebep olabilir. Tüm bu veya daha fazla tehditleri yok edebilmek için belli başlı temiz masa kurallarına çalışanlar tarafından uyulması sağlanır.
- Hassas bilgiler içeren bilgi, belge ve evraklar masa üzerlerinde ya da kolayca ulaşılabilir yerlerde açıkta bulundurulmaz. Bu gibi bilgi ve belgeler kilitli dolap, çelik kasa ya da arşiv odası gibi fiziki koruması olan güvenli alanlarda muhafaza edilir.
- Yetkisiz kişilerin erişiminin engellenmesi için bilgisayar başından ayrılma durumunda ekran kilitlemesi yapılır. Otomatik ekran kilitlemesi devreye alınır.
- Sistemlerde kullanılan parola, telefon numarası ve T.C kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulundurulmaz.
- Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler imha edilir.
- Faks makinelerine gelen yazılar sürekli kontrol edilir ve makinede yazı bırakılmaması için tedbir alınır.
- Her türlü bilgiler, parolalar, anahtarlar ve bilginin sunulduğu sistemler, sunucular, kişisel bilgisayarlar ve benzeri cihazlar yetkisiz kişilerin erişebileceği bir şekilde parola korumasız ve fiziki olarak güvensiz bir şekilde gözetimsiz bırakılmaz.
- Fotokopi ve diğer çoğaltma teknolojilerinin (tarayıcı, sayısal kamera vb.) yetkisiz kullanımını önlemek için uygun idari ve teknik tedbirler alınır.

Ekipman Yerleşimi ve Koruması

- Yüksek maliyetli, özel koruma gerektiren, elektronik cihazların (tıbbi cihazlar dahil) yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine dikkat edilir

- Ekipmanlar, gereksiz erişimleri asgari düzeye indirecek şekilde yerleştirilir.
- Kritik veri içeren araçlar, yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilir.
- Özel koruma gerektiren ekipmanlar izole edilmiş şekilde kullanılır.
- Nem ve sıcaklık gibi parametreler izlenir.
- Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanır.
- Paratoner kullanılır.
- Bilgi işlem araçlarının yakınında yeme, içme ve sigara kullanımı konularını düzenleyen kurallar oluşturulur ve uygulanır.

DESTEK HİZMETLERİ

- Elektrik, su, kanalizasyon ve iklimlendirme sistemlerinin, destekledikleri bilgi işlem birimi için yeterli düzeyde olmasına dikkat edilir.
- Ekipmanların elektrik arızalarından korunması için ana besleme noktalarında elektrik şebekesine yedekli bağlantı yapılır.
- Kritik sistemlerde hizmet kesintisi yaşanmaması için kesintisiz güç kaynağı veya jeneratör kullanılır.
- Jeneratör eğer var ise kullanımı için yeterli düzeyde yakıt bulundurulur.
- Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.

KABLOLAMA GÜVENLİĞİ

- Güç ve iletişim kablolarının (ağ kabloları, güç kaynağı kabloları, telefon kabloları, vb.) fiziksel etkilere ve dinleme faaliyetlerine karşı korunması için önlemler alınır.
- Kablolar binalar arası geçişte yeraltında, bina içlerinde kablo kanalları veya tavalar içerisinden geçirilir.
- Karışmanın (interference) olmaması için güç ve iletişim kabloları fiziksel olarak ayrılır.
- Hatalı bağlantıların olmaması için ekipman, kablolar ve prizler görülebilecek bir şekilde etiketlenir ya da işaretlenir.
- Kablolama yapılırken gelecekteki ihtiyaçlar dikkate alınarak yedekli olarak kablo çekilir.
- Bina içindeki yerel alan ağı ana omurgası fiziksel olarak yedekli bir şekilde çalıştırılır.
- Dağıtım panelleri ve kenar anahtarların konulduğu kabinler yetkisiz erişime karşı kilitli olarak bulundurulur.
- Bahse konu kabinlerin de kesintisiz güç kaynağı ve jeneratör altyapısından faydalanması sağlanır.

EKİPMAN BAKIMI

- Kurumda kullanılmakta olan ekipmanların yıllık bakım planları oluşturulur. Planda yer alan ekipman listesinin envanter ile uyumlu olması kontrol edilir.
- Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılır.
- Bakım işlemleri sadece yetkili personel tarafından yerine getirilir. Son kullanıcıların ya da yetkisiz kişilerin donanım yapılandırmalarında değişiklik yapmasını engellemek için (kasa kilidi, kasa açma/ kapama etiketi gibi) gerekli tedbirler alınır.
- Bakım kayıtları düzenli olarak tutulur. Ekipmanlar bakım için kurum dışına çıkarılırken sabit disklerinde yer alan bilgilerin yetkisiz kişilerin eline geçmemesi için tedbir alınır. Bu kapsamda diskler sökülür ya da diskte yer alan bilgiler kalıcı olarak silinir.
- Ekipmanlar sigortalıysa, sigorta şartlarının sağlanması için gerekli özen gösterilir.
- Üretici garantisi kapsamındaki ürünler için garanti süreleri kayıt altına alınır ve takip edilir.

KURUM DIŞINDAKİ EKİPMANIN GÜVENLİĞİ

- Kuruma ait bilgisayarların kurum dışına çıkarılması ya da kişisel/yüklenici firmalara ait bilgisayarların işyerlerine getirilerek kurumsal amaçlarla kullanımı için yetkilendirme yapılması gerekir.
- Bu şekilde kullanılan ekipmanların ve kullanıcıların listesi oluşturulur ve takip edilir.
- Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenir.
- Bu şekilde kullanılan ekipmanlar, Taşınabilir Ortam Yönetimi tedbirleri alınmak suretiyle kullanılır.
- Tesis dışına çıkarılan ekipmanın gözetimsiz bırakılmamasına ve seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilir.
- Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulur.

EKİPMANIN GÜVENLİ İMHASI

Üzerlerinde kalıcı olarak veri barındıran ekipmanlar (sunucu, masaüstü veya dizüstü bilgisayarın, merkezi veri depolama birimlerinin ve benzeri bilgi sistem cihazlarının sabit diskleri ile USB flaş sürücüsü, USB hafıza ünitesi, flash disk ya da USB hafıza olarak bilinen taşınabilir veri depolama ortamları) usulüne uygun yöntemler kullanılarak imha edilir veya güvenli silme işlemi yapılır.

KİŞİSEL VERİLERİN KORUNMASI

- Anayasa'nın 20'ci maddesinin, 6698 sayılı kanunun ve Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin, kişisel verilerin korunmasına ilişkin hükümlerine azami düzeyde hassasiyet gösterilir.
- Kişisel verilerin ve kişisel sağlık verilerinin işlenmesinde, 6698 sayılı kanunun 4'üncü maddesinde yer alan genel ilkelere; ayrıca kişisel verilerin işlenmesinde Kanun'un 5'inci maddesinde, kişisel sağlık verilerinin işlenmesinde ise Kanun'un 6'ncı maddesinde yer alan hükümlere riayet edilir.
- Kişisel verilerin ve kişisel sağlık verilerinin aktarılmasında, 6698 sayılı kanunun 8'inci ve 9'uncu maddesinde yer alan hükümlere riayet edilir.
- 6698 sayılı kanunun 12'nci maddesinin birinci fıkrası uyarınca veri sorumlusu; verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek, verilerin muhafazasını sağlamak amaçlarıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.
- 6698 sayılı kanunun 12'nci maddesinin ikinci fıkrası uyarınca veri sorumlusu (İdare), kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişiler (sağlık hizmet sunucularında HBYS işletimi hizmeti veren yüklenici) ile birlikte müştereken sorumludur.
- 6698 sayılı kanunun 12'nci maddesinin üçüncü fıkrası uyarınca veri sorumlusu, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. Dolayısı ile Kanun hükümlerine uyumluluğun sağlanıp sağlanmadığı hususunda veri sorumlusu, veri işleyeni (HBYS işletimi hizmeti veren yüklenici) denetleyebilir.
- 6698 sayılı kanunun 12'nci maddesinin dördüncü fıkrası uyarınca veri sorumlusu ile veri işleyen (HBYS işletimi hizmeti veren yüklenici), öğrendiği kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.
- Kişisel verilere ilişkin suçlar bakımından 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ile 140'ıncı madde hükümleri uygulanır.
- 6698 sayılı kanun hükümlerine uygunsuzluk nedeniyle Kişisel Verileri Koruma Kurumu tarafından verilecek idari para cezaları ile ilgili kişiler tarafından açılacak davalarda hükmedilecek maddi ve manevi tazminat davaları, kusurlu olması hâlinde veri işleyen (işletimi hizmeti veren yüklenici) tarafından ödenir.

5651 SAYILI KANUN İLE UYUM

- Türkiye'de internet ile ilgili en kapsamlı düzenleme 2007 yılında 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile sağlanmıştır.
- 5651 sayılı kanun ile temel olarak aşağıdaki hususlarda düzenlemeler yapılmıştır
- İnternet aktörlerinin (içerik sağlayıcı, yer ve erişim sağlayıcı, toplu kullanım sağlayıcı) tanımı yapılmış ve bu aktörlerin hak ve sorumlulukları belirlenmiştir.
- Yasada suçlar bakımından erişimin engellenmesi usul ve esasları düzenlenmiştir.
- İnternet ortamında yayımlanan içerik nedeniyle haklarının ihlal edildiğini iddia eden kişilere ilişkin; içeriğin yayından çıkarılmasını sağlama ve cevap hakkı uygulamalarına ilişkin usul ve esaslara yer verilmiştir.
- Konusu suç teşkil eden (ve/veya küçükler için zararlı olan) içerik kapsamında filtreleme usulü öngörülmüştür.
- Türkiye'de internet ortamındaki yayınlardan kanunda belirtilen katalog suçlara ilişkin şikâyetlerin yapılabileceği internet bilgi ihbar merkezi (ihbarweb.org.tr) kurulmuştur.
- Kurumlarımızda tesis edilmiş olan ağların hemen hemen tamamına yakını bir şekilde internet ortamına bağlı olarak çalışmakta ve Kanunda belirtilen internet aktörlerinden "içerik sağlayıcı, yer sağlayıcı veya toplu kullanım sağlayıcı" rollerinden bir veya birkaçına girebilmektedir. "Erişim sağlayıcı" kuruluşlar, abonelerine ticari olarak internet erişimi sağlayan telekomünikasyon firmaları olup Üniversitemiz bağlı hiçbir kurum bu kategoriye girmemektedir.
- İçerik Sağlayıcı, İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir. Üniversitemiz ve bağlı birimleri web sayfaları vasıtası ile kullanıcılara içerik sundukları için "İçerik Sağlayıcı" konumundadır.
- İçerik Sağlayıcı; İnternet ortamında kullanıma sunduğu her türlü içerikten sorumludur. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur. Bu nedenlerle web sayfalarımızda yer alan her türlü içeriğin mutlaka bir sahibi olmalı ve kayıt altına alınmalı, kurumun web sayfasında içerik yayımlama ile ilgili usul ve esaslar belirlenmelidir.
- Sistemi işleten Üniversitemiz değil ilgili web sitesine içeriği koyan kişi veya kurumlar sorumludur.
- Yer Sağlayıcı, internet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir.
- Yer sağlayıcı; Yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, Kanun ve ilgili mevzuat hükümlerine göre BTK, adli makamlar veya hakları ihlal edilen kişiler tarafından haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde, hukuka aykırı içeriği yayından kaldırmakla, trafik bilgisini ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri iki yıl süre ile saklamakla sorumludur.
- Yer sağlayıcı trafik bilgisi, internet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgilerdir.
- Üniversitemiz ve bağlı birimlerine ait web sayfalarının ve uygulamaların sunumunda kullanılan yazılım ve donanımları işleten birimler "Yer Sağlayıcısı" konumundadır. Bu kapsamda, Web siteleri ve uygulamaları, kuruma ait sunucu/sistemler vasıtası ile sunuluyorsa yer sağlayıcısı ilgili kurumun kendisi,
- Web siteleri barındırma hizmeti, hizmet alımı ile SBYS firmaları veya diğer üçüncü kişilerden alınıyorsa yer sağlayıcısı ilgili SBYS firması veya üçüncü kişiler olmaktadır.

- Web siteleri barındırma hizmeti, hizmet alımı ile SBYS firmaları veya diğer üçüncü kişilerden alınıyorsa, hizmet sözleşmelerine 5651 kanunu ile ilgili maddelerin koyulması ve yapılacak firma denetimleri ile bu verilerin alındığının kontrol edilmesi gerekir.
- İnternet Toplu Kullanım Sağlayıcılar, kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek ve tüzel kişilerdir. Üniversitemiz ve bağlı birimleri, tesis edilen bilişim altyapısı kullanılmak suretiyle, son kullanıcılara internet ortamına erişim sağlıyorsa "İnternet Toplu Kullanım Sağlayıcı" konumundadırlar.

- İnternet Toplu Kullanım Sağlayıcıları; Erişim kayıtlarını ve bu kayıtların doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri 2 (iki) yıl süre ile saklamakla, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme (İnternet ortamında web adresi, alan adı, IP adresi, kelime ve benzeri ölçütlere göre erişimi engelleyen yazılımları ve donanımları) sistemini kullanmakla, kamuya açık alanlarda internet erişimi sağlayan toplu kullanım sağlayıcılar, kullanıcıları tanımlayacak sistemleri kurmakla sorumludur.
- Erişim kaydı olarak kullanıcılara iç ağda dağıtılan IP adres bilgilerinin, IP adreslerinin kullanıma başlama ve bitiş zamanlarının ve bu IP adreslerini kullanan bilgisayarların MAC adreslerinin, hedef IP adreslerinin kayıt altına alınması gerekir.
- İnternet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme sisteminin yanı sıra, ilave tedbir olarak güvenli internet hizmeti de alabilirler.

MAL VE HİZMET ALIMI GÜVENLİĞİ

- Kurum olarak mal ve hizmet alımlarında ilgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak rekabeti engellemeyecek şekilde gerekli güvenlik düzenlemeleri İdari veya Teknik şartnamelerde belirtilmelidir.
- 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.

YAZILIM GÜVENLİĞİ POLİTİKASI

- Kullanıcı hesabı incelemeleri tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en fazla 6 (altı) aylık aralıklarla yapılır.
- Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında gözden geçirilir.
- 60 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır.
- Parolalar kişiye özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.
- Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da parola oluşturma özelliklerine uygun olmak zorundadır. İnternet tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.
- Merkezimiz kullanıcılarının parolasını hatırlamayan kullanıcıların; bilgi işlem talep sistemi üzerinden yazılı olarak talep eden personelin parola sıfırlama işlemi gerçekleştirilir.

E-POSTA KULLANIM POLİTİKASI

- E-Posta kullanımına yönelik işlemler fakültemizin "E- Posta Güvenliği Talimatına" göre yönetilmektedir.
- Her türlü e-posta iletişimi, birimlere ve kişilere özel tanımlanan "ege.edu.tr" uzantılı kurumsal e-posta adreslerinden olmalıdır.
- Kullanıcıyı resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılmaz.
- İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez

- 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.
- Personel 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 ve/ya rar formatında) mesaja eklenecektir.
- 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, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Fakültemiz Bilgi İşlem Birimine 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, Fakültemiz Bilgi İşlem Birimine haber verilmelidir.
- Spam, zincir e-posta, sahte e-posta vb. zararlı 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 Fakültemiz Bilgi İşlem Birimine 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 Fakültemiz Bilgi İşlem Birimine haber verilmelidir.
- Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Bilgi İşlem birimine haber verilmelidir.

BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

Bilgi güvenliğinin ihlaline yönelik işlemler fakültemizin **"Bilgi Güvenliği İhlal Bildirim ve Yönetim Talimatı"**na göre yönetilmektedir.

Bilgi yönetim sistemine yönelik fiziksel tehlikeler, yazılım ve donanımla ilgili sorunlar, bilgi güvenliği, bilgi mahremiyeti, kişisel verilerin korunması, kullanıcı hataları gibi konularda risk değerlendirmesi bilgi işlem çalışanları ve üst yönetim ile yapılan toplantıda belirlenir. Risk değerlendirmesi 6 ayda bir veya ihtiyaç

duyulduğunda yapılır. Böylelikle beklenen veya olası riskleri ve kontrol altına alınmasına ilişkin önlem ve eylem planının tanımlanmasını sağlamaktır.

Risk değerlendirmelerinde Ege Üniversitesi Strateji Daire Başkanlığı tarafından hazırlanan "Ege Üniversitesi İç Kontrol Risk Değerlendirme Kılavuzu" kullanılır. Bu kılavuzda yer alan "Risk iştahı" tablosu kullanılarak riskin düzeyi belirlenir. Ortaya çıkabilecek risk düzeyine göre alınacak önlemler ve eylem planı oluşturulur. Etki ve olasılık üzerinden risk haritası puanı hesaplanır ve tablodan risk düzeyi belirlenir.

Ortaya çıkabilecek risklere karşı iyileştirme çalışmaları gerçekleştirilir.

Risk İştahı tablosu

Risk Düzeyi	**Puanlar**
Düşük	0 - 10
Orta	11 - 40
YÜksek	41 - 100

Risk Haritası

	10	10	20	30	40	50	60	70	80	90	100
	9	9	18	27	36	45	54	63	72	81	90
	8	8	16	24	32	40	48	56	64	72	80
	7	7	14	21	28	35	42	49	56	63	70
Etki	6	6	12	18	24	30	36	42	48	54	60
	5	5	10	15	20	25	30	35	40	45	50
	4	4	8	12	16	20	24	28	32	36	40
	3	3	6	9	12	15	18	21	24	27	30
	2	2	4	6	8	10	12	14	16	18	20
	1	1	2	3	4	5	6	7	8	9	10
		1	2	3	4	5	6	7	8	9	10
						Olasılık					

Risk etkisi puanlaması ve açıklamaları

10 puan:	Temel görevleri tamamen devre dışı bırakır.
9 puan:	Temel görevleri büyük ölçüde devre dışı bırakır.
8 puan:	Temel görevleri kısmen devre dışı bırakır.
7 puan:	Temel görevleri devre dışı bırakmaz ancak işleyişini önemli ölçüde etkiler.
6 puan:	İşleyişi bozmayacak kapsamlı düzeltmeler yapılmasını gerektirir.
5 puan:	İşleyişi bozmayacak düzeltmeler yapılmasını gerektirir.
4 puan:	İşleyişi bozmayacak küçük düzeltmeler yapılmasını gerektirir.
3 puan:	İşleyişi bozma ihtimali olan risk izlenmelidir.
2 puan:	İşleyişi bozacak bir risk olmasa da risk bilinci oluşturulmalıdır.
1 puan:	İşleyişi bozacak bir risk yoktur.

Riskin ortaya çıkma olasılığı puanlaması ve açıklamaları

10 puan:	Ortaya çıkması kesin,
9 puan:	Her an ortaya çıkabilir,
8 puan:	Kısa zaman içerisinde ortaya çıkma olasılığı yüksek,
7 puan:	Kısa zaman içerisinde ortaya çıkma olasılığı var,
6 puan:	Faaliyet dönemi içinde ortaya çıkabilir,
5 puan:	Faaliyet dönemi sonunda ortaya çıkabilir,
4 puan:	Sonraki faaliyet döneminde ortaya çıkabilir,
3 puan:	Uzun vadede ortaya çıkabilir,
2 puan:	Ortaya çıkma olasılığı düşük,
1 puan:	Ortaya çıkma olasılığı yok

ORTAYA ÇIKABİLECEK RİSK	**Risk düzeyi**
Kullanıcı hatası	Düşük
Genel sistem çökme riski	Düşük

Sunucu güvenliği	Orta
Virüs	Orta
Donanım arızası	Orta
Veri kaybı	Düşük
İzinsiz giriş veya çıkış	Düşük

OLAY TANIMI	**YETKİLİ KİŞİ/KURUM**	**İLETİŞİM BİLGİLERİ**
Her türlü bilgi güvenliği ihlal olayları durumunda	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 1544 ve 1533
Virüs, izinsiz giriş, trojan, spyware vb. bulgular için, sistem sunucu servis problemleri için	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 1544 ve 1533
Donanım arızaları, Network Problemleri için	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 1544 ve 1533
Veri kaybı, bilgilere yetkisiz erişim durumlarında	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 1544 ve 1533
Hırsızlık, kaybolma, yanma, kırılma vb. durumlar için	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 1544 ve 1533
Uygunsuz davranışlar ve politikaya uymayan kişiler için	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 1544 ve 1533
Ağ üzerinden Saldırı	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 1544 ve 1533
Bilgisayarınızda Anti Virüs Programı yüklü değilse	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 1544 ve 1533

7. İLGİLİ DÖKÜMANLAR

Kuruma Başlayış ve Kurumdan Ayrılış Formu
Bilgi İşlem İstek Formu
E-Posta Güvenliği talimatıParola
Güvenliği Talimatı
Bilgi Güvenliği İhlal Bildirim ve Yönetim Talimatı
Sosyal Mühendislik Zafiyetleri ve Sosyal Medya Güvenliği Talimatı
Bilgi Sitemleri Uzaktan Bağlantı Erişim Talep Formu

Yedekleme Teslim Formu

8. REVİZYON BİLGİLERİ:

Revizyon No	Revizyon Tarihi	Revizyon Açıklaması
01	07.05.2024	- Revizyonların dokümanlarda nasıl gösterileceğinin eklenmesi, -"Kontrol Eden" kısmında yer alan "Kalite Yönetim Direktörü"' nün "Kalite Yönetim Sorumlusu" olarak değiştirilmesidir. **- "Bilgi Varlıklarımız" başlığı altına** Bgys.ege.edu.tr Adresinde varlıklarımız kayıt altında tutulmaktadır, maddesinin eklenmesi, - "Risk Yönetimi" bölümünün eklenmesi, - **"Sunucu Ve Sistem Odasi Güvenliği" başlığı altına** "Sunucuya ait güncel bilgiler bgys.ege.edu.tr adresinde kayıt altına alınmıştır" maddesinin eklenmesidir.
02	08.08.2024	Dokümanlarımızda yer alan "Ege Üniversitesi Diş Hekimliği Fakültesi" isminin hastane olması nedeni ile "**Ege Üniversitesi Ağız ve Diş Sağlığı Hastanesi**" olarak değiştirilmesidir.