İZMİR EKONOMİ ÜNİVERSİTESİ

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

İçindekiler

1. KAPSAM

İEÜ Kabul Edilebilir Kullanım Politikası tüm kullanıcıları kapsar. Politika maddeleri hem ofis içindeki hem de ofis dışındaki kullanım için geçerlidir. Ayrıca bazı alanlarda kullanıcının sorumluluğunda çalışan 3. parti çalışanları için de kabul edilebilir kullanım kuralları bu politika ile tanımlanmaktadır.

2. PERSONEL KULLANIM

2.1. Personel Bilgisayar Tahsisi Politikası

İEÜ'da görev yapan kullanıcılara, görev tanımları gereği bilgi teknolojileri donanımları tahsis edilmekte, kullandırılmakta ve yenilenmektedir. Donanımların tahsisinde satın alma ve kiralama yöntemi tercih edilmektedir.

Tahsis edilecek donanım, her çalışana, İK biriminden veya DYS (Doküman Yönetim Sistemi) üzerinden gelen talebe istinaden görev tanımına veya İEÜ tarafından belirlenmiş kullanım kriterlerine uygun olarak verilmektedir. Her seviyedeki çalışana normal kullanım ihtiyaçları çerçevesinde standart uygulamaların bulunduğu donanım tahsis edilmektedir. İleri seviye konfigürasyona sahip donanım, standart donanımın kullanıcının ihtiyacını karşılayamadığı özel durumlarda DYS üzerinden talep açılarak, Rektör veya Genel Sekreter ve Bilgi Teknolojileri Direktörlüğü onayı ile verilebilir.

Masaüstü ve dizüstü bilgisayarların satın alma tarihinden itibaren en az beş yıl kullanılması hedeflenmelidir. Beş yıllık kullanım süresi içinde kişinin kullanıcı profilindeki herhangi bir değişiklik sebebiyle bilgisayarının değiştirilmesi gündeme gelirse, mevcut bilgisayar İEÜ bünyesinde başka bir uygun kullanıcıya verilebilir.

Bilgi teknolojileri ile bağlantılı tüm donanım (yazıcı, pc, notebook vb.) talepleri DYS üzerinden talep açılarak, Rektör ve/veya Genel Sekreter ve Bilgi Teknolojileri Direktörülüğünün onayı ile alınmaktadır.

2.2. Personel Kullanım Politikası

İEÜ bilgisayar ve iletişim sistemlerinin kişisel kullanımı, gerekli olduğu durumlarla kısıtlanmalıdır. Kişisel kullanım, e-posta zincirlerinin yayılmasına yardımcı olmak veya yaratmak, uygunsuz veri ve resim alışverişi yapmak, iş aramak, kumar oynamak ve politik aktivitelere katılmak gibi hareketleri içeremez. İş ile ilgisi olmayan kişisel dosyalar (fotoğraflar, mp3, filmler, vb.) tutulmamalıdır. İEÜ BTD ortak paylaşım sunucularında ve her türlü BT donanımında saklanan iş dışı kişisel dosyaları haberli/habersiz bir şekilde denetleme ve silme hakkına sahiptir. Kullanıcı, işi gereği kendisine teslim edilecek tüm demirbaşları iyi korumak ve dikkatle kullanmakla yükümlüdür.

2.3. İEÜ Kaynaklarının Yasalara ve Etik Prensiplerine Uygun Kullanımı

Kullanıcı, internet kullanımı ve sesli haberleşme aktiviteleri dahil olmak üzere, tüm bilgi sistemleri ve iletişim imkanlarının kullanımında ve bu imkanların sağlanmasında, başta 5651 sayılı yasa olmak üzere ilgili Türkiye Cumhuriyeti yasalarına, uluslararası hukuka ve genel etik kurallarına uymakla yükümlüdür. Kullanıcılar, bilgisayarlarında bulunabilecek standart iş ve ofis uygulamaları dışındaki yazılımlar (İEÜ BTD tarafından kurulmuş işletim sistemi, virüs koruma, ofis uygulamaları, iş uygulamaları vb. dışındaki yazılımlar) için telif hakkı koruma düzenlemelerine uymakla şahsen sorumludur.

Diğer kullanıcıların kimlik doğrulama ve erişim kontrol araçlarını (VPN, fiziksel geçiş kontrol kartı, vb.) ele geçirmeye çalışmak, İEÜ kaynaklarına zarar vermek ya da üçüncü taraflara İEÜ kaynaklarını kullanarak zarar vermek yasaktır. Kullanıcılar teknik olarak mümkün olsa bile iş sorumlulukları gereği erişim ihtiyacı olmayan kaynaklara erişmemelidirler. Kullanıcılar bu hususlarda bir zafiyet fark ederse BTD birimine bilgilendirmekle yükümlüdür.

Tüm iletişimde genel prensip olarak kurumsal ve genel etik ve nezaket kurallarına uyulmalıdır. Ayrıca iletişim sırasında kurum çalışanlarına, öğrencilere ve diğer taraflara zarar verecek hakaret içeren ifadeler kullanılamaz. İEÜ bilgi kaynaklarının personel tarafından yasal olmayan şekilde kullanımı halinde yasa uygulayıcılar ile işbirliği yapabilir.

Talep eden kullanıcılara BTD uygun görmesi durumunda ise “lokal admin (yerel yönetici)” yetkisi taahhütname ile verilebilir.

Kullanıcılar bilgisayarlarında kurulu olan ve İEÜ BTD’ nin sağlamış olduğu yazılımların dışındaki kullanacakları yazılımların lisanslarının tam olmasından sorumludur.

Kullanıcı, İEÜ tarafından kendisine tahsis edilecek her türlü kod, şifre, cep telefonu, bilgisayar, tablet, manyetik kart ve benzeri malzemeleri İEÜ’nün belirlediği ve belirleyebileceği amaçlar için kullanmalıdır. Kullanıcı, İEÜ tarafından sağlanan internet hizmetini ve İEÜ’nün mülkiyetinde olan elektronik posta (e-mail) iletişimini sadece iş amaçlı olarak kullanabilir.

İEÜ; bilgisayar veya İEÜ sistemlerine otomatik olarak kaydedilen e-mail iletişimini ve İEÜ tarafından tahsis edilen bilgisayar, tablet, cep telefonunu, ve benzeri donanımı haber vermeksizin denetleyebilir. Kullanıcı konu ile ilgili İEÜ talimatlarına aynen uymalıdır. İEÜ; mülkiyeti İEÜ’ya ait olan tüm donanım ve iletişim ağı üzerinde denetleme yapma hakkına sahiptir. Kullanıcı; ilgili hakkın kullanımının kişisel haberleşme özgürlüğüne müdahale teşkil etmediğini peşinen kabul etmektedir.

Hukuki süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla, İEÜ tarafından uygun görülen sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki

veri akışın iz kayıtları ajanlı veya ajansız iz toplama yöntemleri kullanılarak toplanılabilmektedir. İlgili faaliyetler; kişisel işlemler ile alakalı olarak kullanılmış olsa bile, şahsi bilgi olarak kabul edilmemektedir ve kullanıcılar her zaman denetime açık olduğunu bilerek işlemlerini yürütmelidirler.

Kullanıcı; 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan; intihara yönlendirmeye, çocukların cinsel istismarına, müstehcenliğe, fuhuşa, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırmaya, şiddet ve intihara yönlendirmeye, sağlık için tehlikeli madde teminine, kumar oynanması için yer ve imkan sağlamaya yönelik internet sitelerine girmemeli, devlet büyüklerine hakaret etmesi ve gazete, forum ve benzeri sitelerde İEÜ'yu küçük düşürücü ve kamuoyunu yanıltmaya yönelik yorumlar ile özel hayatın gizliliği, kişilik hakkının korunması ve kişisel verilerin korunmasına ilişkin suç oluşturabilecek nitelikteki bilgi ve işlemleri İEÜ'nün internet hattı üzerinden yapması durumunda cezai ve hukuki sorumluluğun tarafına ait olduğunu bilmelidir.

Kullanıcı, İEÜ'nün sunucuları üzerinde şahsına tahsis edilen kullanıcı kodu/şifre ikilisi ve/veya IP (Internet Protocol) adresini kullanarak gerçekleştirdiği her türlü etkinlikten, İEÜ bilişim kaynaklarını kullanarak oluşturduğu ve/veya kendisine tahsis edilen İEÜ bilişim kaynağı üzerinde bulundurduğu her türlü kaynağın (belge, doküman, yazılım vb.) 5651 Sayılı Kanun uyarınca içerik sağlayıcı sıfatıyla içeriğinden sorumlu olduğunu bilmelidir.

Kullanıcı, tarafına teslim edilmiş elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılım, donanım, araç ve gereç üzerinde İEÜ'nün bilgisi dışında hiçbir mekanik ya da yazılımsal yapılandırma değişikliği yapmamalıdır.

Kullanıcı, kendisine iş amaçlı tahsis edilen bilgisayara İEÜ tarafından yüklenmiş işletim sistemi ve uygulama yazılımları dışında herhangi bir işletim sistemi veya lisanssız yazılım yüklememelidir. İEÜ tarafından yüklenmemiş yazılımlardan doğacak her türlü hukuki sorumluluk kullanıcı sorumluluğundadır.

Kullanıcı, bilgisayarında kendisine verilen "kullancı adı" ve "şifre" ile oturum açmalı, çalışması bitince, oturumu veya bilgisayarı kapatarak bilgisayara başkalarının fiziksel erişimine fırsat vermemelidir. Bilgisayarının başından kısa süreli ayrılmalarında bilgisayar oturumunu kilitlemelidir.

Kullanıcı, İEÜ tarafından tahsis edilen bilgisayar, cep telefonu, tablet, intranet ve internet ortamında yer alan İEÜ ve işle ilgili her türlü veri, bilgi ve belgeyi; flash memory, external hard disk gibi veri saklayıcılarla, donanımlarla ve yazılı, basılı veya dijital alt yapı gibi yöntemlerle İEÜ'ya bilerek veya bilmeyerek zarar verme amacı ile kurum dışına çıkarmamalıdır. Sahip olduğu kişisel sair bir mail adresine yönlendirmemelidir. Bilgi ticareti yapmamalıdır.

Kullanıcı, sosyal medya sitelerindeki kişisel hesaplarını kullanırken İEÜ'ya zarar vermeye yönelik paylaşımlarda ve İEÜ ile veya kendisinin İEÜ nezdindeki pozisyonu ile ilgili yanıltıcı beyan ve açıklamalarda bulunmamalıdır.

2.4. Konfigürasyon ve Güvenlik Ayarları

Kullanıcılar teknik olarak mümkün olsa bile bilgisayarlardaki güvenlik ayarlarının düzeyini kesinlikle düşürmemelidir. Kullanıcılar bilgisayarlar üzerinde yeni kullanıcı oluşturamaz ve mevcut kullanıcıların hakları ve kullanıcı gruplarını değiştiremez. Eğer iş ihtiyaçları gereği konfigürasyon ve güvenlik ayarlarının değiştirilmesi gerekiyor ise yazılı olarak BTD onayına başvurulur. Konfigürasyon ve güvenlik ayar değişiklikleri BTD tarafından yapılmalıdır.

Virüslere ve zararlı yazılımlara karşı güvenliğin sağlanabilmesine yönelik olarak aşağıdaki önlemler alınmalıdır.

- Kullanılan bilgisayarda hazırlanmamış her tür bilgi teknolojileri medyası (CD, DVD, USB vb.) virüs kontrolü yapıldıktan sonra kullanılmalıdır.
- İEÜ' da BTD tarafından merkezi yönetilen bir virüs programı bulunmaktadır.
- İlgisiz ya da şüpheli mesajlar açılmamalı ve bilgisayardan silinmelidir. Şüpheli durumlarda BTD bilgilendirililebilir.

2.5. İEÜ'ya Ait Olmayan Cihazlar

İEÜ'ya ait olmayan cihazlar sadece iş gereği ve BTD onayı ile İEÜ ağına bağlanabilirler. BTD personeli, 3. parti çalışanları İEÜ ağına izinli olarak bağlayabilir. İEÜ'ya ait olmayan cihazlarda BTD teknik kontroller uygulama ve ayar değişiklikleri yapma / yaptırma hakkına sahiptir. Lisansız işletim sistemi, zararlı yazılım bulunduran cihazların İEÜ ağına bağlanmalarına izin verilmez. Tespit edilmesi durumunda ağ erişimi kaldırılır.

2.6. Ofis Araç Gereçlerinin Fiziksel Güvenliği

Sistem odaları içerisindeki cihazlarının yakınında yiyecek, içecek gibi gıda maddeleri tutulamaz. Kullanıcıların doğrudan sorumluluğunda veya ortak kullanımda olan bilgisayarlar ve diğer ofis araçlarını olumsuz etkileyebilecek çevresel etkenler (sıcaklık, nem, aşırı toz, v.b. gibi) BTD' ye bildirilmelidir.

2.7. Güvenlik Olay ve Zafiyetlerinin Raporlanması

Kullanıcılar günlük işlerini yaparken güvenlik olaylarına ve zafiyetlerine karşı duyarlı olmalıdır. Fark edilen her zafiyet, riskin gerçekleşmesi zayıf bir olasılık olsa bile en kısa zamanda BTD' ye bildirilmelidir.

Bu duruma örnek olarak;

- Kullanıcı bilgisayarlarında virüs bulunmasından şüphelenilmesi,

- Kullanıcı parolasının başkaları tarafından öğrenilmiş olmasından şüphelenilmesi veya erişim araçlarının (VPN, fiziksel geçiş kontrol kartı, vb.) kaybedilmesi / çalınması,
- Dizüstü, telefon veya tablet kaybedilmesi / çalınması,
- Erişim kontrollerindeki zafiyet, davetsiz ve şüpheli misafir,
- Kullanıcı girişinin reddedilmesi ve hizmet kesintisi gibi beklenmeyen durumlar verilebilir.

Dizüstü, telefon ve tabletlerin, kritik öneme sahip dokümanların ve veri saklama cihazlarının kaybı veya çalınması durumunda en kısa zamanda BTD bilgilendirilmelidir.

3. HESAP VEREBİLİRLİK

3.1. Hesap Verebilirlik

Kullanıcıya atanmış erişim araçları hiçbir şart altında teknik personel dahil kimseyle paylaşılamaz. Erişim araçlarına örnek olarak; parola, VPN, fiziksel geçiş kontrol kartı, vb. verilebilir. BTD hiçbir zaman kullanıcılardan şifrelerini ve PIN kodlarını söylemelerini, yazılı iletmelerini, fiziksel araçlar için vermelerini (görevden ayrılma durumu hariç) isteyemez. Eğer kullanıcılar erişim ile ilgili konularda destek için telefon ile iletişim kuruyorsa, özellikle karşı tarafın araması durumunda, arayan kişinin kimlik doğrulamasını yapmalıdır. Şüpheli telefon aramaları veya mesajlar, edinilmesi mümkün olan detay bilgiyle birlikte BTD' ye bildirilmelidir.

3.2. Kullanıcı Kimliği

Kullanıcıların İEÜ sistemleri üzerinde kendilerine ait olmayan kullanıcı kodlarını (veya genel anlamıyla kimliklerini) kullanmaları, kullanıcı kimliklerini çeşitli yöntemlerle gizlemek amacıyla jenerik kullanıcı olarak sisteme erişmeleri yasaktır. Bu çerçevede e-posta iletilerindeki gönderen kısmında bir kimlik bilgisi bulunmaktadır ve bu alanın yanıltıcı biçimde değiştirilmesi yasaktır.

İEÜ' da iş sürekliliği gereği jenerik ortak kullanılan hesaplara izin verilmektedir. Bu hesaplar BTD tarafından periyodik olarak izlenmekte,kayıtları tutulmakta ve aksi bir durum belirtilmedikçe belirli sürelerde otomatik olarak kapatılmaktadır.

3.3. Parola (Şifre) Kriterleri

İEÜ sistemleri, teknik olarak mümkün olan durumlarda, parola karmaşıklık ve değişiklik kontrollerini teknik olarak uygulayacak biçimde yapılandırmaktadır. Kullanıcılar parola kriterlerinin teknik olarak zorlanmasının mümkün olmadığı durumlarda aşağıdaki belirtilen kriterlere uymakla yükümlüdür.

- Minimum şifre uzunluğu 8 karakter olmalıdır.
- Şifre yapısı; alfanümerik, büyük ve küçük harfler ve en az bir özel karakter (bunlardan en az üçü sağlanmalıdır) şeklinde olmalıdır.
- Şifre oluşturulurken başkaları tarafından kolay tahmin edilebilecek tarih, isim ve benzeri tanımlar kullanılmamalıdır.
- Şifre girişi sırasında başkalarının izlemediğinden emin olunmalıdır.
- Kullanıcıların EkoID, OASIS dahil İEÜ tarafından sağlanan tüm şifreleri, internet ortamında başka amaçlarla kullanılan şifrelerle aynı olmamalıdır.
- Kullanıcı şifresi kişiye ve yetkiye özeldir ve başkaları ile paylaşılmamalıdır.
- Bilgisayar başında bulunulmayacağı durumlarda bilgisayarlar kullanıcı tarafından kilitlenmeli veya bilgisayar kapatılmalıdır.

3.3.1. Parolaların (Şifrelerin) Kullanımı

Kullanıcı, işiyle ilgili olarak kendisine verilen, kartlı ya da kartsız her türlü şifrenin ve bilginin gizliliğinden ve korunmasından sorumludur. Kullanıcı, her ne sebeple olursa olsun, şifresini/kartını başkasına vermemeli ve kullandırmamalıdır. Kullanıcının şifresi ile verdiği onaylar imzası yerine geçer ve şifresiyle verilen onaylardan imzası ile yapılmış gibi sorumlu tutulabilir. Kullanıcı, şifresi ile İEÜ içine ve dışına gönderdiği tüm bilgilerden şahsen sorumludur.

Kullanıcı, şifresinin başkaları tarafından kullanılması, onay verilmesi, işlem yapılması, İEÜ içine ve dışına bilgi gönderilmesi ya da kendisine verilen yetkiyi kötüye kullanması sonucunda, İEÜ'nün uğrayacağı her türlü zararlardan tamamen sorumludur.

4. İNTERNET KULLANIMI

4.1. Kurumsal ve Kişisel Bilgilerin İnternet Üzerindeki Web Sitelerine Verilmesi

Kullanıcılar internet üzerindeki her hangi bir sisteme veya siteye iş gereksinimleri ve kanuni gereklilikler dışındaki durumlarda (tartışma gruplarına, sohbet odalarına, sosyal medya, alışveriş siteleri, vb.) İEÜ e-posta adresi ile üye olmamalıdır, kurumsal ve kişisel bilgileri paylaşmamalıdır.

4.2. İnternetten Dosya İndirme

Kullanıcılar iş gereksinimleri için internetten veri dosyaları indirebilir, ancak bu işlemden önce anti-virüs imzaları ve işletim sistemi yamalarının güncelliğini kontrol etmelidir.

4.3. İnternet Üzerinden Peer to Peer – P2P Ağ Oluşturma ve Dosya Paylaşımı

İnternet üzerinden P2P ağlara katılım ve dosya paylaşımı yasaktır. Eğer internet üzerinden P2P ağ oluşumu veya dosya paylaşımı iş amaçları için gerekli ise, BTD onayı ile yapılabilir.

5. MESAJLAŞMA KULLANIMI

5.1. İzin Verilen Mesajlaşma Çözümleri

İş amaçlı kullanılabilecek mesajlaşma çözümleri, İEÜ e-postası ve anında mesajlaşma sistemleridir. İEÜ' da 3 farklı domain ("İEÜ.edu.tr", "iue.edu.tr" ve "izmirekonomi.edu.tr") bulunmaktadır. Örnek; Her İEÜ kullanıcısına adı.soyadı@İEÜ.edu.tr, öğrencilere adı.soyadı@std.İEÜ.tr, mezun öğrencilere adı.soyadı@alu.İEÜ.edu.tr formatlı bir e-posta adresleri verilmektedir.

İEÜ'da Rektör ve/veya Genel Sekreter ve Bilgi Teknolojileri Direktörülüğünün onayı ile İEÜ avukatlarına, mütevelli heyeti üyelerine, vb. dış kullanıcılara "İEÜ.edu.tr" uzantılı e-postalar verilebilmektedir.

Emeklilik veya istifa yolu ile ayrılan çalışanlar ayrılış tarihleri itibariyle İEÜ domainleri uzantılı e-posta hesabının şifresi BTD tarafından değiştirilir. En az 15 gün sonunda hesap kapatılır. Kullanıcının talebi doğrultusunda 1 ay süre ile harici e-posta adresine yönlendirilme DYS üzeriden gelecek talep doğrultusunda yapılabilmektedir.

5.2. E-posta Kullanımı

Elektronik mesajlaşma kuralları, yazılı ve yüz yüze olmak üzere aynı özellikleri taşırlar. Yüz yüze iletişimin mümkün olmadığı durumlarda elektronik mesajlaşma kullanılır. Adres listesinde yer alan gruplara mesaj gönderilirken alıcıların tamamının gönderilecek mesajı almak isteyeceğinden emin olunmalıdır. Mesajın doğrudan muhatabı ve gerekiyor ise aksiyon alması gereken kişiler "TO/KİME" alanına, bir aksiyon alması gerekmeyen ve sadece bilgilendirme amacı ile mesaj gönderilen kişiler "CC/BİLGİ" alanına yazılmalıdır. Mesajlara eklenecek dosyaların büyüklükleri önemlidir. Özellikle grafikler ve resimler çok yer tutacağından dikkat edilmeli ve mümkünse

göndermeden önce sıkıştırılmalıdır. Elektronik mesajlar için belirlenmiş sınır 10 Mb'dır. Bu büyüklüğü geçen elektronik mesajlar yollanamayacak ve alınamayacaktır.

10 Mb üstü ekli e-posta gönderimleri için İEÜCloud yapısı kullanılabilir.

5.3. Mesajlaşma Mahremiyeti

İEÜ ile bağlantılı sistem ve alt yapılarda kullanılan anlık mesajlaşma sistemleri üzerinden yapılan tüm elektronik iletişimin kişiye özel olacağı garantisi verilemez. Kullanıcılar elektronik ortamdaki her türlü iletişimlerinin kötü niyetli kişilerin saldırılarına maruz kalabileceğini bilmelidirler. Bu nedenle kritik kurum bilgilerini içeren iletişimin, hem iletişim hattında hem de ulaştığı alıcı noktasında gizlilik ve bütünlüğünün korunabilmesi için şifreleme yöntemleri ile yapılması kesinlikle önerilmektedir. Kullanıcılar gizlilik ihtiyacı olan iletişimleri için teknik çözüm konusunda BTD'ye başvurabilirler.

5.4. Kimlik Hırsızlığı (Phishing) Saldırıları, Mesaj Ekleri Politikası, İstenmeyen (Spam) E-postalar ve Yasak Kullanımlar

İEÜ, kurum kullanıcılarının e-posta adreslerine gelen istenmeyen e-posta ve virüs eklentilerine karşı teknik önlemler uygulamaktadır. Buna rağmen son kullanıcılar saldırı yöntemlerinin yeni olması ya da korunma yöntemlerinin hatalı çalışabilmesi veya bazı durumlarda bu yöntemlerin bazı saldırılara karşı yetersiz kalmaları sebebi ile genel e-posta güvenlik kurallarına uymalıdır. Kullanıcıların;

- Kişileri rahatsız edici, müstehcen, politik ve dini propaganda yapan veya kurumsal değerlere aykırı içerikler taşıyan elektronik mesajları yaratmak veya dağıtmak ve bu sitelerdeki diyaloglarda yer almak
- İnternet aracılığı ile rastgele, tehdit edici ve saldırgan yazı / mesaj göndermek
- Şans mektupları veya zincir mektuplarını içeren mesajları yaratmak veya dağıtmak
- Telif hakkı yasalarına uygun olmayan bilgileri içeren mesajları ve eklerini oluşturmak veya dağıtmak
- Kaynağının izni olmadan bir mesajı ve ekini değiştirerek veya kopyalayarak dağıtmak
- Şifre güvenliğine aykırı olarak şifrelerin herkes tarafından görülmesini sağlamak

yasaktır.

Bunlara ek olarak, e-posta içinde gelen bağlantılara tıklayarak (EkoID, OASIS ve parolası başta olmak üzere) kişisel bilgilerini girmemeli, HTML formatında gelen e-postalardaki resimleri görüntülemek için indirmemeli, e-posta içindeki herhangi bir bağlantıya tıklamamalı, güvenilir kaynaklardan gelmeyen e-postalardaki eklentileri indirmemeli ve gönderen kısmındaki bilginin yanıltıcı olabileceğini unutmamalıdır.

E-posta içindeki herhangi bir bağlantıya tıklamak veya e-posta içindeki resimleri görüntülemek üzere indirmek, istenmeyen e-postanın varolan bir kullanıcıya ulaştığı bilgisini saldırgana verir. Ayrıca resim indirme veya linki ziyaret etme işlemi resim işleyici uygulamalardaki açıklardan dolayı bilgisayarınızın zarar görmesine veya "Cross Site Scripting – XSS" adı verilen istemci tarafında çalışan betiklerin kötü niyetle kullanılmasına ve oturum hırsızlığı saldırılarına imkan verebilir.

Elektronik mesajlaşma politikaları İEÜ Bilgi Güvenliği Yönetim Komitesi tarafından yayınlamıştır. Bu politikalara uyulmaması durumunda ilgili kişi ve yöneticileri İEÜ Bilgi Güvenliği Yönetim Komitesince uyarılacak ve tekrarı halinde kişi hakkında idari işlem yapılacaktır.

6. OFİS EKİPMANLARI, BASILI DOKÜMANLAR VE TAŞINABİLİR VERİ SAKLAMA ARAÇLARI

6.1. Yazıcılar ve Fotokopi Makineleri

Kullanıcılar gizlilik gereksinimi yüksek bir dokümanı yazdırırken, bilginin yetkisi olmayan kişiler tarafından görülmesini veya ele geçirilmesini engellemek için yazdırma esnasında yazıcının yanında bulunmalıdır. Kullanıcılar, gizlilik gereksinimi olsun veya olmasın makineye sıkışmış dahi olsa orijinal ve kopya doküman nüshalarını yazıcı ve fotokopi makinelerinde terk etmemelidirler. Telif hakkı İEÜ'ya ait olmayan dokümanların İEÜ yazıcı ve fotokopi makinelerinde çoğaltılması yasaktır. Yazıcı ve fotokopi makinelerinin kişisel kullanımı yasaktır.

6.2. İhtiyaç Kalmayan Basılı Dokümanların İmha Edilmesi

İmha edilecek tüm hassas, gizlilik içeren dokümanlar, doküman parçalayıcı makine (shredder) ile parçalanmalıdır. Gizlilik gereksinimi olmayan diğer dokümanlar ofis içi veya dışında rastgele bölgelerde bırakılmamalı ve kağıt atık geri dönüşüm kutularına atılmalıdır.

6.3. Faks Makineleri / Sistemleri

Kullanıcılar yüksek düzeyde gizlilik gereksinimi olan bilgilerin gönderiminde, verinin açıkta gönderildiği ve hedef noktaya ulaştığında açık olarak görüntülenen teknolojileri tercih etmemelidir. Faks kullanımına imkan tanıyan veya faks kullanımını zorunlu kılan durumlarda şu kontroller uygulanmalıdır:

- Hassas dokümanlar (Kişilere Özel ve Gizli) alıcı tarafından alıcı cihazın başında beklenmesi durumunda gönderilmeli, otel veya postane gibi yerlerden mümkünse

gönderilmemelidir. Eğer gönderilmesi gerekiyorsa hizmet personeline teslim edilmemelidir.

- Hassas bilginin iletildiği bilgisi en kısa zamanda teyit edilmelidir.
- İmza içeren veya talimat nitelikli dokümanların kabulü durumunda mutlaka orjinal nüshaları alınmalıdır. (orjinal nüshaların takibi gereksinimi elektronik olarak taranmış dokümanlar için de geçerlidir).

6.4. Taşınabilir Veri Saklama Araçları

Taşınabilir olmaları nedeniyle çalınma tehdidiyle karşı karşıya olan taşınabilir veri saklama araçlarının, özellikle kritik veri barındırmaları durumunda fiziksel güvenliği kullanıcıların sorumluluğundadır. Verinin saklanma ihtiyacı sona erdiğinde veriler saklama cihazından silinmeli, CD gibi tek kullanımlık medyaların kullanımı durumunda medya imha edilmelidir.

7. İZLEME VE KAYIT AKTİVİTELERİ, MAHREMİYET

7.1. İEÜ Sistemlerinde Saklanan veya İEÜ Sistemleri Aracılığı ile İletilen Verilerin Mahremiyeti

İEÜ, kendi sistemleri üzerinde saklanan ve İEÜ sistemleri aracılığı ile iletilen tüm bilgileri inceleme hakkını saklı tutar. Kullanıcılar, İEÜ sistemleri üzerinde saklanan veya İEÜ sistemleri aracılığı ile iletilen kişisel bilgileri hakkında mahremiyet beklentisi içinde olmamalıdır.

7.2. Kayıtlar

İEÜ, iç ve dış saldırılara karşı katmanlı güvenlik anlayışını benimsemektedir. Kullanıcılar için sistem giriş logları, erişim logları, kullanıcı aktivite logları, gerekli olan sistemlerde tutulmaktadır.

Kullanıcılar, İEÜ sistemleri üzerinde veya İEÜ sistemlerini kullanarak yasal mevzuata veya kurum içi kurallara aykırı davranışlarından şüphe edilmesi halinde İEÜ BTD kullanıcıların bilgi sistemleri üzerindeki faaliyetlerini izleyebilir.

8. GENEL VERİ KORUMA VE SINIFLANDIRMA SORUMLULUKLARI

8.1. Gizlilik, Kişisel Verilerin Korunması ve Paylaşım İzni

Kullanıcı, işinin ifası sırasında edindiği İEÜ'ya, iştiraklerine, bağlı şirketlerine, yöneticilerine, diğer çalışanlarına, iş ortaklarına ya da öğrencilerine ait ticari, teknik, hukuki, finansal her türlü bilgi ve belge ile

bilgi teknolojileri kapsamındaki her türlü bilginin ve tüm kaynakların, İEÜ'nün çalışmaları sırasında oluşturduğu veya geliştirdiği veya diğer yasal yollarla elde ettiği, ticari, sınai, fikri ve ekonomik sırlar ve bilgiler başta olmak ve bunlarla sınırlı olmamak kaydı ile her türlü bilginin gizli bilgi niteliğinde olduğunu bilmelidir, gizli bilgileri hiçbir şekilde kendisi veya üçüncü şahıslar için menfaat sağlamak üzere kullanmamalıdır, işi gereği izin verilen veya yasal olarak zorunlu olan durumlar haricinde üçüncü şahıslara vermemeli, kopyalamamalı, çoğaltmamalı, işyeri dışına çıkartmamalı veya üçüncü şahıslarca kopyalanmasına, çoğaltılmasına veya kullanılmasına olanak verecek hiçbir eylemde bulunmamalıdır. Kullanıcı, bu çerçevede gizli bilgilerin bunlara sahip olmaması gereken kişilerin eline geçmemesi için makul ve gerekli olan tüm tedbirleri almalıdır. Kullanıcı bilgi talebi konusunda üçüncü kişilerin ısrarı ile karşı karşıya kalması durumunda konuyu yöneticisine raporlamalıdır.

Yukarıda belirtilen gizlilik yükümlülükleri, İEÜ ile kullanıcı arasında mevcut iş sözleşmesi sona erdikten sonra dahi süresiz olarak yürürlükte kalmaya devam eder.

İEÜ, Kullanıcıya ait kişisel verilerin gizliliği, bütünlüğü ve korunmasından sorumlu olup, bu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alır. İEÜ, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. İEÜ ve kişisel veri işleyen ilgili departmanları, iştirakleri ve sözleşme ilişkisi içinde bulundukları üçüncü taraflar öğrendikleri kişisel verileri mevzuata aykırı olarak başkasına açıklamamalı ve işleme amacı dışında kullanmamalıdır. İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, İEÜ bu durumu en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kurulu'na bildirmelidir.

Bu maddede yer alan Veri Paylaşım İzni ile sözleşmeli olarak çalışmakta olan Kullanıcı, İEÜ tarafından ilgili mevzuata istinaden işlenen kişisel verilerinin, 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan, genel ilkelere ve kişisel veri işleme şartlarına uygun olarak İEÜ tarafından;

- iştirakler tarafından yapılacak çeşitli bilgilendirmelerde,
- İEÜ içi yapılacak toplantı, davet gibi organizasyonlarda,
- üst yönetime yapılacak raporlama ve analizlerde,
- çeşitli insan kaynakları uygulamalarında,
- hayat sigortası başvuru işlemlerinde,
- kurum içi acil tıbbi yardımlarda,

• kampanya, pazarlama, tanıtım, reklam, promosyon, hediye, indirim gibi lehine sağlanacak faydalar ve sair katma değerli hizmetler sunulması amacıyla İEÜ ve iştirakleri ile yurt içi veya yurt dışı sözleşme ilişkisi ile çalışılan üçüncü kişilerle paylaşılmasına, bu amaçlarla sms, mail, telefon, e-posta ve sair iletişim yöntemleriyle kendisiyle iletişime geçilmesine,

• yasal olarak kişisel verilerini talep etme hakkına sahip kamu kurum ve kuruluşlarıyla paylaşılmasına,

• İEÜ tarafından işlenen kişisel verilerinin İEÜ tarafından kurulan ortak veri tabanında, bilgi güvenliği ve kişisel verilerin korunmasına ilişkin standartlar ve mevzuata uygun olarak tutulmasına,

• Kişisel verilerinin iş akdi sona erse veya işten yasal olarak ayrılması gerekse dahi, İEÜ tarafından yasal yükümlülüklerinin yerine getirilebilmesi amacıyla, kanunların öngördüğü veya veri işleme amacının gerekli kıldığı süre boyunca veya İEÜ'nün meşru menfaatinin söz konusu olduğu durumlarda herhangi bir süre ile bağlı olmaksızın saklanacağına kullanıcı açık rıza göstermeli ve işbu Kişisel Veri Paylaşım İzninin iş akdinin ayrılmaz bir parçası olduğunu kabul, beyan ve taahhüt ederek faaliyetlerini bu doğrultuda sürdürmelidir.

Kullanıcı; 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun md. 10 ve 11 uyarınca, https://www.İEÜ.edu.tr/tr/kisisel-verilerin-korunmasi adresinden iletilen başvuru yöntemleri ile her zaman İEÜ tarafından işlenen kişisel verilerine erişme, veri işlemeye ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme, ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerinin silinmesini veya yok edilmesini talep etme, düzeltme veya silinme hakkını kullandığına ilişkin bilginin kişisel verilerin aktarıldığı iştiraklere veya yurt içi-yurt dışı çalışılan üçüncü taraflara bildirilmesini talep etme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahiptir.

Kullanıcı, Sözleşme müzakereleri ve Sözleşme ilişkisi sırasında, akademik görevi ve/veya üstleneceği idari görevler ve diğer tüm görevleri nedeniyle İEÜ'nün faaliyetleri ve yönetsel işleyişiyle ilgili olarak öğrendiği veya kendisine verilen gizli bilgiler ve ticari sırlar ile niteliği itibarıyla İEÜ'nün gizli kalmasını bekleyeceği yönetsel işleyişe ilişkin bilgileri, Sözleşme'nin herhangi bir nedenle sona ermesinden sonra dahi, hukuksal zorunluluklar ve akademik veya idari görevi gereği paylaşılanlar hariç olmak üzere, İEÜ'nün yazılı izni olmadan ifşa etmemeyi ve ifşa edilmemesi veya erişilmemesi için gerekli tedbirleri almayı ve gayret göstermeyi kabul ve taahhüt ettiğini bilmelidir.

Kullanıcının çalışması, görevi veya ek görevleri sırasında İEÜ'nün işleriyle ilgili olarak ürettiği veya kendisine İEÜ tarafından temin edilen tüm notlar, bilgi notları ve sair kayıtlar (bilgisayar yazılım programlarına kaydedilmiş olanlar da dahil olmak üzere) İEÜ'ya aittir ve İEÜ tarafından talep edildiği zamanlarda veya

Sözleşme'nin feshedilmesi halinde, gecikmeksizin İEÜ'ya iletilecek ve mevcut kopyaları ile suretleri kalıcı olarak imha edilmelidir.

Kullanıcı, görevi nedeniyle kendisine ve bağlı bulunduğu birime teslim veya zilyetliğinde bulunan her türlü eşya, demirbaş, her türlü mefruşat, elektronik teçhizat vb. ilgili olarak gerek Medeni Kanunda gerekse Türk ceza Kanununda düzenlenen sorumluluklardan bilgi sahibidir. Bu eşyaların muhafazasından, hasar ve ziyan görmemesinden sorumlu olacağını bilmelidir.

8.2. Bilgi Paylaşımı, Veri Sahipliği ve Sınıflandırılması

Kurum içi bilgi paylaşımı sadece görev gereği ilgili veriye ulaşması gereken kullanıcılar arasında olabilir. Kamu kurumları ve üyeler ile bilgi paylaşımı bu irtibat görevini yerine getirmek üzere atanmış personel tarafından gerçekleştirilmelidir.

Kullanıcılar kendileriyle ilgili iş verilerinin sahibi olup, bu varlıkların korunmasından nihai olarak sorumludur. Veri sahipleri kendileriyle ilgili iş verilerinin sınıflandırılmasından ve gerektiğinde yeniden sınıflandırılmasından sorumludur. Verinin elektronik ortamda saklanabileceği gibi, basılı doküman halinde de saklanabileceği unutulmamalıdır.

8.3. Kurumsal Verinin Saklanması

Kullanıcılar sahibi oldukları iş verilerinin yasal yükümlülükler veya iş gereklerinden doğan saklanma süre ve şart ihtiyaçlarını BTD' ye bildirmekle yükümlüdür. Genel prensip olarak üzerinde çalışılan dosyalar ve kritik olmayan dosyalar iş bilgisayarlarında saklanabilir. Ancak kritik ve önem seviyesi yüksek olan dosyalar üzerinde çalışılmadığı durumlarda iş bilgisayarlarına ek olarak fileserver, vb. sistemler üzerinde yedeklenmeli ve saklanmalıdır. Kullanıcılar ortak paylaşım alanları dışındaki verilerinin güvenliğinden ve yedeklenmesinden sorumludur.

8.4. İEÜ Mobil Cihazlar

Kullanıcılar, hassas kurum verilerini İEÜ dizüstü bilgisayarlarında ve mobil cihazlarında saklamaktan kaçınmalıdır. Bu cihazların kullanıcıları özellikle halka açık mekanlarda cihazlarını terk edemez ve cihazların fiziksel güvenliğini sağlamakla yükümlüdürler. Kullanıcılar kendilerine tahsis edilen dizüstü bilgisayarları kullanmadıkları durumlarda kilitli dolap veya çekmecelerde saklamalıdırlar. Uçak, otobüs gibi halka açık ulaşım araçlarında taşınabilir cihazlar baş üstü bagajlarına değil koltuk altına konulmalıdır. Havaalanı, tren ve otobüs garlarında taşınabilir cihazları güvenlik kontrollerinden geçirilirken sürekli olarak izlemeli ve göz teması kesilmemelidir. Taşınabilir cihazlar İEÜ'ya uzaktan erişim için kullanılıyorsa, erişim için kullanılan kullanıcı adı ve parola bilgileri bilgisayar üzerinde herhangi bir dosya içinde saklanmamalıdır.

8.5. İEÜ Ofisi Dışına Gönderilen Bilgisayarlar ve Veri Saklama Araçları

Eğer iş bilgisayarları, cihazlar veya bu cihazlara ait depolama birimleri tamir veya hibe amacı ile kurum dışına gönderilecekse, bu cihazların kullanıcıları ve BTD bilgisayar üzerinde bulunan hassas verilerin silinmesi ve gerekiyorsa yazılı talep doğrultusunda; yedeklenmesinden nihai olarak sorumludur.

8.6. İEÜ Ağına Uzaktan Erişim

İEÜ ağına uzaktan erişmesi gereken kullanıcılar erişim için İEÜ VPN alt yapısını kullanmalıdır. Kullanıcılar uzaktan erişim araçlarını (VPN) koruma konusunda diğer erişim araçlarının korunmasına nazaran daha üstün hassasiyet göstermelidir. Uzaktan erişim kimlik doğrulama için kullanılan cihazların üzerine İEÜ veya kullanıcıyla ilgili bir erişim bilgisi (telefon numarası, sunucu adı, IP adresi, kullanıcı kodu, vb.) yazılmamalı / yapıştırılmamalıdır. Halka açık bilgisayarların uzaktan erişim için kullanımı her koşulda yasaktır.

İEÜ dışından, İEÜ sistemine herhangi bir üçüncü partinin uzaktan erişmesi gerekiyor ise BTD onayı dâhilinde süreli/süresiz ve sadece ilgili sunuculara ait VPN erişimi tanımlanmalı ve gizlilik sözleşmesi imzalanmış olmalıdır.

8.7. Temiz Masa, Temiz Ekran Politikası

Kullanıcılar masaları başında olmadıklarında hassas bilgi içeren basılı dokümanları masa üstünde bırakmamalıdırlar ve bilgisayar ekranlarını açık terk etmemelidirler. Hassas bilgi içeren basılı dokümanlar kullanılmadıklarında masadan kaldırılmalı ve gerekiyorsa kilit altında tutulmalıdır. Kullanıcılar kurum dışında basılı doküman, bilgisayarlar ve veri saklama cihazlarının fiziksel güvenliği konusunda kurum içerisine göre daha hassas davranmalı, asla kontrolsüz biçimde açıkta bırakmamalıdır. Kurum dışında bilgisayar ekranından veya basılı dokümanlardan hassas bilgilerin başkalarınca izlenme riskinin daha yüksek olduğu unutulmamalı, halka açık mekânlarda hassas bilgiler görüntülenmemelidir. Restoranlar ve bina içerisindeki ortak alanlar gibi halka açık mekânlarda iş ile ilgili konular konuşulurken dikkat edilmeli ve başka kişilerin duyabileceği durumlarda konuşma yapılmamalıdır.

8.8. Telefon Görüşmeleri

İEÜ çalışanları özellikle şirket dışında hassas bilgi içeren telefon görüşmesi yapmamaya gayret etmelidir. Hassas bilgilerin iletişimini gerektiren bir görüşme yapılması gerekiyorsa, cep telefonları diğer şahıslara / kurumlara ait telefonlara, kapalı ve yalnız bulunulan mekanlar açık ve kalabalık mekanlara tercih edilmelidir. Gelen aramalarda arayanın kimliğinden emin olunamaması halinde

ya da kritik bilgilerin dağıtımını güvence altına almak için geri arama yapılarak arayanın kimlik doğrulaması yapılmalıdır.

Bu politikalara uyulmadığı tespit edildiğinde ilgili kişi ve yöneticileri İEÜ Bilgi Güvenliği Yönetim Ekibi tarafından Disiplin Yönetmeliği kurallarına bağlı kalınarak uyarılacak ve tekrarı halinde kişi hakkında idari işlem yapılacaktır.

9. KISALTMALAR VE TANIMLAR

Betik (Script)	Uygulamaları denetlemek için kullanılan bir programlama dilidir. Betikler doğrudan kaynak kodundan çalıştırılır. İlk betik dilleri genelde yığın dilleri veya iş denetim dilleri olarak adlandırılırdı. İlk betik dilleri geleneksel düzenle, derle, bağla, çalıştır işlemlerini kısaltmak için yaratılmıştı. Bu şekilde oluşturulmuş bir dosya doğrudan işletim sistemi komut satırından çağrılarak tek adımda ardışık komutlar çalıştırılabilir. Bu tür dosyalarda güvenlik açısından kullanıcı adı ve parola bilgisinin kayıtlı olmaması gerekir.
BIOS	Bilgisayarın yazılımlarını ve donanımlarını hazır hale getirir. Bu işleme booting denir. BIOS (Basic Input/Output System; Temel Giriş/Çıkış Sistemi), bilgisayarın ilk açılma işlevini yerine getiren yazılımdır. BIOS yazılımı bilgisayarda kuruludur ve bilgisayar açılırken bilgisayar tarafından işletilen ilk koddur ("önyükleme bellenimi- boot firmware"). BIOS' un temel işlevi işletim sistemini yüklemek ve başlatmak ve bilgisayarı diğer donanım ve yazılımların çalışmasına hazır hale getirmektir. Bilgisayar başlatıldığında BIOS' un ilk işi klavye, hard disk, CD/DVD sürücüsü, fare gibi sistem aygıtlarını tanımlamak ve kullanıma hazırlamaktır.
Cross Site Scripting - XSS	Bilgisayar güvenlik açığıdır. HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesi olarak tanımlanır. Genelde cross site scripting açıkları, saldırganın sistemi deneme-yanılma yaparak bulması ile ortaya çıkmaktadır. Açığın bulunması ile saldırgan, başka bir alan adından, açığın bulunduğu alan adı ve sayfanın bilgilerini, oturum ayrıntılarını ve diğer nesne değerlerini çalabilir.
P2P Ağ	Peer-to-peer ya da P2P olarak tanımlanır. Peer eş, denk demektir. İki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür. Eşler, sunucuları veya sabit bilgisayarlar tarafından merkezi koordinasyon ihtiyacı olmadan, işlemci gücü, disk depolama veya ağ bant genişliği gibi kendi kaynaklarının bir kısmını, doğrudan diğer ağ katılımcıları için kullanılabilir yapabilir. Sadece sunucuların tedarikçi ve istemcilerin tüketici olduğu geleneksel istemci-sunucu modelinin aksine eşler, hem tedarikçi hem de tüketicidir.
Internet Explorer Güvenlik Alanları (Security Zones)	Internet Explorer tüm web sitelerini dört güvenlik bölgesinden birine atar: Internet, Yerel intranet, Güvenilen Siteler ve Yasak Siteler. Bir web sitesine atanan bölge, bu site için kullanılan güvenlik ayarlarını gösterir. İnternet sitelerinin dinamik içerik sunma ihtiyacı ve tarayıcıların daha fonksiyonel olmaları amacıyla Applet, ActiveX, VBScript, Java Script vb. teknolojiler geliştirilmiştir. Ancak bu fonksiyonellik zaman içinde ortaya çıkan zayıflıklar kullanılarak kötüye kullanılmış / kullanılmaktadır.
İstenmeyen (Spam) E-posta	İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi Spam olarak adlandırılır. Spam çoğunlukla ticari reklam niteliğinde olup, bu reklamlar sıklıkla güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının, yarı yasal servislerin duyurulması amacına yöneliktir. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde mesajın alıcıları veya taşıyıcı, servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınır.
Jenerik / Ortak Hesap	Sistem yazılımları ve bazı sunucu ve uygulama yazılımları varsayılan kurulumları ile belli jenerik kullanıcıları erişim kontrolü için yaratır. Bu kullanıcı hesaplarına jenerik hesaplar denir. Genellikle yönetsel hakları olan bu tür kullanıcı kodları bazı

	durumlarda değiştirilebilir ve yönetsel haklar farklı kullanıcılara gerektiği ölçüde dağıtılabilir. Ancak bazı yazılımlar için bu mümkün değildir. Ortak hesap kullanımı aynı kullanıcı hesabının farklı kullanıcılar tarafından kullanılmasıdır. Bu durum hesap verebilirliğe zarar verir.
Koruma Duvarı (Firewall)	Ağ servisleri belli protokoller üzerinden, bu protokollerden ikisi olan TCP/UDP servisleri de belli portları kullanarak hizmet verir. Genel güvenlik prensibi olarak sadece gerekli sunucuların ve gerekli servislerin (protokol ve port tanımlarıyla) sunulması gerekir. Sadece gerekli servislerin sunulması, ağların güvenlik ihtiyaçlarına göre bölümlenmesi, sadece gerekli sunucuların (teknik olarak IP adreslerinin) hizmetlerine sadece istenen kullanıcılar tarafından ulaşımın sağlanması için bir kontrol cihazı (veya yazılımı) olarak koruma duvarları kullanılır. Koruma duvarları üzerlerinde diğer koruma önlemlerini de barındırabilmektedir (hizmet kesinti saldırılarına karşı koruma, saldırı tespit sistemlerini yanıltmaya yönelik yöntemleri bertaraf etme gibi). Koruma duvarları derinlemesine güvenlik yaklaşımına göre sadece bir katmanı oluşturur ve asla tek başına yeterli güvenliği sağlamaz.
Parola (Şifre)	Kimlik doğrulamada kullanıcı adına ek olarak kullanılan ve sadece kullanıcısı tarafından bilinmesi gereken karakterler bütünüdür.
Phishing (Yemleme)	Phishing (Yemleme) saldırısında amaç (kimlik bilgileri, kart numarası gibi) kişisel bilgilerin ele geçirilebilmesi olup, temelde bir sosyal mühendislik yöntemi olan sahte e-posta ve Web sayfalarının kullanılmasıyla gerçekleştirilir. Phishing'de dolandırıcılar, tüketicilere tanınmış bir firmadan geliyormuş izlenimi verilmiş bilgi güncelleme talebi vb. içeren e-postalar göndermektedir. Bu e-postalarda genellikle cevap için e-postanın içindeki linkin (Web sayfası için kısa yol) tıklanarak gerekli siteye geçilebileceği belirtilmektedir. Ancak, verilen talimat uygulandığında gidilen site dolandırıcılar tarafında hazırlanmış ve gerçeğini taklit eden sahte bir Web sayfası olmaktadır. Bu sahte sitede elde edilen bilgiler mahiyetine göre daha sonra çeşitli dolandırıcılık faaliyetlerinde kullanılabilmektedir. Phishing yönteminde bankaların kimliğinin kullanmasının yanında mağazalar veya e-ticaret kurumlarının ve İnternet servis sağlayıcıların kimliklerinin de kullanıldığı görülmektedir. Pharming adı verilen ve aynı amacı taşıyan bir diğer saldırı türü de DNS (İsim Sunucusu) sunucularının veya isim sorgularının yanıtlarının manipüle edilmesiyle kullanıcıların saldırgan tarafından düzenlenen bir siteye (kullanıcının bilgisi olmadan) yönlendirilerek kandırılması ve kişisel bilgilerinin çalınması şeklinde gerçekleştirilir.
Sanallaştırma (Virtualization) Yazılımları	Sanallaştırma yazılımları bir işletim sistemi yazılımını veya bir uygulamayı üzerinde çalıştığı donanım veya işletim sisteminden soyutlar. İşletim sisteminin soyutlanmasındaki temel amaç aynı anda tek donanımın kaynakları kullanılarak birden fazla işletim sisteminin ve doğal olarak hizmetlerinin kullanılmasıdır. Ancak bir yan etki olarak konuk (guest) işletim sisteminde meydana gelen değişiklikler sadece onun tarafından kullanılan bir ev sahibi (host) işletim sistemi dosyasında sınırlandırıldığından, zarara yol açabilecek testlerin veya güvenlik riski taşıyan aktivitelerin konuk sistemde yapılması ile ev sahibi sistemin korunması da sağlanmış olur. Teknik olarak işletim sistemi sanallaştırma yöntemi ile aynı yöntem kullanılmamakla birlikte sanallaştırma desteği sağlayan uygulamalar da o uygulama ile yapılan işlemlerin geri kalan sistem dosyalarına etki etmesini engeller ve uygulama kapatıldığında kullanım sırasında gerçekleşen tüm değişiklikler yok olur. Bu alandaki en çok kullanılan uygulamalar web tarayıcılarına sanallaştırma desteği sağlayan uygulamalardır. Böylece o bilgisayar üzerinde yapılan işlemlerin başkaları tarafından öğrenilmesine yol açacak kalıntıların bulunmaması sağlanmış olur.
Anti-Virüs ve Virüs İmzaları	Genel olarak kötü niyetli yazılım (malware) olarak adlandırılan virüs, trojan, worm, spyware ve adware yazılımlarının ortak noktası bilgisayar kullanıcılarının (veya daha genel tanımıyla sistem sahiplerinin) bilgi ve onayı olmadan sistemlere girme, bilgi çalma veya zarar verme amacına yönelik olarak yaratılmış olmalarıdır. Virüsler kendilerini kopyalamak için başka bir çalıştırılabilir dosyaya kendini eklemeye ihtiyaç duyarken worm kendi başına ağ üzerinden diğer bilgisayarlara bulaşabilir. Trojan, genel olarak farklı ve kullanıcının isteyerek yüklediği bir uygulamaya eklenip, istenen uygulamanın çalıştırılması ile bulaşır. Spyware bulaştığı bilgisayarda yapılan

	aktiviteleri kaydedip, başka bir sisteme kullanıcının bilgi ve onayı olmadan gönderir. Adware bulaştığı bilgisayara istenmeyen pazarlama materyallerini indirir ve gösterir. Diğer kötü niyetli yazılımlar arasında rootkit'ler, backdoor'lar, bot'lar, keylogger'lar ve dialer'lar sayılabilir. Anti-virüs yazılımları bu tür yazılımları erişim sırasında veya taramalar sırasında saptar ve günümüzde vazgeçilmez bir güvenlik katmanı oluşturur. Anti-virüs yazılımları kötü niyetli yazılımları tespit etmek için birer virüs imza veritabanı kullanır. Sürekli olarak yeni kötü niyetli yazılımlar ortaya çıktığından bu imzaların güncelliği son derece önemlidir.