1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında Üniversitenin bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunmasına yönelik temel bilgi güvenliği kurallarını belirlemektir.

Bu politika ile;

- bilgi varlıklarının yetkisiz erişim, kullanım, değiştirme, açıklama, kayıp ve imhaya karşı korunması,
- çalışanların ve diğer ilgili tarafların bilgi güvenliği sorumluluklarının belirlenmesi,
- bilgi sistemlerinin güvenli kullanımının sağlanması,
- kişisel verilerin ve diğer korunan bilgilerin uygun şekilde işlenmesi,
- fiziksel ve teknik güvenlik kontrollerinin desteklenmesi,
- üçüncü taraflardan kaynaklanabilecek güvenlik risklerinin azaltılması,
- bilgi güvenliği olaylarının zamanında bildirilmesi ve yönetilmesi,
- bilgi güvenliği farkındalığının artırılması amaçlanmaktadır.

2. KAPSAM

- Süleyman Demirel Üniversitesi **Daire Başkanlıkları / Başkanlıkları**,
- **Genel Sekreterlik**,
- **Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi** ile bunların bilgi işleme faaliyetlerinde görev alan çalışanlarını, yöneticilerini, bilgi teknolojileri personelini, hizmet sağlayıcılarını, yüklenicileri ve diğer ilgili tarafları kapsar.

Politika;

- bilgi sistemlerini,
- bilgi varlıklarını,
- kullanıcı hesaplarını,
- kurumsal e-posta hizmetlerini,
- sunucu ve ağ altyapısını,
- fiziksel çalışma alanlarını,
- taşınabilir bilgi varlıklarını,
- üçüncü taraf erişimlerini,
- kişisel veri içeren bilgi varlıklarını,
- bilgi güvenliği süreçlerini kapsar.

3. SORUMLULUKLAR

3.1. Üst Yönetim

- Bilgi güvenliğinin kurumsal olarak desteklenmesini,
- Gerekli kaynakların sağlanmasını,

- Bilgi güvenliği politika ve süreçlerinin uygulanmasını sağlar.

3.2. Bilgi İşlem Daire Başkanlığı

- Bilgi teknolojileri altyapısının güvenli işletilmesinden,
- Kullanıcı ve erişim kontrollerinin teknik olarak uygulanmasından,
- Sunucu, ağ ve sistem güvenliğinin sağlanmasından,
- Teknik güvenlik zafiyetlerinin yönetilmesinden,
- Bilgi güvenliği olaylarının teknik olarak değerlendirilmesinden,
- Kurumsal e-posta hizmetinin güvenli işletilmesinden,
- Teknik güvenlik kontrollerinin yürütülmesinden sorumludur.

3.3. Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi

Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi, kendi sorumluluğundaki bilgi sistemleri ve bilgi işlem altyapısının bu politika ve ilgili EYS dokümanlarına uygun olarak işletilmesinden sorumludur.

3.4. Daire Başkanlıkları ve Genel Sekreterlik

- Kendi sorumluluklarındaki bilgi varlıklarının korunmasından,
- Çalışanların bilgi güvenliği kurallarına uymasının sağlanmasından,
- Erişim yetkilerinin görev ve sorumluluklarla uyumlu olmasının sağlanmasından,
- Bilgi güvenliği olaylarının ilgili birimlere bildirilmesinden sorumludur.

3.5. Çalışanlar ve Diğer Kullanıcılar

Tüm çalışanlar ve kullanıcılar;

- Kendilerine verilen erişim yetkilerini amacı dışında kullanmamak,
- Kimlik doğrulama bilgilerini korumak,
- Bilgi varlıklarını yetkisiz erişime karşı korumak,
- Bilgi güvenliği olaylarını gecikmeden bildirmek,
- Kişisel veri ve gizli bilgilerin korunmasına ilişkin kurallara uymak,
- Bilgi güvenliği farkındalık eğitimlerine katılmak ile yükümlüdür.

4. UYGULAMA

4.1. Personel ve Kullanıcı Güvenliği

- Çalışanların görev, yetki ve sorumlulukları bilgi güvenliği gereksinimleri dikkate alınarak belirlenir.
- Bilgi varlıklarına erişim, kullanıcının görev ve sorumlulukları ile ihtiyaç duyduğu bilgiye göre yetkilendirilir.
- Kullanıcılara yalnızca görevlerini yerine getirmek için gerekli erişim yetkileri verilir.

- Görev değişikliği, birim değişikliği veya görev sona ermesi durumunda kullanıcıların erişim yetkileri gözden geçirilir ve gerekli değişiklikler zamanında gerçekleştirilir.
- İşten ayrılan veya görevi sona eren kullanıcıların hesapları, erişim yetkileri, kartları, tokenları, anahtarları ve kendilerine tahsis edilen bilgi varlıkları ilgili süreçlere uygun şekilde iptal edilir, geri alınır veya güncellenir.
- Çalışanlar ve ilgili taraflar bilgi güvenliği, kişisel verilerin korunması ve görevlerinin gerektirdiği güvenlik kuralları konusunda bilgilendirilir.
- Bilgi güvenliği farkındalık eğitimleri belirlenen plan doğrultusunda gerçekleştirilir.
- Görevin gerektirdiği durumlarda çalışanlar ve üçüncü taraflarla gizlilik ve bilgi güvenliği yükümlülüklerini içeren sözleşme veya taahhütler yapılır.
- Çalışanlar; kamuya açık alanlar, ortak çalışma alanları, toplantı ortamları ve benzeri yerlerde gizli, kişisel veya hassas bilgilerin yetkisiz kişilerce duyulmasını veya görülmesini önleyecek tedbirleri alır.
- Bilgi güvenliği olayları, ilgili olay yönetimi sürecine uygun olarak bildirilir.

4.2. Fiziksel Güvenlik

Bilgi varlıklarının bulunduğu fiziksel alanların korunması amacıyla;

- yetkisiz kişilerin kontrollü alanlara erişimi engellenir,
- fiziksel erişim yetkileri görev ve sorumluluklara göre belirlenir,
- ziyaretçi ve üçüncü taraf erişimleri kontrol edilir,
- kritik bilgi işlem alanları fiziksel ve çevresel tehditlere karşı korunur,
- yangın, su baskını, enerji kesintisi, sıcaklık, nem, deprem, hırsızlık ve benzeri risklere karşı uygun kontroller uygulanır.

Sistem odaları ve kritik bilgi işlem alanlarına ilişkin ayrıntılı kurallar **Sistem Odaları ve Fiziksel Alanların Güvenliği Politikası** kapsamında uygulanır.

4.3. Üçüncü Taraf Güvenliği

- Kurum paydaşları ile Bilgi teknolojileri sistemlerimize veya bilgi varlıklarına müdahale, test, bakım onarım vb. amaç ile geldiklerinde bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdürler.
- Bilgi varlıklarına veya bilgi sistemlerine erişebilecek üçüncü tarafların bilgi güvenliği sorumlulukları sözleşme, protokol, gizlilik sözleşmesi veya ilgili dokümanlarla belirlenir.
- Üçüncü taraflara yalnızca görevlerini gerçekleştirmek için gerekli erişim yetkileri verilir.
- Üçüncü taraf erişimleri gerektiğinde süre, sistem, kullanıcı ve işlem bazında sınırlandırılır.
- Üçüncü tarafların bilgi sistemlerine gerçekleştirdiği bakım, destek, kurulum ve benzeri işlemler ilgili yetkilendirme ve değişiklik yönetimi kurallarına uygun olarak gerçekleştirilir.
- Görev veya sözleşme sona erdiğinde üçüncü taraflara verilen erişim yetkileri kaldırılır.

- Üçüncü tarafların bilgi güvenliği yükümlülükleri ve bilgi varlıklarının korunmasına ilişkin sorumlulukları sözleşme şartlarında tanımlanır.
- Üçüncü taraflarla paylaşılan bilgilerin sınıflandırma seviyesine uygun güvenlik önlemleri uygulanır.

4.4. Sunucu ve Sistem Güvenliği

- Sunucuların kurulumu, yapılandırılması, güncellenmesi, yedeklenmesi ve yönetimi yetkilendirilmiş personel tarafından gerçekleştirilir.
- Sunucular üzerinde gereksiz servis, uygulama ve bağlantılar kullanılmaz veya mümkün olduğunda devre dışı bırakılır.
- Ayrıcalıklı hesapların kullanımı sınırlandırılır ve ayrıcalıklı işlemler gerektiğinde kayıt altına alınır.
- Genel veya paylaşımlı yönetici hesaplarının kullanımı mümkün olduğunca sınırlandırılır.
- Yönetici hesaplarının kimlik doğrulama bilgileri diğer kullanıcı hesaplarından ayrı olarak korunur.
- Sunucu ve sistemlerde gerçekleştirilen değişiklikler ilgili değişiklik yönetimi kurallarına uygun şekilde gerçekleştirilir.
- Sunucuların güvenlik güncellemeleri ve yamaları **Zaafiyet ve Yama Yönetimi Politikası** kapsamında yönetilir.
- Sunucuların yedeklenmesi ilgili yedekleme ve iş sürekliliği kurallarına uygun olarak gerçekleştirilir.
- Sunucular sistem odaları veya fiziksel güvenlik koşulları uygun olan kontrollü alanlarda bulundurulur.
- Sunucuların erişim ve güvenlik kayıtları ilgili mevzuat, riskler ve kurumsal gereksinimler doğrultusunda belirlenen sürelerde korunur.
- Sistemlerde olağandışı faaliyetler ve güvenlik olayları izlenir ve gerektiğinde olay yönetimi süreci başlatılır.
- Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdırlar. Gerekli olduğunda, önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.
- Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda (sistem odalarında) bulundurulmalıdır.
- Sunucu olarak çalıştırılacak bilgisayarlar üzerinde kesinlikle kişisel işlemler yapılmamalı ve kullanım politikasına aykırı bir kullanıma olanak verilmemelidir.

4.5. Kimlik Doğrulama ve Şifre Güvenliği

- Kullanıcı hesapları kişiye özgü olacak şekilde oluşturulur ve hesap bilgileri başka kişilerle paylaşılmaz.
- Kullanıcıların kimlik doğrulama bilgilerini koruması esastır.

- Parolalar kolay tahmin edilebilecek kişisel bilgilerden veya yaygın olarak kullanılan zayıf parolalardan oluşturulmaz.
- Kullanıcılar aynı parolayı farklı ve kritik sistemlerde tekrar kullanmaktan kaçınır.
- Parolalar e-posta, mesajlaşma uygulaması veya güvenli olmayan başka iletişim kanalları üzerinden paylaşılmaz.
- Parolanın ele geçirildiğinden veya yetkisiz kişilerce öğrenildiğinden şüphelenilmesi halinde parola derhal değiştirilir ve gerekli durumlarda olay bildirilir.
- Kritik ve ayrıcalıklı hesaplarda güçlü kimlik doğrulama yöntemleri ve mümkün olduğu durumlarda çok faktörlü kimlik doğrulama (MFA) uygulanır.
- Kullanıcıların sistemlerden ayrılması durumunda oturumların uygun süre sonunda otomatik olarak kilitlenmesi sağlanır.
- Sistem yöneticileri tarafından kullanılan ayrıcalıklı hesapların güvenliği, kayıt altına alınması ve erişim yetkileri düzenli olarak gözden geçirilir.
- Parola unutulması veya hesabın kilitlenmesi durumunda yalnızca Üniversite tarafından yetkilendirilmiş parola sıfırlama ve kimlik doğrulama mekanizmaları kullanılır.
- Parola güvenliğine ilişkin ayrıntılı teknik kurallar, ilgili teknik standartlar ve sistem yapılandırmalarıyla desteklenir
- **Güçlü Şifreler aşağıdaki karakteristiklere sahiptir.**
  - Küçük ve büyük karakterlere sahiptir. (A -Z , a-z)
  - Rakam, noktalama karakterleri ve harflere sahiptir.(0 - 9,!,@,&=(,}?,\)
  - En az on adet Alfa numerik karaktere sahiptir.
  - Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
  - Aile isimleri gibi kişisel bilgilere ait olmamalıdır.
  - Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır.
  - Parolalar 6 ay yaşlanma süresine sahiptir. Kullanıcılar 6 ay sorunda otomatik olarak şifre sıfırlamaya zorlanırlar.

4.5.1. Genel Şifre Koruma Standartları

Süleyman Demirel Üniversitesi bünyesinde kullanılan şifreler kurum dışında herhangi bir şekilde kullanılmamalı ve kimse ile paylaşılmamalıdır.

Aşağıdaki faaliyetleri gerçekleştirmek kesinlikle yasaktır.

- Herhangi bir kişiye telefonda şifre vermek
- E-posta mesajlarında şifre belirtmek
- Üst yöneticiye şifreleri söyleme
- Başkaları ile şifreler hakkında konuşmak
- Herhangi form üzerinde şifre belirtmek.
- Aile isimlerini şifre olarak kullanmak
- Şifreleri aile bireyleri ile paylaşmak.
- Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstererek Bilgi işlem Daire Başkanlığı yetkilisini aramasını söyleyiniz.

- Uygulamalardaki "şifre hatırlama" özelliklerini seçmeyiniz. (Örnek: Outlook, Internet Explorer vs.) Tekrar etmek gerekirse, şifreleri herhangi bir yere yazmayınız ve herhangi bir ortamda elektronik olarak saklamayınız.
- Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirmeyiniz.
- Bilgi işlem Daire Başkanlığı tarafından zafiyet tarama operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda elde edilen önemli verilere yönelik kullanıcıya şifresini değiştirmesi talep edilecektir.
- Derinweb ve sızıntı taramaları sonucunda kullanıcılarımızdan hesaplarını kaptıran /çaldıran kullanıcıların tespit edilmesi durumunda kullanıcılara yönelik parola değiştirme zorlaması yapılmaktadır.

4.5.2. Şifrenin unutulması

- Bütün sistemler üzerinde, kullanıcıların parolasını unutma ihtimaline karşı bir çözüm sunulmuştur.
- Bu çözüm, SDUNET https://sdunet.sdu.edu.tr web adresinden parolamı unuttum bölümü kullanılarak kullanıcının cep telefonu ile ikinci bir doğrulama alınarak parolanın sıfırlanmasını içermektedir. Eğer kullanıcının cep telefonu sistemde kayıtlı değilse kullanıcıların Personel Daire Başkanlığına kimlikleri ile başvurarak telefon numarasını ekletmesi ya da düzeltmesi gerekmektedir.

4.6. Kurumsal E-Posta Güvenliği

4.6.1. Dikkat Edilmesi Gerekli Hususlar

- Süleyman Demirel Üniversitesi bünyesinde oluşturulan e-postalar resmi bir kimlik taşımaktadırlar. Süleyman Demirel Üniversitesi'nin en önemli iletişim kanallarından biridir ve bu kanalın kullanılması kaçınılmazdır. Bunun yanı sıra e-posta, kullanımının kolaylığı ve hızı nedeni ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır. Kişisel verilerin korunması kapsamında e-posta kullanımının sınırlarının belirlenmelidir.
- Kurumun e-posta sistemi, taciz suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.
- Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
- Firma gizli bilgileri veya kişisel veri içeren (ZİYARETÇİ – ÇALIŞAN vb.) hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine eklenen öğeler de dahildir.
- Zincir mesajlar ve mesajlara eklenmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında içeriğe tıklanmadan hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Kişisel kullanım için internet ortamındaki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

- Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
- Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- Kişisel veri, gizli bilgi veya bilgi sınıflandırmasına göre korunması gereken bilgiler e-posta yoluyla gönderilirken bilginin niteliğine uygun erişim, şifreleme veya diğer güvenlik önlemleri uygulanır.
- Özel nitelikli kişisel verilerin elektronik ortamda aktarılması gerektiğinde, ilgili mevzuat, KVYS kuralları ve kurumun güvenli aktarım yöntemleri uygulanır.
- Çalışanlar kendilerine ayrıca bir yetki tanımlanmamışsa e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemez.
- Gönderilen e-postalara eklenecek dosyaların makul boyutlarda olmasına özen gösterilmelidir. Yüksek boyutlu dosyalar e-postanın ekine koymak yerine, Bilgi İşlem Daire Başkanlığı'ndan destek alıp, erişim linki vererek paylaşılması uygun olacaktır. Aksi takdirde e-posta sunucularında meydana gelen problemlerden dolayı ortaya çıkan iş kayıplarından ilgili çalışan sorumludur.
- Dosya ek boyutu yüksek olan eposta gönderecek kişilerin maillerini sıkıştırıp göndermesi gerekmektedir.
- Kurumsal elektronik posta hesapları toplu posta atma işlemlerine uygun olmayıp kesinlikle kullanılmamalıdır. Bu işlemlere yönelik olarak ilgili destek Bilgi İşlem Daire Başkanlığından alınabilir.

4.6.2. Kişisel Kullanım

- Kurumumuzda kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır.
- Süleyman Demirel Üniversitesi personelleri tarafından internet ortamı aracılığı ile iletilen her türlü kişisel e-posta mesajının altında, Süleyman Demirel Üniversitesi tarafından belirlenen ve bir örneği aşağıda yer alan "gizlilik notu" ve "sorumluluk notu" bilgileri yer almalıdır. Bu bilgiler, E-posta iletisinin içeriğinden ve niteliğinden Veri Sorumlusunun sorumlu tutulamayacağı gibi açıklamalar içermelidir.

  - "Bu e-posta iş için gönderilenler hariç sadece yukarıda isimleri belirtilen kişiler arasında özel haberleşme amacı taşımaktadır. Size yanlışlıkla ulaşmışsa lütfen gönderen kişiyi bilgilendiriniz ve e-postayı sisteminizden siliniz. Süleyman Demirel Üniversitesi bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmez. Ayrıca Kişisel Verileri Koruma Kanunu uyarınca Süleyman Demirel Üniversitesi tarafından işlenen kişisel verileriniz ile ilgili olarak http://kvkk.sdu.edu.tr adresinde yer alan aydınlatma metnine ulaşabilirsiniz."
  - "This e-mail communication, except for business usage, is intended for the private use of the people named above. If you received this message in error, please immediately notify the sender and delete it from your system. The SÜLEYMAN DEMİREL ÜNİVERSİTESİ does not accept legal responsibility for the contents of this message. In addition, we inform you about the personal data processed by SÜLEYMAN DEMİREL ÜNİVERSİTESİ'in accordance

with the Personal Data Protection Law with the illumination text published on our website http://kvkk.sdu.edu.tr"

- Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidir. Bu yüzden şifre kullanılmalı ve e-posta erişimi için donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
- Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplamalıdır.
- Kurum çalışanları kurumsal e-postaların Kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekle sorumludur.
- Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.
- Elektronik postaların sık sık gözden geçirilmesi ve veri kaybını önlemek amacıyla maillerinizi ister e-posta sunucusunda bırakabilir ya da kendi bilgisayarınıza ayrıca yedekleyebilirsiniz.
- E-posta adresine sahip kullanıcının herhangi bir sebepten (emekli olma, işten ayrılma gibi nedenlerle) Kurumdaki değişikliğinin yetkililer tarafından BIDB' ye bildirilmesi gereklidir.
- Kişisel veriler içeren herhangi e-posta gönderme ihtiyacı doğması durumunda bu e-posta genel nitelikte kişisel veri barındırıyorsa kesinlikle doğru kişilerin erişebileceği şekilde, özel nitelikli kişisel veri barındırıyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılmalıdır.

- **Kullanıcının e-posta kutusunun üzerinde aşağıdaki limitler uygulanır.**
  - Kurum dışına e-posta gönderim posta büyüklüğü: 150 Mb
  - Kurum dışından e-posta alım posta büyüklüğü: 150 Mb
  - Kurum içi e-posta gönderim posta büyüklüğü: 150 Mb
  - Kurum içi e-posta alım posta büyüklüğü: 150 Mb
  - Günlük e-posta gönderim adeti; personeller için 50, öğrenciler için 25,
  - 1 dk içinde gönderilebilecek en fazla e-posta adeti personeller için 10, öğrenciler için 5 olarak ayarlanmıştır.
- E-posta Kutusu boyut sınırı 50GB olarak belirlenmiştir. (max 99gb oluyor.)
- Süleyman Demirel Üniversitesi personelleri, gönderdikleri, aldıkları veya sakladıkları e-postalarda kişisel veri barındırmamalıdır.
- Tüm e-postalar güvenlik nedeni ile sürekli olarak yedeklenmektedir.

*<u>**Emekli olan personellerimizin posta kutuları tutulmaktadır ve bu posta kutuları posta almaya açık fakat posta göndermeye kapalıdır.**</u>

4.6.3. Mesaj Oluşturmada Dikkat Edilmesi Gereken Hususlar

- Genel olarak e-posta ortamında uzun ve karışık cümleler kurmaktan kaçınmalı, mümkün olduğunca basit, kesin, açık ve yanlış anlaşılmalara neden olmayacak bir dil

kullanılmaya gayret edilmelidir.

- Dilbilgisi kurallarına ve noktalama işaretlerine uygun, yalın bir Türkçe kullanılmalıdır. Hitap edilen alıcının kimliğine göre bir dil ve ifade tonu belirlenmelidir. Mesaj gönderilmeden önce yazım hatalarına karsı kontrol edilmelidir.
- Metin içerisindeki bazı kısımlara dikkat çekmek için, bu kısımları kalın (bold) karakterlerle, altını çizerek, başka renk vb. şekilde yazmak, nezakete uygun bir davranış değildir. Örneğin kalın (bold) karakterle ayrıştırılmış cümle veya sözcükler, yüz yüze konuşmada muhatabınıza bağırarak konuştuğunuz durumlara benzer etki oluşturabilir. Bir cümlenin altını çizmek, muhatabınızın anlayış kabiliyeti ile ilgili bir hakaret olarak değerlendirilebilir. Mutlak ayrıştırılması ve vurgulanması gereken bir bölüm varsa, bunu diğer yazılı dokümanlardaki uygulamalara benzer olarak yapmaya özen gösterilmelidir. Örneğin, alıntı cümlelerini iki tırnak arasında, eğik (italik) harflerle veya ayrı bir paragrafta eğik harflerle yazılabilir.
- E-posta yazışmalarında tüm cümleyi büyük harflerle yazmak alıcıya bağırma anlamına gelir, kaçınılmalıdır
- E-postalar, "konu" kısmını mutlaka doldurarak gönderilmelidir. İçeriğin ne hakkında olduğunu bildiren bir konu baslığı, gönderilere tekrar bakmak gerektiğinde, hem göndericinin hem de alıcının isini kolaylaştırır. Konu baslığı, içeriğe uygun anahtar kelimelerden oluşan kısa bir tanımlama seklinde olmalıdır.
- Elektronik postanın "kime" bölümü konunun direk muhatabı olan kişi, "bilgi" ve "gizli bilgi" bölümleri ise, iletinin bilgi amaçlı gönderilmesi gereken kişiler için kullanılır. E-postanın "bilgi ve gizli" olarak yollandığı kişiler, mesajın doğrudan muhatabı değillerdir. İleti bu alıcılara sadece bilgi vermek amacıyla yollanmış demektir.

Bir konu hakkında hatırlatma, uyarı, şikâyet içeren mesajın "Bilgi" olarak asıl alıcının üstü pozisyonundaki kişilere de yollanması, alıcının yöneticisine şikâyet edilmesi anlamı da taşır. Mesaj alıcıları seçilirken alıcıyı diğer alıcılar önünde küçük düşürecek ifadelerden kaçınılmalıdır.

4.6.4. Gelen Mesajları Yanıtlamada Dikkat Edilecek Hususlar

- Zincir mesajlara, gerekmediği sürece, "tümünü yanıtla" seklinde cevap yazılmamalıdır. Eğer zincirleme olarak uzayan bir mesaja cevap veriliyorsa, bir önceki mesaj dışındaki mesajlar, çok gerekli değilseler silinmelidir. Aksi takdirde mesaj fazlasıyla uzayacak ve okunamaz hale gelecektir. Çok sayıda kişiye yazılan maillere verilecek cevaplarda "tümünü yanıtla" seçeneği ile geri dönülmeden önce söz konusu cevabın ya da yazışmanın tüm alıcıları ilgilendirdiğinden emin olunmalı, gerekirse sadece maili yazan kişiye "yanıtla" seçeneği ile geri dönülmelidir.
- Elektronik ortamda, genel bilgilendirme maksadıyla yönetim tarafından yayınlanan duyurulara, bireysel olarak ve tüm alıcılara geri dönecek şekilde karsı mesaj yazılmamalıdır. Duyurulan konu ile ilgili herhangi bir sorun varsa sadece o mesajı yazan kişiye bir mail atılarak durum ile ilgili olarak bilgi temin edilebilir ya da bilgi verilebilir.

4.7. Bilgi Sınıflandırma ve Paylaşımı

- Bilgiler, bilgi güvenliği ve iş gereksinimleri doğrultusunda belirlenen sınıflandırma

seviyelerine göre korunur.

- Bilgiye erişim, bilginin sınıflandırma seviyesi ve kullanıcının görev gereksinimleri dikkate alınarak sınırlandırılır.
- Gizli ve Çok Gizli bilgilerin yetkisiz kişilerle paylaşılması yasaktır.
- Kişisel veriler ve özel nitelikli kişisel veriler, bilgi sınıflandırmasına ek olarak KVYS ve KVKK gereklilikleri dikkate alınarak korunur.
- Bilginin aktarılması sırasında bilginin sınıflandırma seviyesi ve aktarım kanalının güvenliği dikkate alınır.
- Bilgi sınıflandırma ve etiketleme kuralları **Bilgi Sınıflandırma ve Etiketleme Politikası** kapsamında uygulanır.

4.8. Bilgi Güvenliği Olayları

- Şüpheli e-posta, parola ele geçirilmesi, yetkisiz erişim, veri kaybı, bilgi sızıntısı, zararlı yazılım, cihaz kaybı, fiziksel güvenlik ihlali ve benzeri olaylar gecikmeden ilgili birimlere bildirilir.
- Bilgi güvenliği olayları ilgili **Olay Yönetimi Prosedürü** kapsamında değerlendirilir.
- Kişisel veri içeren olaylarda ayrıca KVYS ve kişisel veri ihlali yönetimi süreçleri uygulanır.
- Olayların tekrarlanmasını önlemek amacıyla gerektiğinde risk değerlendirmesi ve düzeltici faaliyet gerçekleştirilir.

4.9. Bilgi Güvenliği Farkındalığı

1. Çalışanlara görevlerinin gerektirdiği bilgi güvenliği farkındalık eğitimleri, bilgilendirme mailleri, masaüstü pop-up bildirimleri yapılmaktadır.
2. Eğitimlerde özellikle;

    - parola ve kimlik doğrulama güvenliği,
    - oltalama ve sosyal mühendislik,
    - kişisel verilerin korunması,
    - bilgi sınıflandırması,
    - e-posta güvenliği,
    - fiziksel güvenlik,
    - bilgi güvenliği olaylarının bildirilmesi konularına yer verilir.

3. Eğitim ve farkındalık faaliyetlerinin etkinliği gerektiğinde ölçülür ve kayıt altına alınır.

5. YAPTIRIM

Bu politikaya aykırı hareket eden çalışanlar ve diğer ilgili taraflar hakkında olayın niteliğine göre ilgili EYS süreçleri, sözleşme hükümleri, ilgili mevzuat ve Üniversitenin disiplin hükümleri uygulanır.