1. AMAÇ

Bu politikanın amacı, **Süleyman Demirel Üniversitesi** bünyesindeki her türlü kişisel veri içeren kurumun bilgi kaynaklarının güvenliğinin sağlanması, kullanılan e-posta altyapısına yönelik kuralların ortaya koyulmasını, çalışanlarının bu konulara duyarlı olması, bilinç seviyesi kendisine verilen yetki ve sorumlulukları iyi anlaması ve yerine getirmesiyle ilgili kuralları tanımlamaktır.

Bu nedenle kurum, personel güvenliği, fiziksel güvenliği, üçüncü taraf güvenliği, sunucu güvenliği, şifre güvenliği, E-Posta güvenliği ile ilgili konularını ne şekilde ele alacağını bu politika ile belirler.

2. KAPSAM

Bu politika tüm Süleyman Demirel Üniversitesi personelinin güvenlik açısından bilinçlendirilmesini, bilgi sistemlerini kullanan tüm çalışanları ve kurumun sahip olduğu bilgi sistemlerini, kurum e-postasını kullanan bütün çalışanları, bilgi teknolojilerinde, parola ile korunan veya korunması gereken bütün kaynakları (yazılım, donanım, hizmet veya kullanıcı vb.) kullanıcıları, çalışma alanlarını ve sistem yerleşkelerini ve üçüncü taraflarla iletişim halinde olan, çeşitli anlaşmalar tanımlayan ve sonlandıran kişileri kapsamaktadır.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından tüm yönetici ve Veri Sorumlusu personelleri sorumludur.

4. UYGULAMA

4.1. Personel Güvenlik Politikası

- Tüm çalışanlar ile gizlilik anlaşmaları imzalanacaktır.
- Görev tanımı değişen veya Süleyman Demirel Üniversitesi bünyesinden ayrılan kullanıcıların erişim hakları hemen yeniden düzenlenecek veya kaldırılacaktır.
- Bilgi Güvenliği ile ilgili olaylar Bilgi İşlem Daire Başkanlığına ve KVK Komitesine/Temsilcisine hızla bildirilecektir.
- Kişisel Veri Güvenliği Yönetim Sistemi dahilinde olan tüm kritik kişisel verilerin korunmasından tüm çalışanların sorumlu olduğu ve bu sorumluluğun yürütülmesi için gerekli olan tüm politikalara koşulsuz uyulması gerektiği personele eğitim ve bilgilendirme yolları ile aktarılacaktır.
- Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
- Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.

- Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.
- Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
- Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.
- Çalışanlara kamuya açık alanlarda, açık ofis ortamlarında ve ince duvarları olan odalarda gizliliği olan konuşmaların yapılmaması hatırlatılmalıdır.
- Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır

4.2. Fiziksel Güvenlik Politikası

- Kurumsal bilgi varlıklarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.
- Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.
- Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlarına giriş yetkili görevliler gözetiminde gerçekleştirilmelidir.
- Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
- Kritik sistemler erişim yetkilisi ile belirlenmiş alanlarda bulundurulmalıdır.
- Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.
- Kuruma giriş yapacak ziyaretçi veya kurya teslimatları yetkili görevliler gözetiminde gerçekleştirmelidir.
- Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.
- Fotoğraf, video, ses vb. kayıt cihazlarının yetki verilmeyen kişiler tarafından güvenli alanlara sokulması yasaklanmalıdır.

4.2.1. Donanım

- 7/24 kesintisiz çalışan sistemlere mümkün olduğunca donanımsal arıza durumunda müdahale edebilmek için, tüm donanımların hataya dayanıklılık (fault tolerance) ve sistem çalışırken değiştirilebilir (hot swap) özelliklerinin olmasına, kendi içlerinde veya birbirleriyle paralel, yedekli çalışabilir olduğuna dikkat edilmelidir.
- İş sürekliliği için her donanımın aktif-aktif ya da aktif-pasif çalışan yedekli (redundant) yapıda olmalıdır.

- Donanımlarda oluşabilecek parça arızaları için kritik parçalar yedeklenecek, donanım bakımları düzenli olarak belli periyotlarda yapılmalıdır.

4.2.2. İnsan – Hırsızlık – Sabotaj

- Hırsızlık ve sabotaja karşı bina güvenliği, bina girişlerinde ve katlarda kamera bulunmalıdır.
- Ofis alanları sürekli kilitli tutulmalı, sadece yetkili personel için erişim izni verilmelidir.
- Kurum binası dışına çıkarılmış gizli donanım, yazılım, dokümanlar (notebook, desktop pc, dvd, dlt, dosya vb.) açıkta bırakılmamalıdır.

4.2.3. Yangın

- Mümkünse ofis alanlarına ve odaya gelen tüm kablolara dışarıdan gelecek ısıyı engellemek için ısı yalıtımı yapılmalı, yangına dayanıklı kablo ve elektrik ekipmanlarının kullanılması sağlanmalıdır.
- Alarm durumunda ilgili kişilere e-posta yoluyla sistemler tarafından bilgilendirme yapılacaktır. Otomatik yangın alarm sisteminin yanlış alarm ve acil durumlarda durdurulabilir olduğu denetlenecektir.
- Taşınabilir yangın söndürücülerin kapıya olabildiğince yakın olmasına dikkat edilmelidir.
- Veri merkezine girme yetkisine sahip personelin yangın söndürücüyü kullanabilme konusunda yeterli deneyime sahip olması, yangın söndürücülerin doluluğunun periyodik olarak kontrol edilmesi sağlanmalıdır.
- Veri merkezinde özellikle otomatik gazlı yangın söndürme sistemleri tercih edilecektir. Eğer yangın söndürme sistemi gazlı bir sistem ise, yangın alarmı ile birlikte veri merkezine girecek personelin gazdan etkilenmemesi için yapması gerekenleri gösteren talimatnamenin de veri merkezinin dış kapısına ya da uygun bir yere yerleştirilmesi sağlanmalıdır.

4.2.4. Sıcaklık

- Birçok donanım için 10-25 °C arası oda sıcaklıklarının korunması uygun olacaktır.
- Donanımların kullanım kılavuzlarından faydalanarak uygun sıcaklık aralıkları tespit edilip (genelde 20-25 °C), klima ve iklimlendirme sistemleriyle uygun oda sıcaklığı sağlanır.
- Donanımlar duvarlara çok yakın yerleştirilmemelidir. Donanımların duvarlara mesafesini belirlemek için donanımın kılavuzundan faydalanılır. Kılavuzda belirtilmiyorsa donanımlar hava sirkülasyonunu sağlayacak biçimde ve en az 15-20 cm boşluk bırakacak şekilde yerleştirilmelidir.

4.2.5. Deprem veya Patlama

- Donanımların, zeminden çok yükseğe yerleştirilmesinden kaçınılmalıdır.
- Kabinlerin yere, tavana, kendi aralarında rack mount kitlerle sabitlenmesi ve içindeki tüm donanımların vidalarla ve kablo bağlarıyla sabitlenmesi sağlanmalıdır.
- Donanımlar özellikle zeminin üzerindeki katlarda, pencerelerden uzak tutulmalıdır.
- Yedekler kurum dışındaki başka güvenli mekanlarda saklanmalıdır.

4.3. Üçüncü Taraf Güvenlik Politikası

- Kurum paydaşları ile Bilgi teknolojileri sistemlerimize veya bilgi varlıklarına müdahale, test, bakım onarım vb. amaç ile geldiklerinde Gizlilik Sözleşmesi yapılacaktır ve bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdürler.
- Kurum paydaşları ile Bilgi İşlem Daire Başkanlığına ait özel bilgilerin paylaşıldığı proje veya iş anlaşmaları durumunda Gizlilik Sözleşmesi yapılmalıdır.
- Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarımız üzerinde yapacakları çalışmaları Bilgi İşlem Daire Başkanlığına bildirmek zorundadır.
- Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarına, kendilerine verilen yetki kapsamında erişim sağlayacaktır.
- Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarına erişim yetkileri, çalışma alanlarını kapsayacak şekilde kısıtlı yetki verilecektir. İşlem logları saklı tutulacak ve çalışma bittikten sonra verilen yetkiler hemen geri alınacaktır.
- Kurum paydaşlarına bilgi teknolojileri sistemlerimize veya bilgi varlıklarına erişim izni verilecek bilgisayarlar/mobil cihazlar için ERİŞİM KONTROL POLİTİKASI uygulanacaktır. Kurum gerekli gördüğü durumlarda herhangi bir uyarıda bulunmadan VPN bağlantı erişimlerini kesme hakkına sahiptir.
- Kurum içinde kullanılan gizli bilgiler üçüncü tarafların eline geçmemelidir. Üçüncü taraflar kendi kuruluşlarına transfer olabilecek çalışanları görmemelidir.
- Üçüncü taraflara kurumun ağına erişim izni verilmeden önce bilgisayarlarının güvenliğinden emin olmaları gerekir. Kurum, üçüncü taraflara herhangi bir uyarıda bulunmadan ağa erişimlerini kesebilir.
- Anlaşma sona erdiğinde, tarafların, birbirlerindeki dokümanları geri vermesi gerekir.
- Tedarikçiler kuruluşun sistemlerine erişmeden önce koşulların tanımlanmakta olduğu bir anlaşma imzalanmalıdır.
- Gizli bilgilerin dağıtımını içeren kurallar belirlenmeli ve üçüncü taraflara bu bilgiler iletilmeden önce taraflarla bu kurallar hakkında anlaşılmalıdır.
- Eğer bir gizlilik politikası, Kurumun dezavantajlı olmasına neden oluyorsa, Kurum bu dezavantajdan kurtulmak için üçüncü taraf kuruluşla anlaşma yapmamalıdır.

4.4. Sunucu Güvenlik Politikası

- Sunucu kurulumları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.
- Kurum'da bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel(ler) sorumludur.
- Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.
- Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.
- Servislere erişimler sistem yöneticileri tarafından 6 (altı) ay boyunca loglanacak ve erişim kontrol metotlarıyla koruma sağlanacaktır.
- Sunucular üzerinde yapılacak değişiklikler yönetim kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
- 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.
- Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir.
- Sunucu olarak çalıştırılacak bilgisayarlar üzerinde kesinlikle kişisel işlemler yapılmamalı ve kullanım politikasına aykırı bir kullanıma olanak verilmemelidir.
- Port tarama atakları düzenli olarak yapılmalıdır.
- Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.
- Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.
- Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

4.5. Şifre Güvenliği Politikası

Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre bilgi güvenliğini tümüyle riske atabilir. Süleyman Demirel

Üniversitesi çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dâhilinde şifreleme yapmakla sorumludurlar.

4.5.1. Genel

- Bütün sistem seviyeli şifreler (root, administrator), 3 ayda bir değiştirilmelidir.
- Bütün kullanıcı seviyeli şifreler (örnek, e -posta, web vs.) için tavsiye edilen değiştirme süresi 180 günde birdir.
- Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
- Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.
- Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.
- Bir kullanıcı adı ve şifresi aynı anda birden çok bilgisayarda kullanılmamalıdır.

4.5.2. Genel Şifre oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları; kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleridir. Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

- Kullanıcılar giriş yaptıkları bilgisayardan çıktıktan sonra farklı bir bilgisayardan giriş yapabilirler.
- Yazılan parolanın ekranda görünmemesi veya maskelenerek görünmesi sağlanır.
- Kullanıcı parolaları, saklandıkları ortamlarda, geri dönüşü mümkün olmayan bir şekilde bozularak korunur (örneğin Hash), bu sayede en yetkili kişilerin bile kullanıcı parolasını görmesi engellenir. Bilgi kaynaklarına başarılı ve başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerinin kaydı tutulur.
- Kullanıcıların kimlik doğrulaması yaparak oturum açtıkları sistemlerin başından ayrıldıklarında (sisteme parola ile giriş yapıldıktan sonra sistem açık bırakılması halinde) en geç 15 dakika sonra otomatik olarak kapanması (sistemin kilitlenmesi) sağlanır.
- Halka açık veya paylaşılan ağlardan iletilen kimlik bilgileri güçlü şifreleme metotları ile (SSL) korunur.
- Başkaları tarafından öğrenildiğinden şüphelenilen parolalar hemen değiştirilir.

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.

4.5.3. Genel Şifre Koruma Standartları

Süleyman Demirel Üniversitesi bünyesinde kullanılan şifreler kurum dışında herhangi bir şekilde kullanılmamalı ve kimse ile paylaşılmamalıdır. Bütün şifreler Veri Sorumlusuna ait gizli bilgiler olarak düşünülmelidir.

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.

4.5.4. 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. E-Posta Güvenliği Politikası

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.
- Çalışanlar kendilerine ayrıca bir yetki tanımlanmamışsa e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) ve

her türlü **kişisel veri içeren** e-posta 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.
- Yüklü mail gönderecek kişilerin maillerini sıkıştırıp göndermesi gerekmektedir.

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: 15Mb
  - Kurum dışından e-posta alım posta büyüklüğü: 20Mb
  - Kurum içi e-posta gönderim posta büyüklüğü: 50Mb
  - Kurum içi e-posta alım posta büyüklüğü: 50Mb
  - 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 bulunmamaktadır.
- Süleyman Demirel Üniversitesi personelleri, gönderdikleri, aldıkları veya sakladıkları e-postalarda kişisel veri barındırmamalıdır.
- Tüm e-postalar güvenlik nedeni ile sürekli olarak yedeklenmektedir.

*__Emekli olan personellerimizin ve mezun olan öğrencilerimizin posta kutuları tutulmaktadır ve bu posta kutuları posta almaya açık fakat posta göndermeye kapalıdır.__

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.

5. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında **Disiplin Prosedürü** hükümleri uygulanır.