1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında Üniversite tarafından sağlanan bilgi sistemleri, bilişim kaynakları, bilgi varlıkları ve iletişim hizmetlerinin güvenli, uygun ve yetkili kullanımına ilişkin kuralları belirlemektir.

Bu politika ile bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunması, bilişim kaynaklarının yetkisiz veya amacı dışında kullanımının önlenmesi, bilgi güvenliği risklerinin azaltılması ve kullanıcıların sorumluluklarının belirlenmesi amaçlanmaktadır.

2. KAPSAM

Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik, Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi bünyesinde Üniversite tarafından sağlanan veya Üniversitenin bilgi işleme faaliyetlerinde kullanılan;

- bilgisayar ve mobil cihazları,
- bilgi sistemlerini,
- kurumsal e-posta hizmetlerini,
- internet ve ağ hizmetlerini,
- yazılımları,
- sunucu ve depolama kaynaklarını,
- taşınabilir bilgi varlıklarını,
- diğer bilişim ve iletişim kaynaklarını kullanan tüm çalışanları, öğrencileri, hizmet sağlayıcıları, yüklenicileri ve diğer yetkili kullanıcıları kapsar.

3. SORUMLULUKLAR

3.1. Bilgi İşlem Daire Başkanlığı

- Bilişim kaynaklarının güvenli işletilmesine yönelik teknik kontrollerin uygulanmasından,
- Kullanıcı erişimlerinin yetkilendirilmesinden ve gerektiğinde kaldırılmasından,
- Zararlı yazılım ve benzeri teknik tehditlere karşı gerekli kontrollerin uygulanmasından,
- Bilişim kaynaklarının güvenli kullanımına ilişkin kullanıcıların bilgilendirilmesinden,
- Gerekli durumlarda kullanım kayıtlarının ilgili mevzuat ve eys kurallarına uygun olarak tutulmasından sorumludur.

3.2. Birim Yöneticileri

Birim yöneticileri, kendi sorumluluk alanlarındaki kullanıcıların bilişim kaynaklarını görev ve yetkileri doğrultusunda kullanmasını ve bilgi güvenliği kurallarına uymasını sağlar.

3.3. Kullanıcılar

Tüm kullanıcılar;

- kendilerine tahsis edilen bilişim kaynaklarını yalnızca yetkileri ve görevleri kapsamında kullanmak,
- kullanıcı adı, parola ve diğer kimlik doğrulama bilgilerini korumak,
- bilgi varlıklarını yetkisiz erişime karşı korumak,
- Üniversitenin bilgi güvenliği ve EYS dokümanlarına uymak,
- tespit ettikleri bilgi güvenliği olaylarını ilgili birimlere bildirmek ile yükümlüdür.

3.4. Üçüncü Taraflar ve Yükleniciler

Üçüncü taraflar ve yükleniciler, Üniversite bilişim kaynaklarına erişimleri sırasında kendileri için belirlenen bilgi güvenliği, gizlilik, kişisel verilerin korunması ve erişim kontrolü kurallarına uymakla yükümlüdür.

4. UYGULAMA

4.1. Bilişim Kaynaklarının Kabul Edilebilir Kullanımı

1. Üniversite tarafından sağlanan bilişim kaynakları öncelikle Üniversitenin eğitim, araştırma, idari ve hizmet faaliyetlerinin yürütülmesi amacıyla kullanılır.
2. Kullanıcılar kendilerine tanımlanan erişim yetkilerinin dışına çıkamaz ve başka kullanıcıların hesaplarını veya erişim yetkilerini kullanamaz.
3. Kullanıcı hesapları kişiye özgü olarak kullanılır. Kullanıcı adı, parola, token, kart ve benzeri kimlik doğrulama bilgileri başka kişilerle paylaşılmaz.
4. Kullanıcılar, Üniversitenin bilgi sistemleri üzerinde yetkisiz erişim, veri değiştirme, veri silme, sistemleri devre dışı bırakma veya hizmetleri engelleme amacı taşıyan faaliyetlerde bulunamaz.
5. Bilişim kaynaklarının güvenliğini olumsuz etkileyebilecek işlemler, yalnızca yetkilendirilmiş personel tarafından ve ilgili prosedürlere uygun şekilde gerçekleştirilir.
6. Kullanıcılar kendilerine tahsis edilen bilgisayar, mobil cihaz, taşınabilir ortam ve benzeri bilgi varlıklarını kayıp, hırsızlık, yetkisiz erişim ve kötüye kullanıma karşı korur.

4.2. Bilgi Varlıklarının Kullanımı

1. Üniversiteye ait veya Üniversitenin sorumluluğunda bulunan bilgiler yalnızca görev, yetki ve belirlenen kullanım amacı doğrultusunda kullanılır.
2. Bilgilerin kopyalanması, aktarılması, paylaşılması veya kurum dışına çıkarılması sırasında bilgi sınıflandırma seviyesi ve ilgili güvenlik kuralları dikkate alınır.
3. Gizli ve Çok Gizli olarak sınıflandırılan bilgiler, yalnızca yetkilendirilmiş kişilerle ve belirlenen güvenli yöntemler kullanılarak paylaşılır.

4. Kişisel veriler, görev gerekliliği ve hukuki işleme şartları doğrultusunda işlenir ve yetkisiz kişilerle paylaşılmaz.
5. Kişisel verilerin işlenmesi, saklanması, aktarılması ve imhasında KVYS, KVKK ve ilgili EYS dokümanlarında belirlenen kurallara uyulur.
6. Bilgi varlıklarının kullanımı ve paylaşımı sırasında Bilgi Sınıflandırma ve Etiketleme Politikası hükümleri uygulanır.

4.3. Parola ve Kimlik Doğrulama Bilgilerinin Kullanımı

1. Kullanıcılar kendilerine ait parola ve diğer kimlik doğrulama bilgilerini gizli tutar.
2. Parolalar başka kişilere açıklanamaz, e-posta veya güvenli olmayan iletişim kanalları üzerinden gönderilemez.
3. Kullanıcıların başka kişilere ait hesapları kullanması veya hesap bilgilerini başkalarına kullandırması yasaktır.
4. Parolanın ele geçirildiğinden veya yetkisiz kişiler tarafından öğrenildiğinden şüphelenilmesi halinde parola değiştirilir ve olay ilgili birime bildirilir.
5. Kimlik doğrulama bilgilerinin korunmasına ilişkin ayrıntılı kurallar **Bilgi Güvenliği Politikası** ve ilgili erişim kontrol dokümanlarında belirlenir.

4.4. Yazılım Kullanımı

1. Üniversite bilişim kaynaklarında yalnızca lisanslı, yetkilendirilmiş veya Üniversite tarafından kullanımına izin verilen yazılımlar kullanılır.
2. Kullanıcılar, görevleri için gerekli olmayan veya güvenilirliği doğrulanmamış yazılımları bilgi işlem cihazlarına kuramaz.
3. Yazılım kurulumu gerektiğinde Üniversitenin belirlediği yetkilendirme ve destek süreçleri uygulanır.
4. Lisanssız veya telif hakkı ihlali oluşturabilecek yazılımların kullanılması yasaktır.
5. Kullanıcılar yazılımların kullanımında ilgili fikri ve sınai mülkiyet, telif ve lisans hükümlerine uymakla yükümlüdür.

4.5. Zararlı Yazılım ve Güvenlik Kontrolleri

1. Üniversite tarafından sağlanan güvenlik yazılımları ve güvenlik kontrolleri kullanıcı tarafından devre dışı bırakılamaz.
2. Antivirüs, uç nokta güvenliği, güvenlik duvarı ve benzeri güvenlik kontrollerinin devre dışı bırakılması veya değiştirilmesi yalnızca yetkilendirilmiş personel tarafından gerçekleştirilebilir.
3. Kullanıcılar güvenlik yazılımlarının uyarılarını dikkate alır ve tespit edilen şüpheli durumları ilgili birime bildirir.
4. Şüpheli dosyalar, bağlantılar veya yazılımlar yetkisiz şekilde çalıştırılamaz.
5. Zararlı yazılım olayları Olay İhlal Prosedürü kapsamında ele alınır.

4.6. Ağların ve Bilgi Sistemlerinin Yetkisiz Kullanımı

1. Üniversitenin bilişim ağı ve bilgi sistemleri üzerinde yetkisiz tarama, dinleme, izleme, zafiyet araştırması, parola kırma, sızma testi veya benzeri güvenlik testi faaliyetleri gerçekleştirilemez.
2. Güvenlik testi, zafiyet taraması ve benzeri teknik çalışmalar yalnızca Üniversite tarafından yetkilendirilmiş personel tarafından ve ilgili onay süreçleri kapsamında gerçekleştirilir.
3. Üçüncü tarafların Üniversite ağı üzerinde gerçekleştireceği teknik çalışmalar önceden yetkilendirilir ve kapsamı belirlenir.
4. Yetkisiz cihazların Üniversite ağına bağlanması veya güvenlik kontrollerini aşmaya yönelik yöntemlerin kullanılması yasaktır.

4.7. İnternet ve Elektronik İletişim Kullanımı

1. İnternet ve elektronik iletişim hizmetleri Üniversitenin faaliyetlerinin yürütülmesi amacıyla güvenli ve mevzuata uygun şekilde kullanılır.
2. Kullanıcılar, internet ve elektronik iletişim hizmetlerini kullanırken ilgili mevzuata ve Üniversitenin EYS kurallarına uymakla yükümlüdür.
3. Oltalama, zararlı yazılım, dolandırıcılık, yetkisiz erişim veya bilgi güvenliği riski oluşturabilecek internet siteleri ve bağlantılar konusunda gerekli dikkat gösterilir.
4. Üniversitenin bilişim kaynakları kullanılarak hukuka aykırı, tehdit edici, taciz edici, ayrımcı veya bilgi güvenliği kurallarını ihlal eden içerikler oluşturulamaz, depolanamaz veya dağıtılamaz.
5. Kurumsal e-posta kullanımında Bilgi Güvenliği Politikası ve ilgili e-posta güvenliği kurallarına uyulur.
6. İnternet ve elektronik iletişim hizmetlerinin kullanımı sırasında 5651 sayılı Kanun ve uygulanabilir diğer mevzuat hükümlerine uyulur.

4.8. Kurumsal Bilgilerin İzlenmesi ve Kayıt Altına Alınması

1. Üniversitenin bilgi sistemlerinde gerçekleştirilen işlemlere ilişkin log, erişim ve güvenlik kayıtları; ilgili mevzuat, bilgi güvenliği gereksinimleri ve EYS kuralları doğrultusunda oluşturulabilir ve saklanabilir.
2. İzleme ve kayıt faaliyetleri, yalnızca belirlenen amaçlar ve yetkilendirilmiş kişiler tarafından gerçekleştirilebilir.
3. Kişisel veri içeren log ve kullanım kayıtlarının işlenmesinde KVKK ve KVYS gereklilikleri dikkate alınır.
4. Teknik izleme ve kayıt faaliyetlerinin kapsamı, saklama süresi ve erişim yetkileri ilgili prosedür ve teknik dokümanlarda belirlenir.

4.9. Kişisel Verilerin Korunması

1. Kullanıcılar, görevleri kapsamında eriştikleri kişisel verileri yalnızca yetkileri ve görevleri doğrultusunda işler.
2. Kişisel verilerin yetkisiz kişilere açıklanması, aktarılması, kopyalanması veya amacı dışında kullanılması yasaktır.
3. Özel nitelikli kişisel veriler için ilgili mevzuatta ve KVYS dokümanlarında belirlenen ilave teknik ve idari tedbirler uygulanır.
4. Kişisel veri içeren bilgi varlıklarının güvenliğinin ihlal edildiğinin veya ihlal şüphesinin bulunduğunun tespit edilmesi halinde olay ilgili KVYS ve bilgi güvenliği süreçlerine bildirilir.

4.10. Üçüncü Tarafların Kullanımı

1. Yüklenici ve hizmet sağlayıcı personelinin Üniversite bilişim kaynaklarına erişimi görev ve sözleşme kapsamında tanımlanan yetkilerle sınırlandırılır.
2. Üçüncü taraflar Üniversitenin bilgi sistemlerinde yetkisiz tarama, dinleme, izleme veya sızma testi gerçekleştiremez.
3. Teknik test veya müdahale gerektiren faaliyetler Üniversitenin yetkilendirmesi ve belirlenen kapsam dahilinde gerçekleştirilir.
4. Üçüncü taraflara verilen erişim yetkileri görev sona erdiğinde veya ihtiyaç ortadan kalktığında kaldırılır.
5. Üçüncü tarafların bilgi güvenliği ve gizlilik yükümlülükleri ilgili sözleşme ve dokümanlarda tanımlanır.

4.11. Erişimin Kısıtlanması

Üniversite; bilgi güvenliği olayı, teknik arıza, bakım, güvenlik tehdidi, mevzuat gerekliliği veya hizmet sürekliliğinin korunması gibi durumlarda, yetkili süreçler kapsamında belirli kullanıcıların veya kullanıcı gruplarının bilgi sistemlerine erişimini geçici veya kalıcı olarak kısıtlayabilir.

4.12. Bilgi Güvenliği Olaylarının Bildirilmesi

Kullanıcılar aşağıdaki durumları gecikmeden ilgili birime bildirmekle yükümlüdür:

- kullanıcı hesabının ele geçirilmesi veya ele geçirilme şüphesi,
- parola bilgilerinin yetkisiz kişilerce öğrenilmesi,
- bilgisayar veya mobil cihaz kaybı,
- şüpheli e-posta veya bağlantılar,
- zararlı yazılım uyarıları,
- yetkisiz erişim,
- bilgi kaybı veya bilgi sızıntısı,
- kişisel veri ihlali veya ihlal şüphesi,

- bilişim sistemlerine yönelik şüpheli faaliyetler.

Bildirimler Olay İhlal Prosedürü ve ilgili KVYS süreçlerine uygun olarak gerçekleştirilir.

5. YAPTIRIM

Bu politikaya aykırı davranışların tespit edilmesi halinde olayın niteliğine göre;

- Bilgi Güvenliği Olay Yönetimi,
- Kişisel Veri İhlali Yönetimi,
- Risk Yönetimi,
- Düzeltici Faaliyet süreçleri uygulanabilir.

Gerekli durumlarda ilgili mevzuat, sözleşme hükümleri ve Üniversitenin disiplin hükümleri uygulanır.