1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında meydana gelebilecek bilgi güvenliği olayları, bilgi güvenliği ihlalleri, kişisel veri ihlalleri ve gizlilik olaylarının zamanında bildirilmesi, değerlendirilmesi, kontrol altına alınması, sonuçlandırılması ve olaylardan elde edilen deneyimlerin iyileştirme faaliyetlerinde kullanılmasına ilişkin esasları belirlemektir.

Bu politika ile bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunması, kişisel verilerin korunması, olayların etkilerinin azaltılması ve benzer olayların tekrarının önlenmesi amaçlanmaktadır.

2. KAPSAM

Bu politika; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi kapsamında;

- Bilgi güvenliği olaylarını ve ihlallerini,
- Kişisel veri ihlallerini ve gizlilik olaylarını,
- Bilgi sistemlerini ve bilgi varlıklarını,
- Bilgi işleme faaliyetlerini,
- Çalışanları ve öğrencileri,
- Hizmet sağlayıcıları ve diğer üçüncü tarafları,
- Olayların bildirilmesi, değerlendirilmesi, müdahale edilmesi, raporlanması, kapatılması ve sonrasında iyileştirme yapılması süreçlerini kapsar.

3. SORUMLULUK

3.1. Tüm Çalışanlar ve Kullanıcılar

- Bilgi güvenliği olayı, kişisel veri ihlali veya güvenlik zafiyeti şüphesini gecikmeksizin ilgili birime bildirmek,
- Olayla ilgili mevcut bilgi ve kanıtların korunmasına yardımcı olmak,
- Olay müdahalesini engelleyebilecek yetkisiz işlem yapmamak,
- Olay yönetimi kapsamında kendilerinden talep edilen bilgi ve desteği sağlamak.

3.2. Bilgi İşlem Daire Başkanlığı

- Bilgi güvenliği olaylarının teknik açıdan değerlendirilmesini ve yönetilmesini sağlamak,
- Gerekli log, sistem kaydı ve teknik kanıtların korunmasını sağlamak,
- Olayın etkisini azaltmaya yönelik teknik tedbirleri almak,
- Gerektiğinde ilgili sistemleri izole etmek veya erişimleri sınırlandırmak,

3.3. KVYS Sorumluları / Yetkili Birimler

- Kişisel veri içeren olayların KVKK ve Üniversitenin kişisel veri yönetimi kuralları açısından değerlendirilmesini sağlamak,
- İhlale konu kişisel verilerin niteliğini ve etkilenebilecek kişi gruplarını değerlendirmek,
- İlgili bildirim ve bilgilendirme yükümlülüklerinin değerlendirilmesini ve gerekli işlemlerin yürütülmesini sağlamak.

3.4. Üst Yönetim

- Olay yönetimi için gerekli kaynakların sağlanmasını desteklemek,
- Önemli veya geniş etkili olaylarda gerekli kararların alınmasını sağlamak,
- Gerekli durumlarda kriz ve iş sürekliliği süreçlerinin devreye alınmasını sağlamak.

3.5. Hizmet Sağlayıcılar ve Üçüncü Taraflar

Hizmet sağlayıcılar ve üçüncü taraflar, Üniversite bilgi varlıklarını etkileyebilecek olayları sözleşme ve ilgili EYS kuralları doğrultusunda gecikmeksizin Üniversiteye bildirmek ve olay yönetimi çalışmalarına gerekli desteği sağlamakla yükümlüdür.

4. UYGULAMA

4.1. Olay ve İhlal Tanımı

Aşağıdaki durumlar bilgi güvenliği olayı, bilgi güvenliği ihlali veya kişisel veri ihlali kapsamında değerlendirilebilir:

- Yetkisiz erişim veya erişim teşebbüsü,
- Bilgi bütünlüğünün bozulması,
- Bilginin yetkisiz kişilerle paylaşılması,
- Kişisel verilerin yetkisiz erişime, açıklanmaya, kayba veya değiştirilmeye maruz kalması,
- Zararlı yazılım bulaşması,
- Fidye yazılımı saldırıları,
- DDoS ve benzeri siber saldırılar,
- Bilgi sistemlerinde yetkisiz değişiklikler,
- Sistem arızaları ve hizmet kesintileri,
- Yanlış alıcıya kişisel veri veya gizli bilgi gönderilmesi,
- Bilgi varlıklarının kaybolması veya çalınması,
- Bilgi güvenliği politikalarının ihlal edilmesi,
- Bilgi güvenliği açısından önemli güvenlik açıklarının istismar edilmesi.

4.2. Olayın Bildirilmesi

1. Olayı fark eden çalışan veya kullanıcı, olayı gecikmeksizin ilgili birime bildirir.
2. Bilgi güvenliği olayları Bilgi İşlem Daire Başkanlığı tarafından belirlenen olay bildirim kanalları üzerinden bildirilir.

3. Kişisel veri içeren veya kişisel veri ihlali şüphesi bulunan olaylar ayrıca ilgili KVYS sorumlularına/yetkili birime bildirilir.
4. Olaylar gerektiğinde;

   - Olay Bildirim Formu,
   - Bilgi Güvenliği Olay Kayıtları,
   - Kişisel Veri İhlal Bildirim Formu veya EYS kapsamında kullanılan ilgili elektronik kayıt sistemi üzerinden kayıt altına alınır.

5. Hizmet sağlayıcılar ve üçüncü taraflar, kendilerini ilgilendiren bilgi güvenliği veya kişisel veri olaylarını sözleşmelerde belirlenen süre ve yöntemlere uygun olarak Üniversiteye bildirir.

4.3. Olayın Değerlendirilmesi

Olayın değerlendirilmesinde olayın niteliği, kapsamı, etkisi ve aciliyeti dikkate alınır.

- ***Bilgi Güvenliği Açısından***

- Etkilenen bilgi varlıkları ve sistemler,
- Gizlilik, bütünlük ve erişilebilirlik üzerindeki etkiler,
- Etkilenen hizmetler,
- Olayın kapsamı ve yayılımı,
- Olayın önem ve öncelik seviyesi,
- İş sürekliliği üzerindeki olası etkiler değerlendirilir.

- ***Kişisel Veri Açısından***

- İhlale konu kişisel verilerin niteliği,
- Özel nitelikli kişisel veri bulunup bulunmadığı,
- Etkilenen kişi veya kayıt sayısı,
- Verilerin yetkisiz kişilerin eline geçip geçmediği,
- İhlalin ilgili kişiler açısından oluşturabileceği riskler,
- İlgili kişilere bildirim gerekip gerekmediği,
- Kişisel Verileri Koruma Kurumuna bildirim gerekip gerekmediği değerlendirilir.

4.4. Olayın Kontrol Altına Alınması ve Müdahale

Olayın etkisini azaltmak ve yayılmasını önlemek amacıyla olayın niteliğine uygun teknik ve idari tedbirler alınır.

Gerektiğinde;

- Kullanıcı hesabı geçici olarak devre dışı bırakılır,

- Ağ veya sistem erişimleri sınırlandırılır,
- Etkilenen sistem izole edilir,
- Zararlı yazılım bulaşmış sistemler karantinaya alınır,
- Güvenlik açıkları giderilir,
- Yedeklerden geri dönüş yapılır,
- Gerekli sistem veya hizmetler kontrollü şekilde durdurulur.

Müdahale sırasında olayın araştırılması için gerekli loglar, sistem kayıtları ve diğer teknik kanıtların korunması sağlanır.

4.5. Kanıtların Toplanması ve Korunması

- Olayın araştırılması, disiplin süreci veya hukuki süreç açısından gerekli olabilecek kanıtların bütünlüğü korunur.
- Dijital kanıtların toplanması, saklanması ve gerektiğinde ilgili mercilere sunulması sırasında kanıtın kaynağı, elde edilme zamanı, kim tarafından alındığı ve yapılan işlemler kayıt altına alınır.
- Kanıtların bütünlüğünün korunması amacıyla erişim ve işlem kayıtları tutulur.
- Gerektiğinde adli bilişim konusunda uzman kişi veya kuruluşlardan destek alınabilir.

4.6. Raporlama ve Bildirim

4.6.1. İç Bildirimler

- Olayın önem derecesine göre ilgili yöneticiler, Bilgi İşlem Daire Başkanlığı, KVYS /SOME sorumluları ve gerektiğinde Üst Yönetim bilgilendirilir.
- Olayın bilgi sistemlerinin sürekliliğini ciddi şekilde etkilediği durumlarda Kriz / Acil Durum Yönetimi ve İş Sürekliliği süreçleri devreye alınabilir.

4.6.2. Dış Bildirimler

Kişisel veri ihlali veya bilgi güvenliği olayı sonucunda mevzuat, sözleşme veya diğer yükümlülükler kapsamında yapılması gereken bildirimler, yetkili birimler tarafından ilgili süre ve usullere uygun olarak gerçekleştirilir.

Kişisel veri ihlallerinde 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili ikincil düzenlemeler dikkate alınır.

Bildirim yükümlülüğü olayın niteliği, kapsamı ve ilgili mevzuat hükümleri değerlendirilerek belirlenir. GDPR'da yer alan 72 saatlik bildirim süresi, yalnızca GDPR'ın uygulanabildiği durumlarda dikkate alınır; Türkiye'deki KVKK olayları için doğrudan GDPR süresi olarak uygulanmaz.

İlgili kişilere yapılması gereken bilgilendirmeler, uygulanabilir mevzuat ve yetkili makamların kararları doğrultusunda gerçekleştirilir.

4.7. Olayın Sonlandırılması

Olayın kontrol altına alınması ve gerekli müdahalelerin tamamlanmasından sonra;

- Olayın nedeni,
- Olayın etkisi,
- Alınan önlemler,
- Yapılan düzeltmeler,
- Kalan riskler,
- Yeniden oluşma ihtimali değerlendirilir.

Gerekli kontroller tamamlandıktan sonra olay kaydı kapatılır.

4.8. Kök Neden ve Düzeltici Faaliyet

Önemli veya tekrarlayan olaylarda kök neden analizi gerçekleştirilir. Gerekli görülen durumlarda;

- Teknik kontroller,
- İdari kontroller,
- Fiziksel güvenlik kontrolleri,
- Erişim yetkileri,
- Politika ve prosedürler,
- Eğitim ve farkındalık faaliyetleri gözden geçirilir.

Tespit edilen uygunsuzluklar için gerekli olması halinde Düzeltici Faaliyet Prosedürü uygulanır.

4.9. Öğrenme ve İyileştirme

Olaylardan elde edilen deneyimler;

- Risk değerlendirmelerinin güncellenmesi,
- Yeni güvenlik kontrollerinin belirlenmesi,
- Mevcut kontrollerin iyileştirilmesi,
- Politika ve prosedürlerin güncellenmesi,
- Personel eğitimlerinin planlanması amacıyla kullanılır.

Önemli olayların sonuçları gerektiğinde EYS kapsamında gerçekleştirilen yönetim gözden geçirme ve iyileştirme çalışmalarında değerlendirilir.

4.10. Kayıtların Saklanması

Olay kayıtları, bildirimler, loglar, teknik raporlar, kanıt kayıtları ve ilgili diğer belgeler; ilgili mevzuat, EYS doküman ve kayıt yönetimi kuralları ile belirlenen saklama sürelerine uygun olarak korunur.

Kişisel veri içeren olay kayıtlarının saklanmasında ayrıca Kişisel Verilerin İşlenmesi, Saklaması ve İmhası Politikası hükümleri uygulanır.

5. GİZLİLİK

Olaylara ilişkin teknik bilgiler, kişisel veriler, güvenlik açıkları, loglar, kanıtlar ve olay raporları yalnızca görev ve yetki kapsamında erişmesi gereken kişilerle paylaşılır.

Olayla ilgili bilgilerin yetkisiz kişilerle paylaşılması, olayın araştırılmasını, müdahalesini veya ilgili kişilerin haklarının korunmasını olumsuz etkileyebilecek durumlar dikkate alınarak engellenir.

6. YAPTIRIM

Bu politika kapsamında belirlenen kurallara aykırı uygulamalar EYS kapsamında uygunsuzluk olarak değerlendirilir. Çalışanların bilgi güvenliği veya kişisel veri koruma yükümlülüklerine aykırı davranışları için ilgili mevzuat, Üniversite düzenlemeleri ve Disiplin Prosedürü hükümleri uygulanır. Hizmet sağlayıcı ve üçüncü tarafların ihlalleri sözleşme hükümleri kapsamında değerlendirilir. Gerekli durumlarda ilgili olay veya ihlal yetkili kamu kurum ve kuruluşlarına bildirilir.