1. AMAÇ

Bu prosedürün amacı; Süleyman Demirel Üniversitesi Daire Başkanlıklarında uygulanmakta olan Bilgi güvenliği gereklerinin yasal altyapısını açıklamak ve yasalara uyumu kontrol etmek için bir çerçeve sunmaktır.

2. KAPSAM

Bu prosedür; Süleyman Demirel Üniversitesi Daire Başkanlıklarında Bilgi Güvenliği Kapsamına dahil edilen tüm varlıkları kapsar.

3. SORUMLULUKLAR

Bu prosedürün işletilmesinden Süleyman Demirel Üniversitesi Daire Başkanlıklarındaki tüm personel sorumludur.

4. UYGULAMA

4.1.Kurumsal Ve Yasal Kurallara Uyum Esasları

- Birimde çalışan tüm yönetici ve çalışan personel kapsamında yer alan her şahıs, Hizmet alımı olarak firmalar tarafından Kurum kaynaklarını kullanmakta olan üçüncü taraflar, tedarikçiler kurum Bilgi Güvenlik politikası ve konu ile ilgili düzenlenmiş her türlü yasal kurallara uyma zorunluluğundadırlar. Aykırı durumlar söz konusu olduğu hallerde Kurum içi ya da hukuki cezalandırmaya tabi tutulacaklarını bilmektedirler.
- Kurum kaynaklarının kullanımı esnasında oluşacak yasal veya Kurum içi düzenlemelere aykırı faaliyetlerin kayıtlarının tutulması ve gerektiğinde delil olarak yetkili makamlara verilmesi Kurum sorumluluğundadır.
- Kurumda uygulanan bilgi güvenliği politikaları, kaynakların oluşturulması ve sunumu ve kullanımı fikri mülkiyet hakları, personel yasaları ve diğer ilgili yasalara uygun olacaktır.
- Uygulanabilir yasalar Dış Kaynaklı Doküman Listesi ile tanımlanmış ve güncelliği sağlanmaktadır.

4.2.Fikri Mülkiyet Hakları

- Film, müzik, kitap, makale vb. materyallerin, 5846 sayılı Fikir ve Sanat Eserleri Kanunu hükümlerine aykırı şekillerde saklanması ve paylaşılması yasaktır.
- Kurum'da, yalnızca lisans sözleşmeleri kapsamındaki yazılımlar kullanılır. Lisanssız ürünlerin Kurum'a ait bilgi varlıklarında kullanılması yasaktır.
- Ürünlere ilişkin lisanslar, güvenilir kaynaklardan temin edilir.

- Herhangi bir bilişim suçu işlediği saptanan çalışan, yasalara uygun olarak cezai işlem görür.

- Bilgi güvenliği olayı için kanıt oluşturabilecek (yazışmalar, internet erişim kayıtları, DHCP kayıtları) herhangi bir veri, yetkililer gelene kadar değişime uğramayacak ve kanıt özelliğini kaybetmeyecek şekilde saklanacaktır.

4.3.Kayıtların Korunması

- Bilgi sistemlerinin kullanımına ilişkin kayıtların tutulması ve gerektiğinde kanıt olarak yetkili makamlara sunulması, BGYS Komisyonu'nun sorumluluğundadır.

- Kayıt saklama süreleri ve ortamları, T.C. ilgili yasa ve mevzuatına uygun şekilde belirlenir.

4.4.Kişisel Verilerin Korunması

- BGYS Kapsamı dokümanında belirtilen tüm taraflara ilişkin, elde ettiği kişisel verileri korumayı taahhüt eder. Bu kapsamda, yöneticilerine, çalışanlarına ve hizmet sağlayıcılarına sorumluluklarına ilişkin bilgilendirme ve uyarıları yapar. Bunun için kurumumuzda KVKK çalışmaları başlatılmış ve Kişisel Verilerin Korunması ve İşlenmesi Politikası hazırlanmış ayrıca Kişisel Verilerin Korunması Kanunu Uygulama Yönergesi hazırlanmıştır.

4.5.Bilgi Güvenliği Gözden Geçirmeleri

1) Bilgi Güvenliğinin Bağımsız Gözden Geçirmesi

Kuruluşun bilgi güvenliğine ve BGYS 'ye uyumunu sağlamak amacıyla yılda en az birer kez iç denetim ve teknik gözden geçirme faaliyetleri yürütülür.

Bilgi Güvenliği uygulamaları belgelendirme denetimleri ve gözetim denetimleri ile belgelendirme kuruluşları tarafından gözden geçirilmektedir. Bulunan uygunsuzluklar YGG toplantıları için girdi oluşturmaktadır.

2) Güvenlik Politikaları ve Standartları ile Uyum

Güvenlik politikaları ve standartlar ile uyum Üst Yönetim tarafından YGG toplantıları ile gözden geçirilmektedir.

3) Teknik Uyum Gözden Geçirmesi

- Firma tarafından kabul edilmiş kapsam ve formatta her türlü veri kapsamında yer alan her türlü bilgi, bulundukları ortam ve değer seviyelerine göre yasal ve akdi düzenlemelere uygun olarak yedeklenmeli ve yedekleme ortamlarının zaman içinde zarar görme ihtimali göz ardı edilmez.

- Yedekleme ortamlarının periyodik testlerle kontrolleri yapılır.
- Ömrünü doldurmuş ortamlar imha kurallarına uygun olarak ortadan kaldırılmalıdır.
- Ağ üzerinde yapılan her türlü erişim ve hareketler kayıt altına alınmalı yetkisiz erişim ve kural dışı kullanım tespit edilen durumları ilgili prosedürlerle uygulanır.
- Bilgi sistemleri ortamları komite tarafından belirlenmiş kurum içi personel ya da kurum dışı firmalar tarafından teknik testlere tabi tutulmalıdır.
- Testler sonrası tespit edilen kritik açıklıklar anında müdahale edilmelidir. Bu testler en az yılda bir kez tüm sistemler için belirlenmiş prosedürlere uygun olarak uygulanmalıdır.
- Denetleme gereksinim ve aktiviteleri dolayısıyla çalışmakta olan sistemler üstünde kontroller yapılırken, iş sürecinin asgari düzeyde zarar görmesi için dikkatle planlanmalıdır. Sonuçlar YGG Toplantılarında gözden geçirilmektedir.

Bu genel esasların yanında ISO 27001, ISO 9001, ISO 22301, ISO 20000-1 ve ISO 27701 Kapsamlı Politika, Prosedürleri ve yazılı belge haline getirilmiş tüm bilgiler ve kurum içi intranet sayfamızda yayınlanmıştır.

Kurumun üst yönetimi dâhil olmak üzere tüm Kurum çalışanları ve 3. taraflar, Kurum tarafından belirlenmiş ve dokümante edilmiş Politika ve Prosedürlere uygun hareket etmek zorundadır. Uygunsuz hareketler ve aykırılık sebepli suç kapsamında olan her eylem disiplin hükümleri ve / veya yasal yaptırımlarla cezai işlem göreceklerdir.

5. İLGİLİ DOKÜMANLAR

- LST-014 Dış Kaynaklı Doküman Listesi
- PLT-016 Kişisel Verilerin Korunması ve İşlenmesi Politikası
- YNR-001 Kişisel Verilerin Korunması Kanunu Uygulama Yönergesi

6. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	22.10.2021	İlk yayın.
001	22.01.2024	Kontrol kısmı güncellenmiştir.
002	22.12.2024	***"Bu genel esasların yanında ISO 27001, ISO 9001, ISO 22301, ISO 20000-1 ve ISO 27701 Kapsamlı Politika, Prosedürleri ve yazılı belge haline getirilmiş tüm bilgiler ve kurum içi intranet sayfamızda yayınlanmıştır." Şeklinde düzenlenmiştir.***
