T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI
ENTEGRE YÖNETİM SİSTEMİ POLİTİKALARI YÖNERGESİ

BİRİNCİ BÖLÜM
Başlangıç Hükümleri

Amaç

MADDE 1–(1) Bu Yönerge; Üniversitemizin ihtiyaç duyduğu bilginin üretilmesi, saklanması, korunması ve paylaşımı sürecinde; bilgisayar ağı, internet alt yapısı ve tüm bilişim kaynakları ile ilgili yasalara, TÜBİTAK ULAKBİM' in ilgili politikalarına ve TS EN ISO/IEC ISO 27001 Bilgi Güvenliği Yönetim Sistemi, TS EN ISO 9001 Kalite Yönetim Sistemi, TS EN ISO 22301 İş Sürekliliği Yönetim Sistemi, TS ISO/IEC ISO 20000-1 Bilgi Teknolojileri Hizmet Yönetim Sistemi ve ISO 27701 Kişisel Veri Yönetim Sistemi ve standartlarına uygun olarak, etkin ve verimli kullanımını sağlayacak kuralları belirlemek ve ilgili politikaları üretmek amacıyla hazırlanmıştır.

Kapsam

MADDE 2– (1) Bu Yönerge; Süleyman Demirel Üniversitesi personelleri ve öğrencileri ile kendilerine herhangi bir nedenle geçici ve/veya kısıtlı olarak bilişim kaynaklarımızı kullanma yetkisi verilen paydaş ve ziyaretçilerin uyması gereken bilişim politikalarını ve kurallarını kapsar.

Dayanak

MADDE 3– (1) Bu Yönerge, 5237 sayılı Türk Ceza Kanunu'nun İkinci Kısmı (Kişilere Karşı Suçlar) Dokuzuncu Bölümü (Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar-132, 133, 134, 135, 136, 137, 138, 139, 140. Maddeler), Üçüncü Kısmı (Topluma Karşı Suçlar) Onuncu Bölümü (Bilişim Alanında Suçlar-243, 244, 245, 246. Maddeler), 5070 sayılı "Elektronik İmza Kanunu", 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", 2547 sayılı Yükseköğretim Kanununun 12. Maddesi ile 5018 sayılı "Kamu Mali Yönetimi ve Kontrol Kanunu", 2007/4 Sayılı "Kamu Kurumları İnternet Sitesi Kılavuzu" Genelgesine, diğer ilgili mevzuat hükümlerine, 6698 Sayılı "Kişisel Verilerin Korunması Kanunu'na, 7258 Sayılı "Siber Güvenlik Kanunu'na, Ulusal Akademik Ağ (ULAKNET) Kullanım Politikasına ve TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, ISO 9001 Kalite Yönetim Sistemi, ISO 22301 İş Sürekliliği Yönetim Sistemi, ISO 20000-1 Bilgi Teknolojileri Hizmet Yönetim Sistemi ve ISO 27701 Kişisel Veri Yönetim Sistemi ve ISO 27018 Bulut Ortamında Kişisel Verilerin Korunması standartlarına dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4– (1) Bu yönergede geçen;

a) Bilgi İşlem Daire Başkanlığı (BİDB): Süleyman Demirel Üniversitesi adına, Süleyman Demirel Üniversitesi bilişim kaynaklarını yönetme, geliştirme, kontrol etme, her türlü bakım ve onarım işlemleri ile hizmetlerin tümünü gerçekleştiren yetkili birimi,

b) Bilgisayar Ağı: Bilgisayarlar arasında veri/bilgi aktarımı ve etkileşimini sağlayan, geniş ve dar alanlar bütünlüğünde fiziki ağ yapısı ile bunu destekleyen ve kullanımını gerçekleştirmeye yarayan tüm donanım ve yazılımların oluşturduğu sistemi,

c) Bilişim Destek Hizmetleri: Süleyman Demirel Üniversitesi Bilişim Kaynaklarının kurulumu, kullanıma sunumu, bakımı, onarımı ve diğer teknik destekler ile ilgili Rektörlükçe

belirlenen yetki ve sorumluluk düzeylerinde Bilgi İşlem Daire Başkanlığı ve Bilişim Kaynaklarını Kullanıma Sunan Birimlerce yerine getirilen hizmetleri,

ç) Bulut Bilişim Hizmetleri: Üniversite tarafından kullanılan, ağ üzerinden erişilebilen, ölçeklenebilir ve esnek bilgi işlem kaynakları ile hizmetlerin toplamını,

d) Diğer Kullanıcılar: Süleyman Demirel Üniversitesi Bilişim Kaynaklarının kullanım hakkına sahip Esas Kullanıcılar dışındaki, özel veya tüzel kişiliğinde olup kullanım hakları ve biçimleri Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından belirlenen tüm kısıtlı veya geçici kullanım hakkı verilmiş kullanıcıları,

e) Entegre Yönetim Sistemleri (EYS): ISO 27001 Bilgi güvenliği Yönetim Sistemi, ISO 9001 Kalite Yönetim Sistemi, ISO 22301 İş Sürekliliği Yönetim Sistemi, ISO 20000-1 Bilgi Teknolojileri Hizmet Yönetim Sistemi ve ISO 27701 Kişisel Veri Yönetim Sistemi standartlarını ve bu standartların yönetimini,

f) Esas Kullanıcılar: Süleyman Demirel Üniversitesi Bilişim Kaynaklarını eğitim-öğretim, araştırma, yönetim ve hizmet faaliyetleri çerçevesinde kullanan Süleyman Demirel Üniversitesi akademik ve idari görevlerindeki kadrolu, geçici veya sözleşmeli personel ile Süleyman Demirel Üniversitesinde öğrenimini sürdürmekte olan kayıtlı tüm önlisans, lisans ve lisansüstü öğrencilerini,

g) İnternet Altyapısı: Ulusal ve uluslararası bilgisayar ağı üzerinde tüm kullanıcı uçlarının adres yapılarını ve veri/bilgi iletişimi kurallarını içeren belirli protokoller ile etkileşimi ve iletişimini sağlayan sistemini,

ğ) Kişisel Bilişim Kaynakları: Süleyman Demirel Üniversitesi bilişim ve iletişim varlıkları kullanım yönergesinde tanımlanan usul, esas ve diğer kullanıcılara ait taşınabilir bilgi işleme ve depolama cihazları, mobil bilgisayarlar, tablet ve cep telefonları, kablolu ve kablosuz ağ cihazları, bilgisayar sistemleri, donanım, yazılım ve hizmetlerin tümünü,

h) Kullanım: Süleyman Demirel Üniversitesi Bilişim Kaynaklarının ULAKNET tarafından belirlenen kullanım politikası kapsamındaki, eğitim-öğretim, araştırma, uygulama, yönetim ve hizmet sunumu faaliyetleri ile ilgili kullanımları,

ı) Siber Güvenlik: Bilgi sistemlerinin ve ağlarının siber saldırılara karşı korunması, siber tehditlerin tespit edilmesi ve müdahale edilmesi için alınan önlemlerin tümünü

i) Süleyman Demirel Üniversitesi Bilişim Kaynakları: Mülkiyeti veya kullanım hakkı Süleyman Demirel Üniversitesine ait olan, Süleyman Demirel Üniversitesince kiralanan veya lisanslanan bilgisayar ağı, internet altyapısı, bilgisayar sistemi, donanımı, yazılımı ve hizmetlerinin tümünü,

j) Süleyman Demirel Üniversitesi Bilişim Kaynaklarını Kullanıma Sunan Birimler: Süleyman Demirel Üniversitesi Bilişim Kaynaklarını kullanıma sunan akademik birimler (fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, araştırma ve uygulama merkezleri, hastane vb.), idari birimler (daire başkanlıkları, müdürlükler) ile spor, kültür, sosyal etkinliklerin yürütüldüğü birimleri,

k) Web Siteleri: Fakülte, Yüksek Okullar, Araştırma Merkezleri, İdari Birimler, Meslek Yüksek Okulları, Enstitüler, Sosyal Faaliyet Kulüpleri ve kullanıcıya tahsis edilen web sayfalarının tümünü,

ifade eder.

İKİNCİ BÖLÜM
Temel İlkeler

EYS tesisi için gerekli temel ilkeler

MADDE 5– (1) Üniversitemizde yer alan birimlerde, başta kişisel verileri olmak üzere, yazılı veya elektronik ortamda saklanan her türlü bilginin gizlilik, bütünlük ve erişilebilirliğinin sağlanması amacıyla EYS tesis edilir.

(2)EYS'nin tesis edilmesi ve etkin bir şekilde işletilmesi için, üst yönetim desteği ve katılımı zorunludur.

(3)EYS tesis edilmesi için alınması gereken tedbirler, bilgi güvenliği yönetim sistemi politikaları ve kurumların kendilerine özgü güvenlik ihtiyaçları dikkate alınmak suretiyle ayrıntılı olarak belirlenir, yazılı hale getirilir ve tüm kullanıcılara duyurulur.

(4)Etkin bir EYS tesis edilmesi için risk yönetimi yapılır. Tespit edilen riskler için riski azaltacak veya kaldıracak tedbirler belirlenir, üst yönetime sunulur ve uygulanır. Risk yönetimi süreçleri süreklilik arz eder.

(5)Yapay zeka ve otomatize edilmiş karar verme sistemlerinin kullanımında etik ilkeler ve şeffaflık esastır. Bu sistemlerin kullanımı ile ilgili politikalar ayrıca belirlenir.

(6)Bilgi işleme faaliyetlerinin büyük oranda siber ortam üzerinden yapılması nedeniyle, siber güvenlik tedbirlerinin alınması için azami özen gösterilir.

(7)Bilgi güvenliğinin sağlanması için sadece siber güvenlik ile ilgili tedbirlerin alınması yeterli değildir. Personel, evrak, ekipman, fiziksel ve çevre güvenliği için de güvenlik tedbirleri alınması gerekir.

(8)Kullanıcılar, EYS politikalarına uymak ve görevlerini ifa ederken öğrenmiş oldukları bilgileri, sır saklama yükümlülüğü uyarınca süresiz olarak saklamakla yükümlüdür.

(9)Bulut bilişim hizmetlerinin kullanımında veri yerleşimi, veri taşınabilirliği ve satıcı bağımlılığı riskleri dikkate alınır.

(10) Sürdürülebilirlik ilkeleri çerçevesinde enerji verimliliği ve çevresel etki gözetilerek bilişim kaynaklarının kullanımı planlanır.

ÜÇÜNCÜ BÖLÜM
Yetki ve Sorumluluk

Yetki ve sorumluluğun atanması

MADDE 6– (1) Üniversitede İnternet ağının kurulum ve işletmesine ait yetki ve sorumluluk BİDB'ye aittir. BİDB, akademik, idari, eğitim ve araştırma amaçları doğrultusunda bölüm ve birimlerin bilişim kaynaklarına ulaşabilmelerini sağlamak üzere oluşturulan altyapıyı kurmak, işletmek ve güncellemekle sorumludur. BİDB, bölüm ve birimlerde tespit edilen ana ağ erişim noktalarını kurar, bilgi işlem merkezi ile iletişimi için gerekli faaliyetlerini yürütür, bu noktalara kullanıcıların bağlanabilmesi için gerekli ağ anahtarlama cihazlarını temin eder ve yerleştirir. Sistemi teknik düzeyde planlama ve uygulama sorumluluk ve yetkisi BİDB'dedir. BİDB gereken durumlarda ve istek üzerine danışmanlık hizmeti verebilir.

(2)Üniversite bilişim kaynakları kullanıcıları, Üniversite sunucuları üzerinde kendilerine tahsis edilen kullanıcı kodu/şifre ikilisi ve/veya IP (Internet Protocol) adresi kullanılarak gerçekleştirdikleri her türlü etkinlikten, Üniversite bilişim kaynaklarını kullanarak oluşturdukları ve/veya kendilerine tahsis edilen Üniversite bilişim kaynağı üzerinde bulundurdukları her türlü kaynağın (belge, doküman, yazılım, vb.) içeriğinden, kaynağın kullanımı hakkında yetkili makamlar tarafından talep edilen bilgilerin doğru ve eksiksiz verilmesinden, ilgili kaynağın kullanım kurallarına, kanun ve yönetmeliklere karşı sorumludur.

(3)BİDB, Üniversite bilişim kaynakları kullanımı hakkında genel politikaları belirler, bu politikaları gelişen teknolojinin öngördüğü biçimde sürekli olarak değerlendirir ve gerekli değişiklikleri hayata geçirir. Bu tür değişiklikler yapıldığında genel duyuru mekanizmaları ile kullanıcılar bilgilendirilir.

(4)BİDB tarafından EYS kapsamında hazırlanan politikalara kullanıcılar uymak zorundadır.

(5)BİDB, siber güvenlik olaylarının tespit edilmesi, müdahale edilmesi ve raporlanması konularında sorumludur ve bu kapsamda gerekli organizasyonel yapıyı kurar.

(6)Kişisel verilerin işlenmesi ile ilgili olarak BİDB, KVKK kapsamındaki yükümlülükleri yerine getirmekle sorumludur.

DÖRDÜNCÜ BÖLÜM
Politikaların Hazırlanması ve Uygulanması

Politikaların hazırlanması ve uygulanması aşamaları

MADDE 7– (1) EYS politikaları, BİDB tarafından ilgili yasalara aykırı olmayacak şekilde ve TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, ISO 9001 Kalite Yönetim Sistemi, ISO 22301 İş Sürekliliği Yönetim Sistemi, ISO 20000-1 Bilgi Teknolojileri Hizmet Yönetim Sistemi ve ISO 27701 Kişisel Veri Yönetim Sistemleri standartlarına uygun olacak şekilde hazırlanır.

(2)Hazırlanan politikalar, BİDB web sayfasında yayınlanarak hem personele hem de öğrencilere duyurulur.

(3)Hazırlanan politikalar, planlanan zaman aralıklarında veya teknik gereklilikler ortaya çıktığında uygunluğu, elverişliliği ve etkinliğinin sürekliliğini belirlemek amacıyla BİDB bünyesindeki Kalite Birimi tarafından kontrol edilir.

(4)Politikaların yeniden bir bütün olarak yayımlanmasını gerektirmeyen küçük çaplı değişiklikler, değişiklik eki olarak hazırlanır. Değişiklik ekleri, dokümanların yürürlükteki sürümleri üzerine işlenmek suretiyle takip edilir.

(5)Politikalarda önemli ölçüde değişiklik yapılmasını gereken durumlarda, yeni sürümler bir bütün olarak yayımlanır.

(6)Süleyman Demirel Üniversitesi bilişim alt yapısını kullanan tüm kullanıcılar ilgili politika ve prosedürdeki kuralları bilmeli ve bu kurallara uymalıdır.

(7)BİDB çalışanları, EYS kapsamında belirlenen prosedürlere ve politikalara göre hareket ederler. Bu politika ve prosedürlere uymayan talepler yerine getirilmez.

(8)Kullanıcılar, ilgili kanunlara, politikalar kapsamında belirtilen esaslara ve TÜBİTAK ULAKBİM kullanım politikası esaslarına uymak kaydıyla, bilişim kaynaklarını esas kullanıcı veya diğer kullanıcı tanımları ve yetkileri çerçevesinde kullanma ve belirtilen hizmetleri alma hakkına sahiptir.

(9)Yapay zeka destekli sistemlerin kullanımında şeffaflık, hesap verebilirlik ve insan denetimi ilkeleri gözetilir. Bu sistemlerin karar verme süreçlerinde insan müdahalesi ve denetimi sağlanır.

BEŞİNCİ BÖLÜM
Yaptırım ve Son Hükümler

Yaptırım

MADDE 8– (1) EYS politikalarına ve sır saklama yükümlülüğüne uymayanlar hakkında, 657 sayılı Devlet Memurları Kanunu, 2547 sayılı Yükseköğretim Kanunu, iş sözleşmesinin ilgili hükümleri ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ve 7258 sayılı Siber Güvenlik Kanunu'nun ilgili hükümleri uyarınca işlem yapılır.

(2) BİDB, Üniversitenin tüzel kişiliğini ve güvenliğini korumak amacıyla yasalara uygun olarak kısıtlayıcı ve engelleyici önlemler alır.

(3)BİDB, EYS politikalarına ve ilgili diğer yönergelere uymayan kullanıcıların hesabını iptal etme veya geçici bir süreliğine dondurma, sunduğu hizmetin şeklini değiştirme veya son verme hakkına sahiptir.

(4)Siber güvenlik olayları durumunda, BİDB yetkili mercilere derhal bildirimde bulunur ve gerekli müdahale tedbirlerini alır.

Hükümler

MADDE 9− (1) Bu Yönergede hüküm bulunmayan hallerde; ilgili mevzuat hükümleri ile Yükseköğretim Kurulu, Senato ve ilgili Yönetim Kurulu Kararları uygulanır.

Yürürlük

MADDE 10– (1) Bu Yönerge Süleyman Demirel Üniversitesi Senatosu tarafından kabul edildiği tarihte yürürlüğe girer.

Yürütme

MADDE 11– (1) Bu Yönerge hükümlerini Süleyman Demirel Üniversitesi Rektörü yürütülür.

Süleyman Demirel Üniversitesi Senatosunun 01/08/2025 tarih ve 651/12 nolu Toplantı Kararına istinaden yürürlüğe girmiştir.