1. AMAÇ

Bu politika; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında görev, birim veya sorumluluk değişikliği gerçekleşen ya da Üniversite ile iş ilişkisi sona eren personelin; bilgi sistemleri, bilgi varlıkları, kullanıcı hesapları, erişim yetkileri, donanım, yazılım ve diğer kurumsal varlıklara ilişkin erişim ve kullanım haklarının güvenli, kontrollü ve zamanında yönetilmesini amaçlamaktadır.

Politika ile bilgi güvenliğinin, kişisel verilerin korunmasının, hizmetlerin sürekliliğinin ve kurumsal bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunması hedeflenmektedir.

2. KAPSAM

Bu politika;

- Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik, Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi kapsamında görev yapan ve Üniversitenin bilgi sistemleri, uygulamaları, ağ kaynakları, elektronik iletişim hizmetleri, bilgi varlıkları ve diğer kurumsal kaynaklarına erişimi bulunan personeli kapsar.

Politika;

- görev veya birim değişikliği,
- yetki ve sorumluluk değişikliği,
- geçici veya sürekli görev değişikliği,
- Üniversite ile iş ilişkisinin sona ermesi durumlarında uygulanır.

Üçüncü taraflar ve hizmet sağlayıcıların görev veya erişim durumlarının sona ermesi halinde, ilgili sözleşme ve EYS hükümleri doğrultusunda bu politikanın ilgili hükümleri uygulanır.

3. SORUMLULUKLAR

3.1. Personel Özlük İşleri

Personelin görev değişikliği veya iş ilişkisinin sona ermesine ilişkin bilgilerin ilgili birimlere zamanında iletilmesini sağlamak,

- Personel bilgilerinin ilgili sistemlerde güncel tutulmasını sağlamak,
- İşten ayrılma ve görev değişikliği süreçlerinde gerekli kayıtların oluşturulmasını sağlamak.

3.2. İlgili Birim Amiri

- Personelin yeni görevine ilişkin erişim ihtiyaçlarını belirlemek,
- Personelin önceki görevinden kaynaklanan ve artık ihtiyaç duyulmayan erişimlerin kaldırılmasını talep etmek,
- Kurumsal bilgi, dosya, donanım, yazılım ve diğer varlıkların teslim alınmasını sağlamak,

- İşten ayrılma durumunda personelin üzerinde bulunan kurumsal varlıkların teslim edilmesini sağlamak.

3.3. Bilgi İşlem Daire Başkanlığı (BİDB)

- Kullanıcı hesaplarının ve teknik erişim yetkilerinin görev değişikliği veya işten ayrılma durumuna göre düzenlenmesini sağlamak,
- Yetkilendirme, erişim kısıtlama ve hesap kapatma işlemlerini gerçekleştirmek,
- Gerekli durumlarda e-posta, ağ, uygulama, Active Directory ve diğer bilgi sistemlerindeki kullanıcı erişimlerini yönetmek,
- Gerçekleştirilen işlemlere ilişkin kayıtları tutmak ve gerekli kanıtları muhafaza etmek.

3.4. Personel

- Görev değişikliği veya işten ayrılma sürecinde kendisine teslim edilmiş kurumsal bilgi ve varlıkları ilgili birime teslim etmek,
- Yeni görevinde kendisine tanımlanmayan bilgi ve sistemlere erişmeye çalışmamak,
- Görev değişikliği veya işten ayrılma sonrasında yetkisi kaldırılan bilgi ve sistemlere erişmemek,
- Üniversiteye ait bilgi ve kişisel verilerin gizliliğini korumaya devam etmek.

4. UYGULAMA

4.1. Görev veya Birim Değişikliği

Görev veya birim değişikliği gerçekleşecek personelin;

- adı ve soyadı,
- mevcut birimi ve görevi,
- yeni birimi ve görevi,
- görev değişikliğinin yürürlük tarihi,
- ihtiyaç duyulan yeni bilgi sistemi, yazılım, donanım veya erişimler

ilgili birim tarafından belirlenerek yetkili kanallar üzerinden ilgili birimlere bildirilir.

Görev değişikliğinin yürürlüğe girmesinden önce veya kurum tarafından belirlenen uygun süre içerisinde personelin mevcut erişim yetkileri gözden geçirilir.

4.2. Erişim Yetkilerinin Yeniden Düzenlenmesi

Görev değişikliğinde personelin önceki görevine bağlı;

- kullanıcı hesapları,
- uygulama yetkileri,
- ağ ve paylaşım alanları,
- ortak klasörler,
- veri tabanı veya uygulama erişimleri,
- uzaktan erişim yetkileri,
- diğer bilgi sistemi ve kaynak erişimleri gözden geçirilir.

Yeni görev için gerekli olmayan önceki erişim yetkileri kaldırılır veya kısıtlanır.

Yeni görev kapsamında ihtiyaç duyulan erişimler ise ilgili birim amirinin talebi ve yetkilendirme kuralları doğrultusunda tanımlanır.

Personelin yeni görevine ilişkin erişim yetkileri, **görev gerekliliği ve en az yetki prensibi** esas alınarak belirlenir.

4.3. Eski Birime Ait Bilgi ve Varlıkların Teslimi

Görev değişikliği yapan personelin önceki görevinde kullandığı;

- bilgisayar ve diğer donanımlar,
- taşınabilir cihazlar ve ortamlar,
- yazılım ve lisanslar,
- kurumsal dosya ve kayıtlar,
- anahtar, kart ve benzeri fiziksel erişim araçları,
- diğer kurumsal varlıklar

ilgili birim tarafından değerlendirilir ve gerekli görülenler teslim alınarak kayıtları güncellenir.

Kurumsal bilgi ve kayıtların personelin kişisel alanında veya yetkisiz erişilebilecek ortamlarda bırakılmaması sağlanır.

4.4. Yeni Göreve İlişkin Donanım ve Yazılım İhtiyaçları

Yeni görevi nedeniyle personelin farklı bir donanım, yazılım veya bilgi sistemi erişimine ihtiyaç duyması halinde ilgili talep yetkili birim tarafından BİDB'ye iletilir.

Donanım, yazılım ve erişim tahsisleri ilgili prosedürler, bilgi varlıkları yönetimi ve yetkilendirme kuralları doğrultusunda gerçekleştirilir.

4.5. İşten Ayrılma Bildirimi

Üniversite ile iş ilişkisi sona erecek personelin;

- adı ve soyadı,
- birimi ve görevi,
- iş ilişkisinin sona ereceği tarih ve gerektiğinde saat,
- varsa teslim edilmesi gereken kurumsal varlıklar yetkili birimler tarafından belirlenen yöntemle ilgili birimlere bildirilir.

İşten ayrılma bildiriminin, erişimlerin zamanında sonlandırılmasını sağlayacak şekilde mümkün olan en erken zamanda yapılması esastır.

Acil veya beklenmeyen ayrılma durumlarında erişimlerin gecikmeksizin sınırlandırılması veya sonlandırılması sağlanır.

4.6. Kullanıcı Hesaplarının ve Erişimlerin Sonlandırılması

İşten ayrılan personelin;

- Active Directory hesabı,
- uygulama hesapları,
- ağ erişimleri,
- uzaktan erişim yetkileri,
- VPN ve benzeri erişimleri,
- ortak kaynak ve paylaşım alanlarına erişimleri,
- diğer bilgi sistemi erişimleri

ayrılışın gerçekleştiği tarih ve zaman dikkate alınarak sonlandırılır veya yetkisiz erişimi engelleyecek şekilde devre dışı bırakılır.

İşten ayrılan personele ait erişim yetkilerinin devam etmesine yönelik istisnalar ancak yetkili makamın onayı, belirlenmiş amaç ve süre kapsamında uygulanabilir.

Ayrılan personelin hesabı başka bir personele devredilmez ve kullanıcı adı, parola veya kimlik doğrulama bilgilerinin başka kişiler tarafından kullanılmasına izin verilmez.

4.7. Elektronik Posta Hesaplarının Yönetimi

İşten ayrılan personele ait elektronik posta hesabının kapatılması, erişimin engellenmesi, belirli bir süre tutulması veya kurumsal ihtiyaç doğrultusunda kontrollü şekilde yönetilmesi; ilgili mevzuat, bilgi güvenliği kuralları, iş sürekliliği ihtiyaçları ve Üniversitenin elektronik iletişim hizmetlerine ilişkin kurallar doğrultusunda gerçekleştirilir.

Ayrılan personelin elektronik posta hesabının başka bir personel tarafından kullanılması veya kullanıcı kimliğinin devredilmesi mümkün değildir.

Kurumsal iletişimin devamlılığının sağlanması gereken durumlarda, yetkili birimler tarafından uygun görülen teknik ve idari yöntemler kullanılır.

4.8. Kişisel Verilere Erişimin Sonlandırılması

Görev değişikliği veya işten ayrılma sonucunda personelin artık görev gereği erişmesi gerekmeyen kişisel verilere ve özel nitelikli kişisel verilere erişim yetkileri kaldırılır.

Kişisel verilere erişim, yeni görev kapsamında gerçekten ihtiyaç duyulması halinde ve yetkilendirme kuralları doğrultusunda yeniden tanımlanır.

Görev değişikliği veya işten ayrılma işlemleri sırasında kişisel verilerin yetkisiz kişilerle paylaşılmaması, aktarılmaması veya erişilebilir hale getirilmemesi sağlanır.

4.9. Kurumsal Bilgi ve Dosyaların Devri

Görev değişikliği veya işten ayrılma durumunda personelin yürüttüğü görev kapsamında oluşturduğu veya kullandığı kurumsal bilgi, belge, kayıt ve dosyalar ilgili birime teslim edilir veya Üniversitenin belirlediği kurumsal sistemlerde erişilebilir durumda tutulur.

Kurumsal bilgi ve kayıtların personelin kişisel e-posta hesabına, kişisel bulut depolama alanlarına veya yetkisiz harici ortamlara aktarılması yasaktır.

4.10. Donanım ve Diğer Varlıkların İadesi

İşten ayrılan veya görev değişikliği nedeniyle kendisine tahsis edilen varlıkların artık kullanımına ihtiyaç bulunmayan personel;

- bilgisayar,
- dizüstü bilgisayar,
- tablet ve mobil cihaz,
- taşınabilir depolama ortamları,
- donanım ve çevre birimleri,
- fiziksel erişim kartları/anahtarlar,
- diğer Üniversite varlıklarını ilgili birime teslim eder.

Teslim ve zimmet işlemleri ilgili envanter ve varlık yönetimi kayıtları üzerinden gerçekleştirilir.

Kullanım dışı bırakılan veya başka personele tahsis edilecek bilgi teknolojileri ekipmanlarında veri güvenliği işlemleri, Teçhizatın Elden Çıkarılması Politikası ve ilgili bilgi varlığı yönetimi hükümlerine göre yürütülür.

4.11. İşlemlerin Kayıt Altına Alınması

Görev değişikliği ve işten ayrılma kapsamında gerçekleştirilen;

- erişim yetkilerinin kaldırılması veya değiştirilmesi,
- kullanıcı hesaplarının devre dışı bırakılması,
- varlık ve zimmet teslimleri,
- e-posta hesabına ilişkin işlemler,
- bilgi ve dosya devirleri,
- gerekli diğer teknik ve idari işlemler izlenebilirliği sağlayacak şekilde kayıt altına alınır.

4.12. Gizlilik ve Sorumluluk

Görev değişikliği veya işten ayrılma sonrasında personelin görev süresince edindiği Üniversiteye ait gizli bilgiler, kişisel veriler ve erişim yetkileri kapsamında öğrendiği bilgiler bakımından ilgili mevzuat, sözleşmeler ve Üniversitenin EYS politika ve prosedürlerinden doğan yükümlülükleri devam eder.

5. YAPTIRIM

Bu politikaya aykırı hareket edilmesi halinde, olayın niteliğine göre ilgili mevzuat, Üniversitenin disiplin düzenlemeleri, sözleşme hükümleri ve EYS kapsamında belirlenen düzeltici/iyileştirici faaliyetler uygulanır.

Bilgi güvenliği veya kişisel veri ihlali niteliği taşıyan durumlar, Olay İhlal Bildirim ve Yönetim Politikası ve ilgili olay yönetimi süreçleri kapsamında değerlendirilir.