1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi bünyesinde bulunan bilgi varlıklarının yetkisiz erişim, görüntüleme, kullanma, değiştirme, kaybetme veya ifşa edilmesi risklerine karşı korunmasını sağlamak; fiziksel çalışma alanlarında ve bilgi sistemlerinde temiz masa ve temiz ekran kurallarını belirlemektir.

Bu politika kapsamında özellikle kişisel veri, özel nitelikli kişisel veri, kurum içi bilgiler, Hizmete Özel, Gizli ve Çok Gizli sınıfta bulunan bilgiler ile diğer hassas bilgi varlıklarının çalışma ortamında yetkisiz kişilerin erişimine açık bırakılmasının önlenmesi amaçlanmaktadır.

2. KAPSAM

Bu politika; Süleyman Demirel Üniversitesi bünyesinde görev yapan;

- Akademik ve idari personeli,
- İşçileri ve sözleşmeli personeli,
- Bilgi varlıklarına erişimi bulunan diğer çalışanları,
- Görevlendirme kapsamında kurumsal bilgi varlıklarına erişen ilgili tarafları, ve bu kişilerin kullandığı ofis, çalışma alanı, toplantı odası, arşiv, ortak kullanım alanları ve bilgi işlem çalışma ortamlarını kapsar.

Politika; basılı belgeler, bilgisayar ekranları, taşınabilir cihazlar, çıkarılabilir medya, yazıcı/fotokopi cihazları ve benzeri bilgi taşıyan fiziksel ve elektronik ortamları kapsar.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından, görev ve yetkileri kapsamında:

- Tüm çalışanlar,
- Bilgi varlıklarının sahipleri,
- Birim yöneticileri,
- Bilgi İşlem Daire Başkanlığı,
- Bilgi Güvenliği Yönetim Sistemi kapsamında görev ve sorumluluğu bulunan kişiler sorumludur.

Tüm çalışanlar, kendilerine tahsis edilen çalışma alanlarında ve kullandıkları bilgi sistemlerinde bu politikada belirtilen kurallara uymakla yükümlüdür.

4. UYGULAMA

4.1.Temiz Masa

1. Çalışanlar, kendilerine tahsis edilen çalışma alanlarının düzenli ve güvenli tutulmasından sorumludur.
2. Kişisel veri, özel nitelikli kişisel veri, personel bilgileri, sağlık bilgileri, finansal bilgiler, kullanıcı bilgileri, güvenlik bilgileri veya Gizli/Çok Gizli sınıftaki bilgiler çalışma masaları üzerinde yetkisiz kişilerin erişebileceği şekilde bırakılmamalıdır.
3. Çalışan masasından ayrılırken, üzerinde bulunan hassas bilgi içeren belgeleri yetkisiz erişime karşı korumalı; gerekli durumlarda bu belgeleri kilitli dolap, çekmece veya güvenli arşiv alanlarında muhafaza etmelidir.
4. Kullanımı tamamlanan ve saklama yükümlülüğü bulunmayan basılı belgeler, Bilgi Varlıkları ve Bilgi Sınıflandırma Politikası ile ilgili imha prosedürlerine uygun olarak güvenli şekilde imha edilmelidir.
5. Gizli veya Çok Gizli sınıfta bulunan belgeler normal çöp kutularına atılmamalıdır. Bu belgeler kurumun belirlediği güvenli imha yöntemleri kullanılarak imha edilmelidir.
6. Kullanılmış not kağıtları, taslaklar, fotokopiler veya çıktıların üzerinde kişisel veri ya da kurum açısından hassas bilgi bulunması halinde bunlar müsvedde amacıyla tekrar kullanılmamalıdır.
7. Çalışanlar, çalışma alanlarından ayrılmadan önce masa üzerinde yetkisiz kişilerin erişebileceği herhangi bir bilgi veya belge bulunup bulunmadığını kontrol etmelidir.
8. Terk edilmiş çalışma alanlarında kişisel ajanda, not kağıdı, rapor, liste, personel bilgileri veya diğer hassas bilgi içeren dokümanlar bırakılmamalıdır.
9. Çalışma masalarında bulunan USB bellek, harici disk, CD/DVD ve benzeri çıkarılabilir medya, yetkisiz kişilerin erişimine karşı korunmalıdır.
10. Kullanıcı adı, parola, PIN, erişim kodu, kriptografik anahtar ve benzeri kimlik doğrulama bilgileri Post-it, not kağıdı veya görünür başka bir yüzeye yazılarak bırakılmamalıdır.
11. Masa, çekmece, dolap ve kasa anahtarları yetkisiz kişilerin erişebileceği şekilde açıkta bırakılmamalıdır.
12. Kurumsal belgeler; yazıcı, fotokopi, tarayıcı, faks ve benzeri cihazlar üzerinde denetimsiz şekilde bırakılmamalıdır.
13. Hassas bilgi içeren belgelerin çıktısı alınırken mümkün olduğunca güvenli yazdırma veya kullanıcı doğrulamalı yazdırma yöntemleri kullanılmalıdır.
14. Yazıcı veya fotokopi cihazından alınan kişisel veri veya gizli bilgi içeren belgeler, çıktı alındıktan sonra gecikmeksizin teslim alınmalıdır.

15. Çalışma alanında kişisel veri, Gizli veya Çok Gizli bilgi içeren fiziksel veya elektronik medya bulunması halinde, çalışma alanına erişimler görev ve yetki esasına göre kontrol edilmelidir.
16. Toplantı odaları ve ortak kullanım alanlarında toplantı sonrasında belge, not, tahta yazısı, ekran görüntüsü veya diğer hassas bilgiler bırakılmamalıdır.
17. Ziyaretçiler, stajyerler, yükleniciler ve diğer yetkisiz kişiler çalışma alanlarında bilgi varlıklarına erişebilecek şekilde gözetimsiz bırakılmamalıdır.

4.2. Temiz Ekran

1. Çalışanlar, kendilerine tahsis edilen masaüstü ve taşınabilir bilgisayarların güvenli kullanımından sorumludur.
2. Bilgisayar ekranlarında görev gereği ihtiyaç duyulmayan kişisel veri, özel nitelikli kişisel veri, Gizli veya Çok Gizli bilgi içeren belgeler ve uygulamalar yetkisiz kişilerin görebileceği şekilde açık bırakılmamalıdır.
3. Çalışan bilgisayarının başından ayrıldığında ekranını kilitlemelidir.
4. Bilgisayarların otomatik ekran kilitleme süreleri, kurumun bilgi güvenliği standartlarına ve teknik yapılandırmalarına uygun olarak belirlenmelidir.
5. Çalışanlar, bilgisayar ekranlarını ziyaretçiler, öğrenciler, diğer çalışanlar veya yetkisiz kişilerin göremeyeceği şekilde konumlandırmalıdır.
6. Özellikle kişisel veri, özel nitelikli kişisel veri, kullanıcı hesapları, güvenlik kayıtları ve Gizli/Çok Gizli bilgiler görüntülenirken ekranın yetkisiz kişiler tarafından görülmesi engellenmelidir.
7. Ortak kullanım alanlarında veya toplantı odalarında kullanılan ekranlarda hassas bilgiler açık bırakılmamalıdır.
8. Bilgi sistemlerinde kullanılan parola, PIN, erişim kodu, kriptografik anahtar ve benzeri kimlik doğrulama bilgileri ekran üzerinde görünür şekilde bulundurulmamalıdır.
9. Kurumsal çalışma dosyaları, yetkisiz kişilerin erişimine açık masaüstü klasörlerinde veya ortak alanlarda tutulmamalı; kurum tarafından belirlenen güvenli depolama alanlarında saklanmalıdır.
10. Kurumsal bilgi varlıklarına ilişkin çalışmalar, yetkilendirilmiş ağ sürücüleri, doküman yönetim sistemleri, kurumsal uygulamalar veya kurum tarafından belirlenen diğer güvenli depolama alanlarında tutulmalıdır.
11. Bilgisayarlarda yetkisiz veya güvenliği ihlal edebilecek yazılımlar, dosyalar, bağlantılar veya kısayollar bulundurulmamalıdır.
12. Kurumun bilgi güvenliği politikalarına aykırı, zararlı, hukuka aykırı veya kurumun çalışma ortamına uygun olmayan içerikler bilgi sistemlerinde bulundurulmamalıdır.

13. Çalışma sona erdiğinde, gerekli olmayan uygulamalar kapatılmalı ve hassas bilgi içeren ekranlar açık bırakılmamalıdır.

4.3. Fiziksel Bilgi Varlıklarının Korunması

1. Hizmete Özel, Gizli ve Çok Gizli sınıftaki fiziksel belgeler, erişim yetkisi bulunmayan kişilerin ulaşamayacağı şekilde muhafaza edilmelidir.
2. Gizli ve Çok Gizli belgeler, mümkün olduğunda kilitli dolap, kilitli çekmece veya kontrollü arşiv alanlarında saklanmalıdır.
3. Hassas belgelerin çalışma alanları arasında taşınması sırasında yetkisiz kişilerin görmesini veya almasını engelleyecek tedbirler alınmalıdır.
4. Hassas bilgi içeren belgeler, yetkisiz kişilere teslim edilmemeli veya yetkisiz kişilerin bulunduğu ortamlarda bırakılmamalıdır.
5. Hassas bilgi içeren belgelerin kaybolması, yanlış kişiye gönderilmesi, yetkisiz kişilerce görülmesi veya erişilmesi halinde ilgili Olay İhlal Bildirim ve Yönetimi süreçleri işletilmelidir.

4.4. Çıktı ve Kopyaların Kontrolü

1. Kişisel veri veya gizli bilgi içeren belgelerin gereksiz sayıda çıktısı alınmamalıdır.
2. Çıktıların yetkisiz kişilerin erişimine açık yazıcılarda bekletilmemesine dikkat edilmelidir.
3. Kopyalanması gerekmeyen belge ve çıktılar güvenli şekilde imha edilmelidir.
4. Hassas bilgi içeren belgelerin kopyalanması, taranması veya başka bir ortama aktarılması yalnızca iş gerekliliği ve yetki kapsamında gerçekleştirilmelidir.

5. BİLGİ SINIFLANDIRMASI İLE İLİŞKİ

1. Temiz masa ve temiz ekran uygulamalarında bilgi varlıklarının sınıflandırma seviyeleri dikkate alınır.
2. Özellikle Hizmete Özel, Gizli ve Çok Gizli sınıfta bulunan bilgi varlıkları için yetkisiz erişimi önleyici fiziksel ve teknik tedbirler uygulanır.
3. Bilginin sınıflandırılması ve sınıflandırma seviyesine göre uygulanacak koruma tedbirleri Bilgi Sınıflandırma ve Etiketleme Politikası kapsamında belirlenir.

5. YAPTIRIM

Bu politikada belirtilen kurallara aykırı uygulamalar, ilgili Düzeltici Faaliyet**,** Olay Yönetimi veya ilgili diğer EYS süreçleri kapsamında değerlendirilir.

İhlalin niteliğine göre, ilgili mevzuat, kurum düzenlemeleri ve Disiplin Prosedürü hükümleri uygulanır.