1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi bünyesinde üretilen, alınan, işlenen, saklanan, kullanılan ve paylaşılan bilgi varlıklarının bilgi güvenliği açısından taşıdığı önem ve gizlilik seviyesine göre sınıflandırılmasını ve uygun şekilde etiketlenmesini sağlamaktır.

Bu politika ile bilgilerin gizlilik, bütünlük ve erişilebilirlik gereksinimlerinin belirlenmesi, bilginin yalnızca yetkili kişiler tarafından erişilebilir olması ve bilgi varlıklarının yaşam döngüsü boyunca uygun güvenlik kontrollerinin uygulanması amaçlanmaktadır.

2. KAPSAM

Bu politika;

- Daire Başkanlıklarını,
- Genel Sekreterliği,
- Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimini,
- Kurum çalışanlarını,
- Kurum bilgi varlıklarını kullanan diğer yetkili kullanıcıları,
- Kurum tarafından oluşturulan veya Kurum dışından alınan bilgileri,
- Fiziksel ve elektronik ortamdaki bilgi varlıklarını,

Doküman, evrak, kayıt, veri tabanı, e-posta, rapor, yazılım, sistem kayıtları ve diğer bilgi varlıklarını kapsar.

3. SORUMLULUKLAR

3.1. Üst Yönetim

- Bilgi sınıflandırma sisteminin uygulanmasını desteklemekten,
- Bilgi güvenliği gereksinimlerinin karşılanması için gerekli kaynakları sağlamaktan sorumludur.

3.2. Bilgi Sahibi

- Bilginin sınıflandırma seviyesini belirlemekten,
- Bilginin gizlilik, bütünlük ve erişilebilirlik gereksinimlerini değerlendirmekten,
- Bilgiye kimlerin erişebileceğini belirlemekten,
- Bilgi sınıflandırmasını gerektiğinde güncellemekten,
- Bilginin yaşam döngüsü boyunca uygun şekilde korunmasını sağlamaktan sorumludur.

Bilgi sahibi, kural olarak bilgiyi üreten veya bilgi üzerinde iş süreçleri açısından yetki ve sorumluluğu bulunan birimdir.

3.3. Bilgi İşlem Daire Başkanlığı

- Bilgi sınıflandırmasının uygulanabilmesi için gerekli teknik altyapıyı sağlamaktan,
- Elektronik ortamdaki sınıflandırılmış bilgilerin uygun erişim kontrolleri ile korunmasına destek olmaktan,
- Teknik olarak uygulanabilir olduğu durumlarda elektronik etiketleme ve sınıflandırma mekanizmalarını desteklemekten,
- Bilgi güvenliği kontrollerinin uygulanmasından sorumludur.

3.4. Kullanıcılar

- Eriştikleri bilgilerin sınıflandırma seviyesine uygun hareket etmekten,
- Bilgileri yalnızca görevleri kapsamında kullanmaktan,
- Gizlilik ve etiketleme kurallarına uymaktan,
- Bilgilerin yetkisiz kişilere açıklanmasını, kopyalanmasını veya paylaşılmasını önlemekten sorumludur.

4. UYGULAMA

4.1. BİLGİ SINIFLANDIRMA

4.1.1. Bilgi Sınıflandırma İlkeleri

1. Kurum bünyesindeki bilgiler; bilginin yetkisiz açıklanması, değiştirilmesi, kaybolması veya erişilememesi halinde Kuruma verebileceği zarar ve bilgi güvenliği gereksinimleri dikkate alınarak sınıflandırılır.
2. Bilgi sınıflandırması, bilginin gizlilik gereksinimi başta olmak üzere bütünlük ve erişilebilirlik gereksinimleri dikkate alınarak yapılır.
3. Bilginin sınıflandırılması, yalnızca bilginin bulunduğu ortama göre değil, bilginin içeriğine ve taşıdığı riske göre yapılır.
4. Bilginin fiziksel veya elektronik ortamda bulunması sınıflandırma seviyesini değiştirmez.
5. Aynı bilgi farklı ortamlarda bulunduğunda mümkün olduğunca aynı sınıflandırma seviyesinde korunmalıdır.
6. Bir bilgi varlığı içerisinde farklı sınıflandırma seviyelerinde bilgiler bulunması halinde, uygulanacak koruma tedbirleri en yüksek gizlilik seviyesine sahip bilgiye göre belirlenir.
7. Bilginin sınıflandırması, bilgi sahibi tarafından belirlenir ve bilgi yaşam döngüsü boyunca gerektiğinde gözden geçirilir.

8. Bilgi sınıflandırması en az yılda bir kez ve ayrıca aşağıdaki durumlarda gözden geçirilmelidir:
   - Bilginin kullanım amacı değiştiğinde,
   - Bilginin sahibi veya sorumlu birimi değiştiğinde,
   - Mevzuat veya sözleşme gereksinimleri değiştiğinde,
   - Bilgiye yönelik risk değiştiğinde,
   - Bilginin kamuya açık hale gelmesi gerektiğinde,
   - Bilginin saklama süresi veya kullanım süresi sona erdiğinde.

4.1.2. Bilgi Sınıflandırma Seviyeleri

4.1.2.1. Açık Bilgi

Açık bilgiler, Kurum tarafından kamuya açıklanmasında sakınca bulunmayan bilgilerdir.

Örnekler:

- Kamuya açık web sitesi içerikleri,
- Kamuya açıklanmış duyurular,
- Kamuya açık etkinlik bilgileri,
- Kamuya açık mevzuat ve rehberler,
- Kurum tarafından yayımlanmasına karar verilen bilgiler.

Açık bilgiler üzerinde ayrıca gizlilik etiketi bulunması zorunlu değildir.

4.1.2.2. Birime Özel Bilgi

Birime Özel bilgiler, yalnızca ilgili Kurum personelinin veya belirli çalışma gruplarının görevlerini yerine getirmesi amacıyla kullandığı bilgilerdir.

Örnekler:

- Birim içi çalışma dokümanları,
- İş süreçlerine ilişkin operasyonel bilgiler,
- Kurum içi yazışmalar,

- Birim toplantı notları,
- Kamuya açıklanmamış ancak yüksek gizlilik gerektirmeyen çalışma dokümanları.

Bu bilgiler görev gereği olmayan kişilerle paylaşılmamalıdır.

4.1.2.3. Hizmete Özel Bilgi

İçerdiği bilgi itibariyle çok gizli, gizli ve özel gizlilik dereceleri ile korunması gerekmeyen ancak bilmesi gerekenlerden başkası tarafından bilinmesi istenmeyen evraklardır.

4.1.2.4. Gizli Bilgi

Gizli bilgiler, yetkisiz erişim veya açıklama halinde Kurum açısından önemli güvenlik, hukuki, mali, idari veya itibari zarar doğurabilecek bilgilerdir.

Örnekler:

- Kişisel veriler,
- Özel nitelikli kişisel veriler,
- Bilgi sistemlerine ilişkin güvenlik bilgileri,
- Güvenlik açıkları ve zafiyet bilgileri,
- Kimlik doğrulama ve güvenlik bilgileri,
- Sözleşmelerde gizlilik kapsamında değerlendirilen bilgiler,
- Ticari sır niteliğindeki bilgiler,
- Yetkisiz açıklanması Kuruma zarar verebilecek stratejik bilgiler,
- Güvenlik testleri ve zafiyet analizleri,
- Henüz kamuya açıklanmamış kritik bilgi ve raporlar.

Not: Her kişisel veri otomatik olarak "Gizli" sınıfına alınmak zorunda değildir; ancak kişisel verilerin korunmasına ilişkin mevzuat ve Kurumun kişisel veri güvenliği kuralları ayrıca uygulanır. Bilginin sınıflandırılması yapılırken hukuki yükümlülükler ve riskler birlikte değerlendirilir.

4.1.2.5. Çok Gizli Bilgi

Çok Gizli bilgiler, bilmesi gerekenlerin dışında diğer kişilerin bilmelerinin istenmediği ve izinsiz açıklandığı takdirde devletin güvenliğine, ulusal varlık ve bütünlüğe, iç ve dış menfaatimize hayati bakımdan son derece büyük zarar verecek, yabancı bir devlete faydalar sağlayacak ve güvenlik bakımından olağan üstü önemi haiz evraklardır.

4.1.3. Mevzuat Ve Gizlilik Dereceli Evrak

Mevzuat kapsamında özel gizlilik derecesine tabi olan evrak ve bilgiler, ilgili mevzuatta belirtilen kurallara göre işleme alınır. Mevzuatla belirlenmiş özel gizlilik dereceleri ile Kurumun bilgi sınıflandırma sistemi birbirinden bağımsız değerlendirilmemeli; ilgili mevzuatın daha yüksek bir koruma gerektirmesi halinde daha yüksek güvenlik seviyesi uygulanmalıdır.

Özellikle aşağıdaki türdeki bilgi ve belgeler, tabi oldukları mevzuat ve düzenlemeler kapsamında ayrıca değerlendirilir:

- Gizlilik dereceli resmi evrak,
- Kişiye özel evrak,
- Kişisel veri içeren belgeler,
- Özel nitelikli kişisel veri içeren belgeler,
- Resmî yazışmalar,
- Hukuki veya sözleşmesel gizlilik yükümlülüğü bulunan bilgiler.

4.2. BİLGİ SAHİPLİĞİ

1. Her bilgi varlığı için mümkün olduğunca bir bilgi sahibi belirlenmelidir.
2. Bilgi sahibi, bilginin sınıflandırılmasından ve uygun koruma seviyesinin belirlenmesinden sorumludur.
3. Bilgi sahibinin bilgisi ve onayı olmadan, bilginin sınıflandırma seviyesini değiştirecek işlem yapılmamalıdır.
4. Bilgi sahibinin değişmesi halinde bilgi sınıflandırması yeniden değerlendirilmelidir.
5. Bilgi sahibinin belirlenemediği durumlarda ilgili birim yöneticisi, bilginin sınıflandırılmasını sağlamak üzere sorumluluk üstlenir.

4.3. BİLGİ ETİKETLEME

1. Sınıflandırılmış bilgilerin sınıflandırma seviyesinin anlaşılmasını sağlayacak uygun etiketleme yöntemi kullanılmalıdır.
2. Etiketleme; bilginin bulunduğu ortama uygun şekilde yapılmalıdır.
3. Fiziksel belgelerde sınıflandırma etiketi dokümanın kolayca görülebilecek bir bölümünde bulunmalıdır.
4. Elektronik belgelerde sınıflandırma etiketi, dokümanın içeriğine ve kullanılan sisteme uygun şekilde uygulanmalıdır.
5. Gizli sınıfındaki fiziksel veya elektronik bilgilerin uygun şekilde etiketlenmesi zorunludur.

6. Birime Özel bilgilerin etiketlenmesi, kullanılan sistemin teknik özellikleri ve ilgili birimin ihtiyaçları doğrultusunda uygulanabilir.
7. Açık bilgiler için ayrıca sınıflandırma etiketi kullanılması zorunlu değildir.
8. Bilginin sınıflandırması değiştirildiğinde ilgili etiket de güncellenmelidir.
9. Bir dokümanın içeriğini önemli ölçüde değiştiren kişi veya birim, bilginin sınıflandırmasının değişmesi gerekip gerekmediğini değerlendirmelidir.
10. Bilginin kopyalanması veya farklı bir ortama aktarılması halinde sınıflandırma seviyesi korunmalıdır.

4.4. DOSYA VE DOKÜMAN İSİMLENDİRME

1. Elektronik dosya ve dokümanların isimlendirilmesinde Kurumun doküman yönetimi kurallarına uyulmalıdır.
2. Gerektiğinde dosya adlarında bilgi sınıflandırma seviyesinin belirlenmesini kolaylaştıracak standart ifadeler kullanılabilir.
3. Dosya adlarında kişisel veri, parola, kimlik doğrulama bilgisi veya gereksiz hassas bilgi bulunmamalıdır.
4. Dokümanların sürüm bilgisi ve değişiklik durumu, Kurumun doküman yönetimi kurallarına uygun olarak takip edilmelidir.

4.5. BİLGİNİN KOPYALANMASI VE Çoğaltılması

1. Gizli bilgilerin kopyalanması yalnızca iş gereksinimi bulunan ve yetkili kişiler tarafından gerçekleştirilmelidir.
2. Gereksiz kopya oluşturulmamalıdır.
3. Fiziksel kopyalama işlemlerinde yazıcı, fotokopi ve tarayıcı cihazlarında belge bırakılmamalıdır.
4. Kullanıcılar, yazıcı veya fotokopi cihazlarından aldıkları dokümanların cihaz üzerinde unutulmamasından sorumludur.
5. Gizli bilgi içeren dokümanların kopyaları da asıl doküman ile aynı veya daha yüksek güvenlik seviyesinde korunmalıdır.

4.6. BİLGİNİN AKTARILMASI

1. Bilgi transferlerinde bilginin sınıflandırma seviyesi dikkate alınmalıdır.
2. Gizli bilgilerin aktarımında yalnızca Kurum tarafından onaylanmış güvenli iletişim ve dosya paylaşım yöntemleri kullanılmalıdır.
3. Gizli bilgilerin elektronik ortamda aktarılması gerektiğinde gerekli güvenlik önlemleri ve uygun durumlarda şifreleme uygulanmalıdır.

4. Fiziksel ortamda aktarılan gizli bilgiler, yetkisiz kişilerin erişimini önleyecek şekilde korunmalıdır.
5. Bilginin sınıflandırma seviyesi, bilgi farklı bir ortama aktarıldığında veya kopyalandığında korunmalıdır.
6. Üçüncü taraflara bilgi aktarımında ilgili sözleşme, gizlilik ve kişisel veri güvenliği gereksinimleri uygulanmalıdır.

4.7. BİLGİNİN SAKLANMASI VE İMHASI

1. Bilgiler, sınıflandırma seviyesine uygun ortamlarda saklanmalıdır.
2. Gizli bilgiler yalnızca yetkilendirilmiş kişilerin erişebileceği ortamlarda tutulmalıdır.
3. Bilginin saklama süresi sona erdiğinde, ilgili mevzuat ve Kurumun saklama/imha kuralları doğrultusunda güvenli şekilde silinmeli, yok edilmeli veya anonim hale getirilmelidir.
4. Fiziksel belgelerin imhasında bilgi sınıflandırma seviyesine uygun yöntem kullanılmalıdır.
5. Elektronik ortamlardaki bilgilerin silinmesi gerektiğinde, Kurumun güvenli silme ve imha kurallarına uyulmalıdır.

4.8. DIŞ KAYNAKLI BİLGİLER

1. Kurum dışından alınan bilgi ve dokümanlar, Kurum içerisinde kullanılmadan önce bilgi güvenliği açısından değerlendirilmelidir.
2. Dış kaynaklı bilgilerin sınıflandırılması, mümkün olduğunda bilginin sahibi veya sorumlu birim tarafından yapılmalıdır.
3. Üçüncü taraflarca belirlenmiş gizlilik sınıflandırmaları varsa bunlar dikkate alınmalıdır.
4. Dış kaynaklı bilgilerin Kurum içerisindeki sınıflandırma sistemi ile eşleştirilmesi gerektiğinde, daha yüksek koruma gerektiren sınıflandırma seviyesi esas alınmalıdır.

4.9. SINIFLANDIRMA DEĞİŞİKLİĞİ

Bilginin sınıflandırması aşağıdaki durumlarda yeniden değerlendirilebilir:

- Bilginin kamuya açıklanması,
- Bilginin kullanım amacının değişmesi,
- Bilginin hukuki statüsünün değişmesi,
- Bilginin içerdiği kişisel verilerin veya hassas bilgilerin değişmesi,
- Bilgiye yönelik risk seviyesinin değişmesi,
- Bilginin saklama süresinin sona yaklaşması,
- Bilgi sahibinin veya sorumlu birimin değişmesi.

Sınıflandırma değişikliği bilgi sahibi veya yetkilendirilmiş kişi tarafından onaylanmalı ve gerekli durumlarda kayıt altına alınmalıdır.

4.10. BİLGİ SINIFLANDIRMA, ETİKETLEME, SAKLAMA VE İMHA TABLOSU

Sınıf	Erişim	Etiketleme	Aktarım	Saklama	İmha	Örnek
AÇIK	Kamuya açık	Zorunlu değil. Dokümanda "AÇIK" etiketi kullanılabilir.	Normal iletişim kanalları, kamuya açık sistemler	İlgili mevzuat/kurum ihtiyacına göre	Kurum prosedürüne göre	Web sitesi duyuruları, kamuya açık raporlar, basın açıklamaları, ilanlar
BİRİME ÖZEL	İlgili birim/personel ile sınırlı	Doküman üzerinde **"BİRİME ÖZEL"** etiketi	Kurum tarafından onaylanan iletişim ve bilgi paylaşım kanalları	İş süresi boyunca/ihtiyaca göre	Güvenli silme/imha	Birim içi çalışma dokümanları, toplantı notları, iş planları, taslaklar, iç yazışmalar
HİZMETE ÖZEL	Görevi gereği erişmesi gereken yetkili kurum personeli ve ilgili hizmet/iş sürecinde bulunan kişiler	**"HİZMETE ÖZEL"** etiketi zorunlu	Kurum tarafından onaylanmış güvenli kanallar; gerektiğinde erişim kontrolü ve şifreleme	Belirlenen saklama süresince	Güvenli silme/imha	Kurumsal uygulama kayıtları, hizmet süreçlerine ilişkin operasyonel bilgiler, personel/öğrenci işlemlerine ilişkin görev dokümanları, henüz yayımlanmamış çalışma belgeleri
GİZLİ	Yalnızca yetkilendirilmiş kişiler	**"GİZLİ"** etiketi zorunlu	Güvenli aktarım; gerektiğinde şifreleme; yetkisiz kişilerin erişimi engellenir	Mevzuat ve saklama planına göre	Güvenli ve kontrollü imha	Kişisel veriler, güvenlik bilgileri, gizli raporlar, güvenlik açıklarına ilişkin bilgiler, erişim/yetkilendirme kayıtları, denetim bulguları

Sınıf	Erişim	Etiketleme	Aktarım	Saklama	İmha	Örnek
ÇOK GİZLİ	Çok sınırlı sayıda, özel olarak yetkilendirilmiş kişiler	**"ÇOK GİZLİ"** etiketi zorunlu	Şifreli ve kurum tarafından onaylanmış güvenli kanallar; aktarım kayıt altına alınır; mümkün olduğunda ek kimlik doğrulama uygulanır	Minimum gerekli süre	Kontrollü ve kayıtlı imha	Kritik güvenlik bilgileri, siber güvenlik olaylarına ilişkin hassas bilgiler, kritik sistem bilgileri, güvenlik zafiyetlerinin ayrıntıları, kritik altyapı bilgileri, soruşturma/inceleme kapsamında erişimi ciddi risk oluşturabilecek bilgiler

4.11. BİLGİ SINIFLANDIRMA KONTROLÜ

Bilgi sahipleri, kendilerine ait bilgilerin uygun sınıflandırma seviyesinde olup olmadığını **en az yılda bir kez** gözden geçirmelidir.

Gözden geçirme sonucunda;

- Sınıflandırmanın uygun olduğu,
- Sınıflandırmanın yükseltilmesi gerektiği,
- Sınıflandırmanın düşürülmesi gerektiği,
- Bilginin artık saklanmasına gerek olmadığı değerlendirilir ve gerekli işlemler gerçekleştirilir.

4.12.İHLAL VE BİLDİRİM

Aşağıdaki durumlar bilgi güvenliği olayı olarak değerlendirilir ve ilgili süreçlere uygun şekilde bildirilir:

- Gizli bilginin yetkisiz kişiye gönderilmesi,
- Yanlış sınıflandırma yapılması,
- Gizli bilgi etiketinin kaldırılması veya değiştirilmesi,
- Gizli bilginin yetkisiz şekilde kopyalanması,

- Gizli bilginin yetkisiz ortamda saklanması,
- Bilginin yetkisiz kişilere açıklanması,
- Bilginin kaybolması veya yetkisiz erişime maruz kalması.

5. YAPTIRIM

Bu politikaya aykırı hareket eden personel hakkında, olayın niteliğine göre Kurumun ilgili prosedürleri, disiplin hükümleri ve yürürlükteki mevzuat kapsamında gerekli işlemler uygulanır. Üçüncü tarafların bilgi sınıflandırma ve koruma kurallarına aykırı hareket etmesi halinde ilgili sözleşme hükümleri ve yürürlükteki mevzuat uygulanır.