1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi bünyesinde ve Kurum ile üçüncü taraflar arasında gerçekleştirilen bilgi, kişisel veri, yazılım ve bilgi varlıklarının elektronik veya fiziksel yollarla aktarılması sırasında bilgilerin gizlilik, bütünlük ve erişilebilirliğinin korunmasını**, yetkisiz** erişim, değiştirme, kaybolma, ifşa ve kötüye kullanım risklerinin önlenmesini sağlamaktır.

Bu politika kapsamında gerçekleştirilen bilgi ve yazılım transferlerinin Kurumun bilgi güvenliği kurallarına, ilgili mevzuata, sözleşmelere ve Kurum tarafından belirlenen güvenlik gereksinimlerine uygun olarak gerçekleştirilmesi esastır.

2. KAPSAM

Bu politika;

- Süleyman Demirel Üniversitesi çalışanlarını,
- Kurum adına bilgi işleyen veya bilgiye erişen diğer personel ve kullanıcıları,
- Kurumun bilgi ve yazılım alışverişi yaptığı üçüncü tarafları,
- Tedarikçileri, hizmet sağlayıcıları ve iş ortaklarını,
- Kurumun bilgi sistemleri, e-posta, dosya paylaşım, elektronik iletişim ve veri aktarım ortamlarını,
- Elektronik ve fiziksel ortamlar üzerinden gerçekleştirilen bilgi, kişisel veri ve yazılım transferlerini kapsar.

Politika; bilgi sistemleri üzerinden gerçekleştirilen elektronik veri aktarımının yanı sıra kâğıt doküman, taşınabilir medya ve diğer fiziksel ortamlar aracılığıyla gerçekleştirilen bilgi transferlerini de kapsar.

3. TANIMLAR

- **Kurum:** Süleyman Demirel Üniversitesi.
- **Bilgi Transferi:** Bilginin Kurum içerisinde veya Kurum ile üçüncü taraflar arasında elektronik, fiziksel veya sözlü yöntemlerle aktarılması.
- **Gizli Bilgi:** Yetkisiz kişilerin erişmesi, kullanması, açıklaması veya değiştirmesi durumunda Kuruma, çalışanlara, öğrencilere, üçüncü taraflara veya diğer ilgili taraflara zarar verebilecek bilgiler.
- **Hassas Bilgi:** Bilginin gizliliğinin, bütünlüğünün veya erişilebilirliğinin korunmasının özel önem taşıdığı bilgiler.

- **Üçüncü Taraf:** Kurum dışında bulunan ve Kurum adına hizmet sunan, Kurum ile bilgi alışverişinde bulunan gerçek veya tüzel kişiler

4. SORUMLULUKLAR

4.1. Bilgi İşlem Daire Başkanlığı;

- Bilgi transferinde kullanılan bilgi sistemlerinin güvenliğinin sağlanmasından,
- Kurumsal elektronik iletişim ve dosya paylaşım altyapılarının güvenli şekilde işletilmesinden,
- Gerekli teknik güvenlik kontrollerinin uygulanmasından,
- Uygun durumlarda aktarım kayıtlarının ve loglarının tutulmasından,
- Kurumsal sistemlerde kullanılan şifreleme ve güvenlik mekanizmalarının güvenli yöntemlere uygunluğunun sağlanmasından,
- Yetkisiz yazılım kurulumu ve güncellemelerin önlenmesine yönelik teknik kontrollerin uygulanmasından sorumludur.

4.2. Birim Yöneticileri ve Bilgi Sahipleri

- Paylaşılacak bilginin uygun şekilde sınıflandırılmasını,
- Bilgiye erişmesi gereken kişi ve tarafların belirlenmesini,
- Bilginin yalnızca görev ve iş gereksinimi kapsamında paylaşılmasını,
- Üçüncü taraflarla gerçekleştirilecek bilgi transferlerinde gerekli onay ve sözleşmelerin bulunmasını sağlar.

4.3. Çalışanlar ve Kullanıcılar

- Bilgi transferlerini yalnızca Kurum tarafından izin verilen yöntemlerle gerçekleştirmekten,
- Bilginin yalnızca yetkili kişi veya taraflara gönderilmesinden,
- Gizli ve hassas bilgilerin korunmasından,
- Kurum tarafından belirlenen şifreleme ve güvenli aktarım yöntemlerini kullanmaktan,
- Bilginin yanlış kişiye gönderilmesi, kaybolması veya yetkisiz erişim şüphesi oluşması halinde durumu derhal ilgili birime bildirmekten sorumludur.

4.4. Üçüncü Taraflar

Üçüncü taraflar, Kurum tarafından kendilerine aktarılan bilgileri yalnızca yetkilendirildikleri amaç doğrultusunda kullanmak ve Kurum tarafından belirlenen bilgi güvenliği gereksinimlerine uymakla yükümlüdür.

5. UYGULAMA

5.1. Genel Bilgi Transferi Kuralları

1. Bilgi transferi gerçekleştirilmeden önce gönderen ve alıcının kimliği ve yetkisi mümkün olduğu ölçüde doğrulanmalıdır.
2. Bilgi yalnızca **iş gereksinimi bulunan ve yetkilendirilmiş kişi veya taraflarla** paylaşılmalıdır.
3. Bilginin aktarımında kullanılan yöntem, bilginin gizlilik seviyesine ve güvenlik gereksinimine uygun olmalıdır.
4. Gizli veya hassas bilgilerin yetkisiz kişilere aktarılması, çoğaltılması, değiştirilmesi veya açıklanması engellenmelidir.
5. Bilgi transferlerinde bilgi güvenliği, kişisel verilerin korunması, ilgili mevzuat, sözleşme ve Kurum politikaları dikkate alınmalıdır.
6. Bilgi transferinin yanlış alıcıya gönderildiğinin veya yetkisiz kişilerin eriştiğinin tespit edilmesi halinde olay derhal ilgili birime bildirilmelidir.

5.2. Elektronik Bilgi Transferi

1. Elektronik bilgi transferleri mümkün olduğunca Kurum tarafından sağlanan ve yetkilendirilen bilgi sistemleri üzerinden gerçekleştirilmelidir.
2. Gizli, hassas veya kişisel veri içeren bilgilerin aktarımında uygun güvenlik önlemleri uygulanmalıdır.
3. Bilginin gizliliğinin korunmasının gerekli olduğu durumlarda aktarım sırasında uygun şifreleme mekanizmaları kullanılmalıdır.
4. Şifreleme yöntemleri ve güvenlik sertifikaları, Bilgi İşlem Daire Başkanlığı tarafından Kurumun bilgi güvenliği standartlarına ve kabul edilmiş güvenli yöntemlere uygun şekilde yönetilmelidir.
5. Elektronik transferlerde alıcı adresi gönderim öncesinde kontrol edilmelidir.
6. Hassas bilgi içeren e-postalar, mümkün olduğunda alıcının kimliğinin doğrulanmasını ve erişimin sınırlandırılmasını sağlayacak yöntemlerle gönderilmelidir.
7. Gizli veya hassas bilgiler, Kurum tarafından onaylanmamış kişisel e-posta hesapları veya yetkisiz dosya paylaşım servisleri üzerinden gönderilmemelidir.
8. Kurumsal bilgi ve kişisel verilerin aktarımında Kurum tarafından onaylanmamış anlık mesajlaşma, dosya paylaşım veya sosyal medya uygulamaları kullanılmamalıdır.
9. Elektronik bilgi transferlerine ilişkin gerekli durumlarda erişim ve işlem kayıtları tutulmalıdır.
10. Transfer sırasında kullanılan sistemlerin güvenliği ve bütünlüğü korunmalıdır.

5.3. E-Posta Kullanımı

1. Kurumsal iş iletişimleri için Kurum tarafından tahsis edilen e-posta hesapları kullanılmalıdır.
2. E-posta gönderilmeden önce alıcı adresi, ekler ve mesaj içeriği kontrol edilmelidir.
3. Gizli veya hassas bilgi içeren e-postalar yalnızca yetkili alıcılara gönderilmelidir.
4. Hassas veya gizli bilgilerin e-posta yoluyla aktarılması gerektiğinde, bilginin niteliğine uygun şifreleme veya Kurum tarafından belirlenen diğer güvenli aktarım yöntemleri kullanılmalıdır.
5. Özel nitelikli kişisel verilerin elektronik ortamda aktarılması sırasında Kurumun kişisel veri güvenliği prosedürleri ve güvenli aktarım yöntemleri uygulanmalıdır.
6. Gerekli durumlarda KEP, şifreli dosya, güvenli dosya paylaşım sistemi veya Kurum tarafından onaylanan diğer güvenli iletişim yöntemleri kullanılabilir.
7. Şifreli olarak gönderilen dosyaların parolası aynı iletişim kanalı üzerinden gönderilmemelidir.
8. E-posta ile gönderilen bilgilerin gönderen kişi veya birimi ve gerektiğinde geri dönüş iletişim bilgilerini içermesi sağlanmalıdır.
9. Kurumsal e-posta hesapları yalnızca görev ve iş gereksinimleri doğrultusunda kullanılmalıdır.
10. Kurumsal e-posta üzerinden saldırgan, tehditkâr, ayrımcı, hakaret içeren veya Kurumun bilgi güvenliğini tehlikeye düşüren içerikler gönderilemez.
11. E-posta eklerinde yer alan kişisel veri, gizli bilgi ve diğer hassas bilgiler gereksiz yere çoğaltılmamalı veya saklanmamalıdır.

5.4. Fiziksel Ortamda Bilgi Transferi

1. Kâğıt ortamındaki gizli veya hassas bilgiler yetkisiz kişilerin erişemeyeceği şekilde korunmalıdır.
2. Gizli dokümanların posta veya kargo yoluyla gönderilmesi durumunda, bilginin niteliğine uygun güvenli gönderim yöntemi kullanılmalıdır.
3. Gerekli durumlarda gizli dokümanlar kapalı ve uygun şekilde muhafaza edilerek gönderilmeli; dış ambalaj üzerinde bilginin gizlilik seviyesine ilişkin gereksiz açıklamalara yer verilmemelidir.
4. Hassas bilgi içeren fiziksel ortamların tesliminde teslim alan kişinin kimliği doğrulanmalı ve gerektiğinde teslim kaydı tutulmalıdır.
5. Taşınabilir medya, harici disk, USB bellek veya benzeri ortamlarla bilgi aktarılması gerektiğinde yalnızca Kurum tarafından izin verilen ortamlar kullanılmalıdır.

6. Taşınabilir ortamlarda bulunan gizli veya hassas bilgiler, bilginin niteliğine göre şifrelenmelidir.
7. Kullanım amacı sona eren taşınabilir ortamlardaki kişisel veya gizli bilgiler, Kurumun güvenli silme/imha kurallarına uygun şekilde silinmeli veya imha edilmelidir.

5.5. Üçüncü Taraflarla Bilgi Transferi

1. Üçüncü taraflara bilgi aktarılmadan önce aktarılacak bilginin niteliği, aktarım amacı, aktarım yöntemi ve üçüncü tarafın yetkisi değerlendirilmelidir.
2. Kurumun gizli bilgileri veya kişisel verileri üçüncü taraflara yalnızca iş gereksinimi ve yetkilendirme kapsamında aktarılmalıdır.
3. Üçüncü taraflarla gerçekleştirilecek bilgi transferlerinde gerekli durumlarda gizlilik sözleşmesi, veri işleme sözleşmesi, hizmet sözleşmesi veya diğer ilgili sözleşmeler yapılmalıdır.
4. Üçüncü tarafların Kurum bilgilerine erişim ve kullanım koşulları sözleşmelerde veya ilgili dokümanlarda açıkça belirlenmelidir.
5. Üçüncü taraflara aktarılacak bilgiler mümkün olan en az bilgi ile sınırlandırılmalıdır.
6. Üçüncü taraflarla dosya paylaşımı mümkün olduğunca Kurum tarafından yetkilendirilmiş ve kontrol edilen dosya paylaşım sistemleri üzerinden yapılmalıdır.
7. Üçüncü taraflara gönderilen elektronik ortamların bilgi içermediği veya içeriğin güvenli şekilde temizlendiği kontrol edilmelidir.
8. Gizli veya hassas bilgilerin üçüncü taraflara aktarımında uygun şifreleme ve erişim kontrolleri uygulanmalıdır.
9. Üçüncü tarafın bilgi güvenliği yükümlülükleri, ilgili sözleşme ve Kurumun tedarikçi güvenliği kuralları kapsamında takip edilmelidir.

5.6. Kişisel Verilerin Transferi

1. Kişisel verilerin aktarımı, ilgili mevzuat ve Kurumun kişisel veri koruma politika ve prosedürlerine uygun olarak gerçekleştirilmelidir.
2. Kişisel veriler yalnızca aktarım amacı için gerekli olduğu ölçüde paylaşılmalıdır.
3. Özel nitelikli kişisel verilerin aktarımında artırılmış güvenlik önlemleri uygulanmalıdır.
4. Kişisel verilerin elektronik ortamda aktarılması sırasında aktarım kanalının güvenliği sağlanmalı ve gerekli durumlarda şifreleme kullanılmalıdır.
5. Kişisel verilerin üçüncü taraflara aktarılmasında aktarımın hukuki dayanağı, alıcı taraf, aktarım amacı ve gerekli güvenlik tedbirleri değerlendirilmelidir.
6. Veri aktarımına ilişkin gerekli dokümanların hazırlanması ve onay süreçlerinin yürütülmesinde Kurum tarafından kullanılan KVKNET ONE modülünden yararlanılmalıdır.

7. Veri aktarım sürecinde E-DANIŞMAN soru seti sonucunda gerekli olduğu belirlenen sözleşme, taahhüt, protokol, aydınlatma veya diğer dokümanların hazırlanması, imzalanması ve muhafaza edilmesi sağlanmalıdır.

5.7. Uluslararası Bilgi Transferi

1. Bilginin uluslararası aktarılması durumunda, aktarımın hukuki ve bilgi güvenliği gereksinimleri değerlendirilmelidir.
2. Uluslararası aktarım sırasında yalnızca yetkili kişilerin gerekli bilgilere erişmesi sağlanmalıdır.
3. Gizli, hassas veya kişisel veri içeren bilgilerin uluslararası aktarımında uygun güvenlik ve şifreleme önlemleri uygulanmalıdır.
4. Kişisel verilerin yurt dışına aktarılması halinde yürürlükteki kişisel verilerin korunması mevzuatı ve Kurum prosedürleri uygulanmalıdır.

5.8. Yazılım Transferi, Kurulumu ve Güncellenmesi

1. Kurum bilgi sistemlerine yazılım kurulumu yalnızca yetkilendirilmiş personel tarafından gerçekleştirilmelidir.
2. Yazılım, güncelleme ve bakım işlemleri Bilgi İşlem Daire Başkanlığı tarafından belirlenen yetki ve prosedürler çerçevesinde gerçekleştirilmelidir.
3. Kurum sistemlerine kurulacak yazılımların kaynağı ve güvenilirliği kontrol edilmelidir.
4. Yetkisiz, lisanssız veya güvenilir olmayan kaynaklardan edinilen yazılımlar Kurum sistemlerine kurulamaz.
5. Yazılım güncellemeleri güvenilir kaynaklardan alınmalı ve gerekli güvenlik kontrolleri yapıldıktan sonra uygulanmalıdır.
6. Üçüncü taraflara yazılım veya yazılım bileşeni aktarılması durumunda lisans, güvenlik, gizlilik ve kullanım koşulları dikkate alınmalıdır.
7. Yazılım veya kaynak kodunun üçüncü taraflarla paylaşılması gerektiğinde yetkilendirme ve sözleşmesel yükümlülükler kontrol edilmelidir.

5.9. Bilgi Bütünlüğü ve Değişiklik Kontrolü

1. Bilgi transferi sırasında bilginin yetkisiz şekilde değiştirilmesi, silinmesi veya bozulması önlenmelidir.
2. Kritik bilgi ve dosyaların transfer veya değişiklik öncesinde gerekli görülmesi halinde yedekleri alınmalıdır.
3. Kurumsal dokümanlarda değişiklik talebinde bulunan kişinin veya birimin kimliği belirlenebilir olmalıdır.

4. Kritik bilgi sistemlerinde gerçekleştirilen değişiklikler yetkilendirme ve değişiklik yönetimi süreçlerine uygun olarak gerçekleştirilmelidir.

5.10. Toplantılar ve Sözlü Bilgi Paylaşımı

1. Gizli veya hassas bilgiler yalnızca bu bilgiye erişme yetkisi bulunan kişilerle paylaşılmalıdır.
2. Toplantılarda gizli veya hassas bilgi paylaşılması durumunda katılımcılara bilginin gizliliği ve bilgi güvenliği yükümlülükleri hatırlatılmalıdır.
3. Gizli veya kişisel bilgiler kamuya açık alanlarda veya yetkisiz kişilerin duyabileceği ortamlarda konuşulmamalıdır.
4. Çalışanlar gizli bilgileri telesekreter, sesli mesaj veya benzeri sistemlere bırakmamalıdır.
5. Gizli bilgi içeren toplantıların ses veya görüntü kaydı, gerekli yetkilendirme ve ilgili mevzuata uygunluk sağlanmadan gerçekleştirilemez.
6. Toplantı kayıtlarının alınması halinde kayıtların erişim, saklama ve imha koşulları belirlenmelidir.

5.11. Telefon ve Mobil İletişim

1. Gizli veya hassas bilgiler telefon görüşmeleri sırasında yalnızca gerekli olduğu ölçüde paylaşılmalıdır.
2. Kamuya açık veya güvenli olmadığı değerlendirilen ortamlarda gizli bilgi paylaşılmamalıdır.
3. Gizli bilgi içeren dokümanların cep telefonu ile fotoğrafının çekilmesi veya Kurum tarafından yetkilendirilmemiş uygulamalar aracılığıyla paylaşılması yasaktır.
4. Kurumsal bilgi ve kişisel verilerin mobil cihazlar üzerinden aktarımında Kurum tarafından belirlenen güvenlik kurallarına uyulmalıdır.

5.12. Kurum İçi Sistemlere Bilgi ve Uygulama Yerleştirilmesi

1. Kurumun intranet, bilgi sistemleri veya diğer kurumsal platformlarına bilgi veya uygulama eklenmesi yetkilendirme süreçlerine uygun olarak gerçekleştirilmelidir.
2. Kurumsal sistemlere yerleştirilen bilgi ve uygulamaların Kurumun bilgi güvenliği kurallarına uygunluğu kontrol edilmelidir.
3. Kurum bilgi sistemlerinde bulunan bilgi ve uygulamalara erişim, görev ve iş gereksinimi doğrultusunda yetkilendirilmelidir.
4. Kurum bilgi sistemlerinde bulunan bilgiler, yetkisiz kişiler tarafından erişilemeyecek, değiştirilemeyecek veya çoğaltılamayacak şekilde korunmalıdır.

5.13. Donanım ve Fiziksel Bilgi Varlıklarının Transferi

1. Kuruma ait bilgi içeren donanımların veya bilgi varlıklarının yerinin değiştirilmesi yetkili kişilerin onayı ile gerçekleştirilmelidir.
2. Donanım transferinden önce üzerinde bulunan gizli veya kişisel bilgilerin korunması sağlanmalıdır.
3. Kurum dışına çıkarılacak bilgi varlıklarında gerekli yetkilendirme ve kayıt işlemleri uygulanmalıdır.
4. Kullanımdan çıkarılan veya üçüncü taraflara devredilen cihazlarda bulunan bilgiler Kurumun güvenli silme ve imha prosedürlerine uygun şekilde silinmelidir.

5.14. Kayıt ve İzleme

1. Bilgi transferi yapılan sistemlerde, teknik olarak mümkün ve gerekli olduğu durumlarda işlem kayıtları tutulmalıdır.
2. Log kayıtları yetkisiz erişim ve değişikliğe karşı korunmalıdır.
3. Bilgi transferiyle ilişkili güvenlik olayları, Kurumun Bilgi Güvenliği Olay Yönetimi süreçlerine uygun olarak değerlendirilmelidir.
4. Kayıtların saklama süreleri ilgili mevzuat, Kurum politikaları ve bilgi güvenliği gereksinimleri doğrultusunda belirlenmelidir.

6. YASAKLAR

Aşağıdaki işlemler yasaktır:

- Yetkisiz kişilere gizli veya hassas bilgi gönderilmesi,
- Kurumsal bilgilerin kişisel e-posta hesapları üzerinden yetkisiz şekilde paylaşılması,
- Kurum tarafından onaylanmamış dosya paylaşım servisleri üzerinden gizli bilgi aktarılması,
- Kurum tarafından yetkilendirilmemiş mesajlaşma uygulamaları üzerinden kişisel veri veya gizli bilgi paylaşılması,
- Yetkisiz yazılım kurulması,
- Lisanssız veya güvenilir olmayan yazılımların Kurum sistemlerine yüklenmesi,
- Kurumsal bilgilerin yetkisiz şekilde çoğaltılması,
- Gizli bilgilerin kamuya açık alanlarda yetkisiz kişilerin erişebileceği şekilde paylaşılması,
- Bilgi transferi sırasında güvenlik kontrollerinin kasıtlı olarak devre dışı bırakılması.

7. İHLAL VE BİLGİ GÜVENLİĞİ OLAYLARI

Bilgi transferi sırasında;

- Bilginin yanlış kişiye gönderilmesi,
- Kişisel verilerin yetkisiz kişilere aktarılması,
- Gizli bilginin ifşa edilmesi,
- Bilginin kaybolması,
- Yetkisiz erişim,
- Bilginin değiştirilmesi veya bozulması,
- Taşınabilir ortamın kaybolması,
- Yetkisiz yazılım veya dosya paylaşımı

gibi durumların meydana gelmesi veya bundan şüphe edilmesi halinde olay derhal Kurumun bilgi güvenliği olay bildirim ve müdahale süreçlerine uygun olarak ilgili birime bildirilmelidir.

6. YAPTIRIM

Bu politikaya aykırı hareket eden çalışanlar ve ilgili taraflar hakkında, olayın niteliğine göre Kurumun ilgili prosedürleri, sözleşmeleri, disiplin hükümleri ve yürürlükteki mevzuat kapsamında gerekli işlemler uygulanır.

Üçüncü tarafların bu politikada veya sözleşmelerinde belirtilen bilgi güvenliği yükümlülüklerine aykırı hareket etmesi halinde, sözleşmesel hükümler ve ilgili mevzuat kapsamında gerekli işlemler gerçekleştirilir.