## İÇİNDEKİLER



| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| BİLGİ GÜVENLİĞİ BİRİMİ | BİDB ŞUBE MÜDÜRÜ | BİDB DAİRE BAŞKANI |

## 1. Amaç

Bu politikanın amacı, ESOGÜ BİDB bünyesinde çalışan personelin kullandıkları çalışma ortamlarında hassas bilgileri yetkisiz kişilerce erişimini engellemek için minimum gereklerin tanımlanmasıdır.

## 2. Kapsam

ESOGÜ BİDB bünyesinde görev alan ve hassas bilgilere erişebilen tüm personeli kapsar.

## 3. Dayanak

ESOGÜ BİDB bünyesinde gerçekleştirilen tüm kişisel verilerin güvenliği ile ilgili ISO:27001 Standardı ve Türkiye Cumhuriyeti Cumhurbaşkanlığı Siber Güvenlik Başkanlığı Bilgi ve İletişim Güvenliği Rehberi'nde yer alan tedbir maddeleri dayanak alınır.

## 4. Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

## 5. Sorumlular

Bu talimatnamenin oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Talimatnamenin uygulanmasından Sunucu ve İnternet Sistemleri Yönetim Birimi ve Yazılım Birimi personeli sorumludur.

## 6. Kurallar

Uygulama geliştirilirken

### 6.1. Kayıt Yönetimi

- Veri tabanı tablolarının tasarımında kişisel veriler (T.C. kimlik numarası, pasaport numarası vb.) birincil anahtar olarak kullanılmamalıdır.

| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| BİLGİ GÜVENLİĞİ BİRİMİ | BİDB ŞUBE MÜDÜRÜ | BİDB DAİRE BAŞKANI |

- İstemci ve sunucu uygulamalarında dosyalarda ve çerezlerde geçici olarak tutulan kişisel verilerin işleme gereksinimi veya kanuni saklama süresi sona erdiğinde güvenlik ihlali oluşturamayacak şekilde (geri getirilemeyecek, tekrar elde edilemeyecek vb.) yok edilmelidir.
- Veri tabanı tasarımı kişisel verilerin yedekleme, anonimleştirme ve veri aktarımı işlemlerini kolaylaştıracak şekilde yapılmalıdır.
- İlgili kişinin açık rızası olmadan kişisel veri web sayfalarının gizli alanlarında saklanmamalıdır. Kişisel veri, tarayıcı ön belleğinde (cache) saklanmamalıdır. Uygulamada kullanılan çerezlerin kişisel veri içermesi zorunluluk ise secure bayrağı (secure flag) kullanılmalıdır. Ayrıca, istemci tarafında web depolama (web storage) özelliği ile kişisel veriler kayıt altına alınmamalıdır.
- Uygulamanın girdi olarak kullandığı kişisel veri üzerinde girdi/çıktı doğrulama eksikliğinden kaynaklı zafiyetlere karşı güvenlik kontrolleri uygulanmalıdır.

### 6.2. Erişim Kayıtları Yönetimi

- Kişisel veri barındıran ortamlara yapılan başarılı ve başarısız erişimler kayıt altına alınmalıdır.
- Erişim kayıtları özel nitelikli kişisel veri barındırmamalıdır. Kayıtlarda özel nitelikli kişisel verinin bulundurulmasının zorunlu olduğu durumlarda, işlem detayının anlaşılabileceği şekilde kişisel verilerin güvenliği maskeleme vb. yöntemler ile sağlanmalıdır.
- Kişisel veriye gerçekleştirilen erişim kayıtları dışarı ve içeri aktarılabilir olmalıdır. Çalışan sistem üzerinde yapılacak içeri aktarma işlemi mevcut kayıtları yok etmemeli veya değiştirmemelidir.

### 6.3. Yetkilendirme

- Özel nitelikli kişisel verilerin tutulduğu ortamlara erişim için çok faktörlü kimlik doğrulaması yapılmalıdır.
- Dış sistemler/uygulamalar arası kişisel veri akışı için erişim doğrulama kontrolü yapılmalıdır. Dış sistemler ve uygulamalar arasındaki kişisel veri akışlarında erişim ile ilgili girdi parametreleri ve sonuçlar kayıt altına alınmalıdır.
- Sistem içi kişisel verinin akışı için erişim doğrulama kontrolü yapılmalıdır.

## 7. Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.