GAZİ ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

ÜÇÜNCÜ TARAF BİLGİ GÜVENLİĞİ POLİTİKASI

Revizyon Tarihçesi

Revizyon No	Revizyon Gerekçesi	Revizyon Tarihi

İçindekiler Tablosu

1. AMAÇ

Bu politika BİDB bünyesinde üçüncü taraflar ile yapılan sözleşmeler çerçevesinde güvenlik esaslarının belirlenmesi, üçüncü taraflara erişim yetkisi tahsisi konularında uyulacak esas ve usulleri belirlemek üzere hazırlanmıştır.

2. KAPSAM

Bu politika, yapılan sözleşmeler kapsamında BİDB bilgi işlem altyapısını kullanmakta olan, erişen, yöneten, saklayan veya işleyen hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

3. TANIMLAR VE KISALTMALAR

Kurum	Gazi Üniversitesi
BİDB	Bilgi İşlem Daire Başkanlığı
BGYS	Bilgi Güvenliği Yönetim Sistemi
Kullanıcı	Kurumsal Bilgiye Erişen Kişi

4. POLİTİKA

- Üçüncü taraf personeline kurum bilgi sistemlerine erişim izni, erişilecek sistem sahibi ve BGYS Birimi tarafından aşağıdaki esaslar dikkate alınarak gerçekleştirilecek değerlendirme çerçevesinde sağlanacaktır:
  - Üçüncü taraf çalışanı veya firma temsilcisi erişmek istediği bilgi sistemlerini ve ne amaçla erişeceğini ilgisi sistemin sahibine bildirir.
  - Erişimin şekli ve seviyesi (fiziksel erişim, mantıksal erişim, erişimin kurum içinden veya dışından sağlanması gibi) Fiziksel Güvenlik Uygulamaları Prosedürü ve Erişim Denetimi Politikası'na uygun olarak belirlenir.
  - Erişilecek bilginin hassasiyeti ve değeri Sistem Sahibi tarafından belirlenmelidir.
  - Üçüncü taraf personel tarafından gerçekleştirilecek erişim esnasında uygulanacak denetim kuralları ve erişimin nasıl kayıt altına alınacağı BGYS Birimi tarafından belirlenir.
  - Kurum harici tarafların erişimine açık olmayan bilgilerin korunması için gerekli kontroller BGYS Birimi tarafından tanımlanmalıdır. İlgili kontrollerin uygulanması sistem yöneticileri sorumluluğundadır.
  - Kurum dışındaki taraflara ilişkin hukuki ve yasal şartlar ve bunların sözleşmeden doğan yükümlülükleri Sistem Sahibi ve ilgili Birim Sorumlusu tarafından dikkate alınmalıdır.

- Mevcut bilgi güvenliği politikasının, prosedürlerinin ve talimatlarının korunması ve iyileştirilmesi de dahil olmak üzere hizmet alımı ile ilgili değişiklikler söz konusu olduğunda üçüncü taraflara ilişkin riskler Sistem Sahibi ve BGYS Birimi tarafından gözden geçirilmelidir. Değişiklik talepleri hem kurumumuzdan hem de üçüncü taraflardan gelebilir.

- Gizlilik maddeleri içeren sözleşme veya gizlilik anlaşmasına imza atmadan üçüncü taraf personele hassas verilere erişim izni tanınmamalıdır. Bu sözleşme veya gizlilik anlaşmalarında bağlantı veya erişim şartları belirlenmelidir.

- Üçüncü taraf, sözleşme kapsamındaki faaliyetlerini yerine getirmek üzere kurum ağına dışarıdan getireceği bir sistem bağlamayı talep ederse ilgili bağlantı BİDB tarafından verilecek izin ve belirlenecek esas ve usuller çerçevesinde yapılabilecektir.

- Kurumumuz bilgi sistemlerine erişim yetkisi sağlanmış olan üçüncü taraf firma ve organizasyonlar güvenlik ile ilgili konularda irtibat sağlanabilecek bir kişi belirtmelidir.

- Üçüncü taraf firma ve organizasyonlar tarafından Başkanlık bilgi sistemlerine uzaktan erişim ihtiyacı hasıl olduğunda buna ilişkin talepler ve verilen izinler (erişimin zaman aralığı, nereden ve kim tarafında erişildiğini belirtecek şekilde) kayıt altına alınmalıdır. Uzaktan erişim, BİDB'den sorumlu Daire Başkanının izni ile ve ilgili prosedürler çerçevesinde belirlenen esas ve usullere uygun olarak gerçekleştirilir.

- Üçüncü taraf personelin kurumumuz teknoloji ağı ve sistemlerine erişimi, hizmet sözleşmelerinde tanımlanan görevlerinin gerektirdiği ile sınırlıdır.
- Üçüncü taraf personelin görevi gereği kurumumuz sistemlerine / uygulamalarına erişimi Erişim Denetimi Politikası ve Parola ve Şifreleme Politikasına uygun olarak sağlanacaktır.
- Üçüncü taraf personelin sözleşmede tanımlı olan görevi yerine getirebilmesi için kurumumuz bilgi sistemlerine ayrıcalıklı haklarla erişmesi gerekiyorsa (örn, root veya admin dengi yetkilere sahip olarak) aşağıdaki şartların yerine getirilmiş olması gerekir:
  - Erişim yetkisi "**Bilmesi Gerek Prensibi**" temeline dayanarak verilmelidir.
  - Ayrıcalıklı hesaplara erişim yetkisi Erişim Denetim Politikası takip edilerek verilmelidir.
  - Ayrıcalıklı hesaplara erişim yetkisi "görevler ayrılığı" güvenlik prensibine dayanacaktır ve bu hesaplar kişiye özel olmalı ve yetkili personeller tarafından izlenebilmelidir.

- Etki alanında üçüncü taraflar için açılan hesaplar sözleşme süresi bitiminde derhal kapatılır.

- Üçüncü taraf firma ve organizasyonlarla yapılacak sözleşmelerde güvenlik gereksinimlerinin yerine getirilmesi için aşağıdaki şartların anlaşmaya dahil edilmesi sağlanmalıdır.
  - Kurumumuz Bilgi Güvenliği Politikasına atıfta bulunulması.
  - Varlıkların korunmasına yönelik uygulanacak denetimler. Bu kapsamda;
    - Bilgi, yazılım ve donanım dahil olmak üzere tüm varlıkların korunmasına yönelik yerine getirilmesi gereken yükümlülükler
    - Uygulanacak fiziksel güvenlik kontrolleri ve mekanizmaları
    - Kötü amaçlı yazılımlara ilişkin güvenlik kontrolleri
    - Varlık üzerinde herhangi bir tahribat veya tahrifatın mevcut olup olmadığını anlamaya yönelik uygulanacak denetimler
    - Anlaşma sona erdiğinde veya anlaşma henüz yürürlükteyken kararlaştırılan bir zaman diliminde bilginin iadesini veya imha edilmesini temin etmek için uygulanabilecek önlemler
    - Bilginin çoğaltılması ve ifşa edilmesi ile ilgili kısıtlamalar
  - Kullanıcının uyulması gereken güvenlik konularında eğitilmesi
  - Gerekli durumlarda anlaşılır ve belirlenmiş bir bilgi değişim yönetimi
  - Sözleşme kapsamında hizmet sağlayacak personelin değişimi ile ilgili hükümler
  - Üçüncü taraf firmalar ile yapılan sözleşmeler kapsamında Başkanlığımız bilgi sistemlerine erişerek faaliyet gösteren personelin bilgi sistemlerine erişimi ile ilgili esas ve usuller sözleşmede belirlenmelidir. Bu kapsamda sözleşmede yer alması gereken asgari şartlar şunlardır:
    - Üçüncü taraf firma personeli fiziksel güvenlik de dahil olmak üzere tüm güvenlik politikalarına, prosedürlerine ve ilgili mevzuata uygun hareket etmelidir
    - Başkanlık üçüncü taraf personelin bilgi sistemlerine erişimini izleme ve kendi takdiri doğrultusunda bu erişimi engelleme hakkına sahiptir
    - Üçüncü taraf personel tarafından yerine getirilen çalışmalar esnasında oluşan/kullanılan varlıklar anlaşma feshedildikten sonra sahibine iade edilmeli veya imha edilmelidir;
    - Bilgi varlıklarına erişim hakkı anlaşma sonlandıktan sonra iptal edilmelidir,
    - Üçüncü taraflar, kurumumuza sağlanan hizmetlerle ilgili herhangi bir alt yüklenici kullanma kararı almadan önce kurumumuza danışmalı, onay almadan

hiçbir surette alt yüklenici çalıştırmamalıdır.

- Üçüncü taraflarla yapılan gizlilik anlaşmaları veya iş sözleşmeleri bilgiye ve bilginin taşındığı fiziksel ortamlara yönelik koruma mekanizmalarını içermelidir.
- Üçüncü taraflarla yapılan gizlilik anlaşmaları veya iş sözleşmelerinde, bilginin dinlenmesi, çoğaltılması, değiştirilmesi, yanlış yönlendirilmesi ve imhası ihtimaline karşı alınacak güvenlik önlemleri belirtilmelidir.
- Üçüncü taraflarla yapılan gizlilik anlaşmaları veya iş sözleşmelerinde, elektronik haberleşme yoluyla geçebilecek kötü niyetli yazılımlara karşı alınacak güvenlik önlemleri belirtilmelidir.
- Üçüncü taraflarla yapılan gizlilik anlaşmaları veya iş sözleşmelerinde, bilgi iletimi ortamları ve koşullarından bahsedilmelidir.
- Üçüncü taraflarla yapılan iş sözleşmelerinde hassas bilgi tanımı açıkça yapılmış olmalıdır.

5. YAPTIRIM VE CEZA

Tüm kullanıcılar Üçüncü Taraf Bilgi Güvenliği Yönetim Sistemi Politikası ile birlikte; BGYS kapsamındaki tüm ilgili politika ve prosedürlerdeki kuralları bilmek ve bu kurallara uymaktan, bilgi varlıklarına erişim hakkı istemek için kurum tarafından onaylanmış süreç ve prosedürleri kullanmaktan, şifre, e-imza gibi kurum tarafından verilmiş olan kimlik doğrulama bilgilerini korumaktan, bilgi kendi kullanımındayken bilginin gizliliğini, bütünlüğünü ve erişebilirliğini varlık sahibi tarafından belirlenen önlemlere uygun olarak korumaktan sorumludur. Üçüncü Taraf Bilgi Güvenliği Yönetim Sistemi Politikası tarafından düzenlenen kurallara uymayanlara Disiplin Prosedürü çerçevesinde yaptırım ve cezalar uygulanır. Bu cezalar 657 sayılı Devlet Memurları Kanunu ve kişinin bağlı olduğu ilgili diğer mevzuatlara uygun olarak belirlenir.

6. GÖZDEN GEÇİRME VE ONAY

Üçüncü Taraf Bilgi Güvenliği Yönetim Sistemi Politikası yılda bir kez BGYS Sorumlusu koordinesinde gözden geçirilir ve varsa değişiklikler Bilgi İşlem Daire Başkanı tarafından onaylanır. Gözden geçirme, Yönetimin Sistemi Gözden Geçirme Toplantısı gündemine alınarak gerçekleştirilir.