PAMUKKALE ÜNİVERSİTESİ
BİLGİ YÖNETİMİ POLİTİKASI

Pamukkale Üniversitesi (PAÜ), bilgi yönetimi politikasının (BYP) amacı, tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamak ve aynı zamanda uyulması gereken kuralları ortaya koymaktır. Bu politika kurum bünyesinde bulunan ve bilgi işlem altyapısını kullanmakta olan tüm birimleri ve bağlı kuruluşları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamakla birlikte;

a) Veri dosyaları, sözleşmeler vb. den oluşan bilgi varlıkları,
b) Uygulama yazılımları, sistem yazılımları ve hizmetlerden oluşan yazılım varlıkları,
c) Yönlendirici cihazları, güvenlik cihazları, sistem yönetim sunucuları, yasal yükümlülükler kapsamında kurulmuş sunucu sistemleri, bilgisayarlar, iletişim donanımı ve veri depolama ortamlarını içeren fiziksel varlıklar,
d) Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan oluşan hizmet varlıkları,
e) Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıklarını kapsamaktadır.

Bilgi Güvenliği Hedefleri ve Prensipleri

PAÜ BYP politikası, üniversite personeline kurumun bilgi güvenliği gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, personelin bilinç ve farkındalık seviyelerini artırmak ve bu şekilde üniversitemizde oluşabilecek riskleri asgari düzeye indirmek, üniversitemizin itibarını ve bilgi güvenliği imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş gizlilik ve uygunluğu temin etmek, teknik açıdan bilgi güvenliği tedbirlerini almak, kurumun temel ve destekleyici iş faaliyetlerini en az kesinti ile devam etmesini sağlamayı hedeflemektedir. Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir.

- Kurumu içeriden veya dışarıdan gelebilecek tehditlere karşı korumak,
- Üretilen veya kullanılan bilgilerin gizliliğini güvence altına alarak kurumun imajını korumak,
- Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak,

- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak
- Bilgi Güvenliği Prosedürlerini yerine getirerek personelin bilgi güvenliği farkındalıklarını artırmak amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

Söz konusu risk yönetimi faaliyetlerinde amaç, üniversitemiz bünyesinde bulunan bilgi varlıkları için risk seviyesini kabul edilebilir risk seviyesinin altında tutmaktır. Kabul edilebilir risk seviyesinin altında kalan bilgi varlıkları için de aksiyonlar atanarak iyileştirme çalışmaları yapılması amaçlanmaktadır.

Bilgi Güvenliği İlkeleri

Bilgi güvenliği ilkeleri, kurumdaki bilgi güvenliği ile ilgili genel kuralları koyar. Bu ilkeler kullanıcılara çeşitli konu ve kavramlarla ilintili beklenen davranışları tanımlar. Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:

a) Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalıdır,
b) Kritiklik düzeylerine göre işlediği bilgiyi yedeklemelidir,
c) Risk düzeylerine göre belirlenen güvenlik önlemlerini almalıdır,
d) Bilgi güvenliği ihlal olaylarını bilgi güvenliği yetkilisine bildirmeli, raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır,
e) Kurum içi bilgi kaynaklarını (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletmemelidir,
f) Kurum bilişim kaynaklarını, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetlerde kullanmamalıdır,
g) Kurumun tüm çalışanları; bu politikaya, izlek ve talimatlarına uymakla sorumludur.
h) İş süreçlerinin gereksinimi olarak her türü bilgi, en az kesintiyle kapsam dâhilindeki birimler, hizmet verenler ve gereken üçüncü taraflarca erişilebilir olacaktır.
i) Bilgilerin bütünlüğü her durumda korunacaktır.
j) Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.
k) Bilgi Güvenliği Yönetim Sisteminin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeye indirilecektir.
l) Bilgi; bilginin elektronik iletişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak korunacaktır.