Veri Sınıflandırma Politikası

DEĞİŞİKLİK TAKİP LİSTESİ

No	Tarih	Açıklama
00		İlk Yayın

İÇİNDEKİLER

1. AMAÇ 2
2. KAPSAM 2
3. SORUMLULUKLAR 2
4. VERİ SINIFLANDIRMA 2
4.1. VERİ SINIFLANDIRMA SEVİYESİ 2
5. UYGULAMA 3
6. YENİDEN SINIFLANDIRMA 3
7. İLGİLİ DOKÜMANLAR 3

1. AMAÇ

Bu politika ile Pamukkale Üniversitesi bilgi varlıklarının kritiklik düzeyine uygun sınıflandırmasına ilişkin kuralları belirleyerek verilerin erişimi, işlenmesi ve saklanmasına dair bir çerçeve oluşturulması amaçlanmıştır. Verilerin sınıflandırılması bilgi varlıklarının korunması için temel güvenlik kontrollerinin belirlenmesine yardımcı olacaktır.

2. KAPSAM

Pamukkale Üniversitesi Bilgi Teknolojileri ve sistemleri başta olmak üzere basılı ve dijital tüm bilgi varlıklarını ve tüm çalışan, yüklenici, üçüncü taraf ve veriye erişim yetkisi olan tüm paydaşlarını kapsamaktadır.

3. SORUMLULUKLAR

Bilgi varlığının yönetilmesi, oluşturulması, işlenmesi, yayınlanması ve imhasından sorumlu tüm kişiler ilgili veri yönetim politika, prosedür ve talimatlarına uygun davranmaktan ve/ veya uyulmasını sağlamaktan sorumludur. Bu politikanın uygulatılmasından üniversitemiz üst yöneticisi sorumludur. Bu politika ve bağlı diğer politikaların ihlal edilmesi/ ihlal edilmesine sebep olunması durumunda İhlal Olayı Yönetimi Prosedürüne göre işlem yapılır.

4. VERİ SINIFLANDIRMA

4.1. VERİ SINIFLANDIRMA SEVİYESİ

Bilgi Güvenliği bağlamında bilgi varlıklarının seviyelerine göre sınıflandırılması hassasiyet düzeyine göre verilerin ifşa edilmesi, değiştirilmesi veya yok edilmesi durumunda üniversiteye olan etkisine göre sınıflandırılmasıdır. Buna göre bilgi kaynaklarını aşağıdaki derecelere göre sınıflayabiliriz.

Sınıflandırma	Tanım
Tasnif Dışı	Halka açık bilgilerdir. Bilgiye herhangi bir kişinin erişmesi, kurum dışına çıkması kurum için bir kayıp/zarar oluşturmaz. Örneğin, vizyon, misyon, kurumsal duyurular, kurumsal faaliyetler gibi.
Hizmete Özel	Bilginin kurum dışına çıkması durumunda göz ardı edilebilir düzeyde kayıp/sıkıntı yaşanabilir. Bilgiye erişim kurum içerisindeki belirli çalışanlara açıktır. Prosedürler, süreç bilgileri, bölüm / birim bilgileri, kazaya ramak kaldı raporları gibi içerdiği konular itibarıyla diğer gizlilik dereceli konular dışında olan ancak güvenlik işlemine ihtiyaç gösteren evrak, belge, doküman ve bilgiler Hizmete Özeldir.
Gizli	Bilgiye yetkisiz erişim durumunda ciddi kayıplar/zararlar oluşabilir. Örneğin, imaj kaybı, tazminat ödenmesi, sözleşme feshi, pazar kaybı, müşteri kaybı vb. Bilgiye erişim "bilmesi gereken ilkesi" ne uygun olarak kısıtlanmalıdır. Proje raporları, yatırım projeleri, marka tesciline ait bilgiler, proje değerlendirme raporları, detaylı topoloji, kurum bütçesi, performans raporları vb.
Çok Gizli	Bilginin yetkisiz kişilerin eline geçmesi veya ifşa edilmesi durumunda çok ciddi büyüklükte kayıplara, zararlara ve imaj kaybına yol açabilir. Yönetim kurulu kararları,

	stratejik plan, yatırım planları, şifreler, Ar-ge projeleri, BT güvenliğine ilişkin analiz raporları. vb. İfşası durumunda kurum hakkında kapatma davası açılması, üst yönetimden tutuklamalar, vb. konulara neden olabilir. Kişiye özel bilgiler çok gizli sınıfında değerlendirilir. Kurum çalışanları ve kuruma hizmet veren tedarikçi çalışanlarının özel bilgileridir. Bilginin kurum dışına çıkması / kurum içinde paylaşılması, yayılması yasal ve mevzuata aykırı uygunsuzluk yaratabilir. Örnek: Çalışan maaş bilgileri, hastalık / tahlil sonuçları, mahkeme ilamları gibi Kişiye Özel bilgiler çok gizli olarak sınıflandırılır.

5. UYGULAMA

Bilgi güvenliğinin amacı Bilgi Güvenliği Politikasında belirtildiği gibi üniversite bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini korumaktır. Bu nedenle bilgi varlıkları ortamı ve kaynağından bağımsız olarak veri sınıflandırma çizelgesine uygun kategorilere göre sınıflandırılarak korunmalıdır. Çizelgede belirlenmeyen bilgi varlıkları içeriklerinin kapsamına göre değerlendirilerek içeriği ve içeriğin tehlikeye atılmasıyla oluşacak risklere göre mümkün olduğu kadar düşük ancak gerektiği kadar yüksek seviyede sınıflandırılmalıdır.

6. YENİDEN SINIFLANDIRMA

Yasal ve sözleşmeden doğan yükümlülüklerdeki değişikliklerin yanı sıra verilerin kullanımındaki veya Üniversite için değerindeki değişikliklere bağlı olarak atanan sınıflandırmanın hala uygun olduğundan emin olmak için Kurumsal Verilerin sınıflandırılmasının periyodik olarak yeniden değerlendirilmesi önemlidir. Bu değerlendirme ilgili komisyon tarafından yapılmalıdır. Yıllık bazda bir değerlendirme yapılması önerilir; ancak, komisyon mevcut kaynaklara göre hangi sıklığın en uygun olduğunu belirlemelidir.

Veri kümelerinin yeniden değerlendirilmesi gerektiği ve mevcut kontrollerde boşlukların tespit edildiği durumlarda komisyon tarafından karar verilerek yeni düzenlemeler belirlenir.

7. İLGİLİ DOKÜMANLAR

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

6698 sayılı Kişisel Verilerin Korunması Kanunu

ISO 27001 Varlık Sınıflandırması Ve Etiketleme Talimatı

Pamukkale Üniversitesi Bilgi Güvenliği Politikası

Pamukkale Üniversitesi Varlık Yönetim Prosedürü

Pamukkale Üniversitesi İhlal Olayı Yönetimi Prosedürü

657 sayılı Devlet Memurları Kanunu

2547 sayılı Yükseköğretim Kanunu