1.AMAÇ

Bu politika, Hakkari Üniversitesi veri tabanlarının güvenliğini sağlamak, yetkisiz erişim ve veri ihlallerini önlemek, Üniversite'nin bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaçlar.

2.KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında Hakkari Üniversitesi bünyesinde kullanılan tüm veri tabanlarını ve veri tabanlarına erişen tüm kullanıcıları kapsar.

3.TANIMLAR VE KISALTMALAR

3.1.Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, risk yaklaşımına dayalı yönetim sistemidir.

3.2.Bilgi: Hakkari Üniversitesi süreçlerinin devamlılığı için gerekli olan ve bu nedenle değeri olan, dolayısı ile uygun şekilde korunması gereken bir veridir.

3.3.Bilgi varlıkları: TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi dâhilinde Hakkari Üniversitesi'nde bulunan ve bilgi güvenliği için anlam taşıyan tüm varlıklar.

3.4.Üniversite: Hakkari Üniversitesi

3.5.Rektör: Hakkari Üniversitesi Rektörü.

3.6.Kalite Yönetim Temsilcisi: Kalite Yönetim Sistemi şartlarını, gerekli proseslerin oluşturulmasını, uygulanmasını ve sürekliliğini sağlayarak, Hakkari Üniversitesi Kalite Yönetim Sisteminin performansı ve iyileştirme için fırsatlar ile ilgili üst yönetime rapor sunan, Hakkari Üniversitesinde, müşteri şartlarının bilincinde olunmasını tüm çalışanlarda sağlayan, Hakkari Üniversitesi Kalite Yönetim Sistemindeki değişiklikleri planlayan ve uygulayan, kalite yönetim sisteminin bütünlüğünü güvence altına alan Hakkari Üniversitesi çalışanı

3.7.Daire Başkanı: Hakkari Üniversitesi Bilgi İşlem Daire Başkanı

3.8.Veri Tabanı: Veri yönetim sistemi tarafından organize edilen ve depolanan yapılandırılmış veri

koleksiyonudur.

3.9.Log kaydı: Bir sistemdeki olayların ve işlemlerin tarih ve saat bilgisi ile birlikte sıralı bir şekilde tutulduğu metin dosyasıdır.

4.SORUMLULAR

4.1.Bilgi Güvenliği Yönetim Sistemi Komisyonu: Bu politikanın hazırlanmasından ve güncellenmesinden sorumludur.

4.2.Rektör: Politikanın onaylanması ve yürürlüğe konulmasından sorumludur.

4.3.Kalite Yönetim Temsilcisi: Prosedürün KYT-PRD-01 Dokümanların Kontrolü Prosedürü'ne göre kontrol edilmesinden, prosedüre doküman kodu verilmesinden, prosedür revizyona uğrarsa takibinden ve revizyon numarasının verilmesinden, prosedürün güncel doküman listesine eklenmesinden ve listenin takibinden sorumludur.

4.4.Daire Başkanı: Politikanın kontrolü ve uygulanabilirliğinin sağlanmasından sorumludur.

4.5.İlgili Personel/Birim: Politika içinde belirtilen faaliyetlerin gerçekleştirilmesinden sorumludur.

5.UYGULAMA

5.1. Veritabanı sistemleri envanteri BLG-LST-Veri Envanteri Listesi işlenerek dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.

5.2. Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir. Log kayıtlarına, yetkilinin izni olmadan kesinlikle hiçbir şekilde erişim yapılamaz.

5.3. Veri tabanı aksiyon ve güncellemelerinde erişim yetkisi sadece Hakkâri Üniversitesi Bilgi İşlem Daire Başkanlığı Yazılım& Web Şubesi'ne ait olup, yetkilendirme işlemleri BLG-PRD-XXX Kullanıcı Hesap Yönetimi ve Erişim Yetkilendirme Prosedürüne uygun yapılmalıdır.

5.4. Veri tabanı yedekleri Ağ ve Sistem Hizmetleri Şubesi çalışanı tarafından belirlenip ve yedekler BLG-PRD-XXX Yedekleme Prosedürü çerçevesinde düzenli aralıklarla alınmalıdır.

5.5. Veri tabanı sistemlerinde yapılacak bakım onarım, yama ve güncelleme çalışmalarından önce, Hakkâri Üniversitesi Bilgi İşlem Daire Başkanlığı Yazılım&Web Şubesi tarafından ilgili birimlere duyuru yapılmalıdır.

5.6. Veri tabanına acil erişim gerekmesi durumunda aksiyon öncesinde ve sonrasında Daire Başkanı'na Yazılım&Web Şubesi tarafından bilgilendirme yapılır.

5.7. Veri tabanı sunucuları fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulmalıdır.

5.8. Veri tabanı sunucularının kaynakları (cpu, ram, disk, ağ trafiği vb.) düzenli olarak kontrol edilmelidir.

5.9. Veri tabanı çalışmalarında canlı ortam ile test ortamı ayrı olmalıdır.

5.10. Veri tabanlarına Üniversite dışından erişim sağlayan tedarikçiler ile Bilgi İşlem Daire Başkanlığı arasında Gizlilik Sözleşmesi imzalanacaktır.

5.11. Veri tabanlarına tedarikçiler tarafından Üniversite dışından yapılacak erişimler BLG-POL-XXX Uzak Erişim Politikası'na uygun olmalıdır.

5.12. Politika ihlali disiplin kurallarına tabi olmanıza neden olabilir ve yasal sonuçlar doğabilir.

6.İLGİLİ DOKÜMANLAR

6.1. BLG-PRD-XXX Kullanıcı Hesap Yönetimi ve Erişim Yetkilendirme Prosedürü

6.2. BLG-PRD-XXX Yedekleme Prosedürü

6.3. BLG-POL-XXX Uzak Erişim Politikası