1. AMAÇ

Bu politika, içeriden veya dışarıdan gelebilecek her türlü tehdide karşı Hakkari Üniversitesinde kullanılan bilgi varlıklarını korumak, bilgiye erişilebilirliği iş prosesleriyle gerektiği şekilde sağlamak, yasal mevzuat gereksinimlerini karşılamak, sürekli iyileştirmeye yönelik çalışmalar yapmak ve üniversite bünyesinde çalışanların ve diğer ilgili tarafların uyması gereken bilgi güvenliği şartlarının çerçevesini çizmek amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika,Hakkari Üniversitesi Bilgi İşlem Daire Başkanlığı yönetimindeki TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi dâhilinde Hakkari Üniversitesi'nde bulunan ve bilgi güvenliği için anlam taşıyan tüm varlıkları 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. Gizlilik: Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır.

3.9. Bütünlük: Bilginin yetkisiz kişilerce değiştirilmemesi, silinmemesi ve bozulmamasıdır.

3.10. Erişilebilirlik: Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

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: Politikanın KYT-PRD-01 Dokümanların Kontrolü prosedürüne 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. Kullanıcı: Politika içinde belirtilen faaliyetlerin gerçekleştirilmesinden sorumludur.

5. UYGULAMA

5.1. Bu politika ile iç ve dış paydaşların bilgi varlıklarına güvenli bir şekilde erişimini sağlanır.

5.2. Bilgi varlıklarını korumak için, mevcut en iyi uygulamaları esas alarak varlıkların saklanması, iletilmesi, erişilmesi, işlenmesi faaliyetleri kontrol altına alınmalı, görevler ayrılığı prensibi ile süreç içi kontrollerin kurulmuş olması sağlanmalıdır.

5.3. İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı Üniversitenin bilgi varlıklarını korumayı, bu varlıkların kullanımının kesintisiz ve güven içinde devam etmesi için bilgi güvenliği şartlarını uluslararası standartlar, yasa ve mevzuatlar çerçevesinde sağlanır ve işletilir.

5.4. Yürütülen tüm faaliyetlerde Bilgi Güvenliği Yönetim Sisteminin üç temel öğesi olan gizlilik, bütünlük, erişilebilirliğin sürekliliği sağlanmalıdır.

5.5. Bilgi varlıkları üzerinde oluşabilecek riskler BLG-FRM-XXX Risk Analiz Formu ile dokümante edilip değerlendirilmeli, bu riskleri azaltmak için gerekli donanım, yazılım, eğitim için gerekli kaynaklar ve BGYS' nin devamlılığı sağlanmalıdır.

5.6. Bilgi güvenliğine ilişkin riskleri göz önünde bulundurarak, Üniversitenin güvenilirliği ve itibarı korunmalıdır.

5.7. Bilgi güvenliğinin ihlali durumunda BLG-PRS-XXX Bilgi Güvenliği Olayları İhlal Prosedürü istinaden gerekli yaptırımlar uygulanır.

5.8. Bilgi Güvenliği konusunda tüm paydaşlarımızın bilinçlendirilmesi yönünde sürekli çalışma yapılmalıdır.

5.9. Tedarikçi Firma seçiminde, firmaları BLG-LST-XXX Onaylı Tedarikçi Listesine işlerken tedarikçilerin ve alt yüklenicilerinin bilgi güvenliği performansını dikkate almayı onlarla BGYS konularında işbirliği içinde olmak amaçlanmalıdır.

5.10. Çalışanlar ve üçüncü taraflarla kurumun gizlilik ihtiyaçlarını güvence altına almayı amaçlayan gizlilik anlaşmaları yapılır.

5.11. Bilgi Güvenliği Yönetim Sisteminin sürekli iyileştirilmesine yönelik çalışmaların üst yönetim tarafından gözden geçirilmesi sağlanır.

5.12. Bu politika ve bağlantılı diğer politika, yönerge ve prosedürlerin ihlal edilmesi veya ihlal edilmesine sebep olunması halinde Üniversite idari/sözleşmeli personel için 4857 sayılı İş Kanunu, 657 sayılı Devlet Memurları Kanunu ile Devlet Memurları Disiplin Yönetmeliği, akademik personel için 2547 Sayılı Yükseköğretim Kanunu, öğrenciler için Yükseköğretim Kurumları Öğrenci Disiplin Yönetmeliği işletilmektedir.

6. İLGİLİ DOKÜMANLAR

6.1. KYT-PRD-01 Dokümanların Kontrolü prosedürü

6.2. BLG-FRM-XXX Risk Analiz Formu

6.3. BLG-PRS-XXX Bilgi Güvenliği Olayları İhlal Prosedürü

6.4. BLG-LST-XXX Onaylı Tedarikçi Listesi