1. AMAÇ

Bu politikanın amacı, Hakkari Üniversitesi'nin fiziksel varlıklarının, bilgi sistemlerinin ve çalışanlarının korunmasını sağlamak ve yetkisiz erişimi, hırsızlığı, sabotajı ve diğer güvenlik risklerini en aza indirmektir.

2. KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında bilgi varlıklarına erişim sağlayan tüm fiziksel güvenlik konularını ve akademik/idari personelleri kapsamaktadır.

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.

4. UYGULAMA

4.1. Üniversite bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.

4.2. Üniversite dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.

4.3. Tanımlanan farklı güvenlik bölgelerine erişim yetkileri düzenli aralıklar ile kontrol edilmelidir.

4.4. Ofis girişleri ve koridorlar güvenlik açısından kamera ile kayıt altına alınmalıdır.

4.5. Kritik bilgiler, kilitli dolap/çekmece/kasalarda muhafaza edilmelidir.

4.6. Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.

4.7. Ofislerde bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulmalıdır.

4.8. Bireysel kargolar, Üniversite girişinde güvenlik tarafından kargo getiren giriş bilgileri kayıt altına alınarak Üniversite içerisine giriş hakkı bulunmaktadır.

4.9. Kullanılan yazı tahtasını toplantı sonunda temizlemelidir.

4.10. Toplantıda yapılan çalışmaların, alınan kararların ve toplantı notların tutulduğu evrak ve belgeler toplantı yapılan alanda ya da çöp kovasında bırakılmamalıdır.

4.11. Güvenlik kameralarının yerleştirildiği alanlarda kameraların görüntü almasını engelleyecek herhangi bir fiziksel engel bulundurulmamalı, kameralar kapatılmamalı ve fiziksel hasar verilmemelidir.

4.12. Hasar / hırsızlık gibi oluşabilecek risklere karşı güvenlik sağlanmalıdır.

4.13. Ekipmanların kullanımı zimmetlenen kişiye aittir, bu ekipmanların güvenliğini sağlanması kişinin sorumluluğundadır.

4.14. Personeller, çalışma alanları için tahsis edilmiş politika, prosedür ve talimatlara uygun hareket etmelidir.

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