1.AMAÇ

Bu politika; Hakkari Üniversitesi veri merkezi güvenlik kontrollerini ve uyulması gereken kuralları sağlamaktadır.

2.KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında veri merkezi güvenlik kontrollerini ve veri merkezine erişimi olan 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

3.8.Veri Merkezi: Bilgisayar sistemleri, telekomünikasyon ekipmanları ve veri depolama birimleri gibi kritik bilgi işlem altyapısını barındıran özel olarak tasarlanmış ve kontrollü bir ortamdır.

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: Politika içinde belirtilen faaliyetlerin gerçekleştirilmesinden sorumludur.

5.UYGULAMA

5.1. Sistem odası/veri merkezi; yemekhane, su, havalandırma, atık su gideri, sulu yangın söndürme, havalandırma kanalları ve üniteleri, doğal gaz ve yanıcı bileşenlerin depolandığı yerler gibi risk teşkil edecek noktalardan mümkün olabildiğince uzakta konumlandırılmalıdır.

5.2. Sel baskını, böcek baskını, rutubet ve nem vb. gibi olaylara karşı uygun bir alanda olmalıdır.

5.3. Yangına karşı tüm riskler değerlendirilmeli ve önlemler alınmalıdır.

5.3.1. Kapı yangına dayanıklı olmalıdır.

5.3.2. Duvarlar yanmaz boya ile boyanmalıdır.

5.3.3. Yangın algılama ve alarm sistemleri kullanılmalıdır. Hem elle hem de otomatik olarak yapılan yangın söndürme sistemleri/cihazları kullanılmalıdır.

5.3.4. Yangın söndürme sistemi uygunluğu sağlanmalı yangın esnasında suyun elektronik cihazlara vereceği zarar için gerekli tedbirler alınmalıdır. Yangın durumunda veri merkezine suyla müdahale edilmemelidir.

5.4. Sistem odası/veri merkezinin depreme karşı dayanıklılık testi yapılmış olmalı ve bu durum belgelendirilmelidir.

5.5. Veri merkezi yerleşkesinde, gerekli yıldırım koruma tertibatı sağlanmalıdır.

5.6. Sistem odası/ veri merkezinde yanıcı, yakıcı, parlayıcı ve toz oluşturan maddeler bulundurulmamalıdır.

5.7. Data ve elektrik kablolama için TSE standartlarına uygun malzemeden imal edilmiş kablo kanalları kullanılmalıdır.

5.8.Tüm prizler, metal yapı elemanları topraklanmalıdır.

5.9. Veri merkezi topraklama ölçümleri periyodik olarak yapılmalı ve sonuçlar kayıt altına alınmalıdır.

5.10. Data kablolarının seçiminde yanmaya karşı dayanıklı kablolar seçilmelidir.

5.11. Kablolar döşenirken kıvrılmalara izin verilmemeli, 90 derecelik keskin dönüşler daha yumuşak şekilde yapılmalıdır.

5.12. IP Kamera ile izleme sistemi kurulmalı. Odanın durumu, giriş çıkışları ve yapılan işlemler kameralarla kayıt altına alınmalıdır.

5.13. Veri merkezine güvenli giriş sistemleri uygulanmalıdır.

5.14. Veri merkezine sadece yetkili kişiler tarafından giriş-çıkış yapılmalıdır.

5.15. Destek, bakım gibi hizmetler için Veri Merkezine giriş sağlayan kişilere, Ağ ve Sistem Hizmetleri Şubesi personelleri nezaretinde sınırlandırılmış şekilde erişim izni verilmelidir.

5.16. Veri Merkezinin bulunduğu alan ok, tabela vb. ile gösterilmemelidir.

5.17. Aktif soğutma klima, havalandırma fanı gibi ekipmanlar yedekli olarak kullanılmalı ve bakımları kontrol altında olmalıdır.

5.18. Veri Merkezindeki kabinlerin ve rafların depreme karşı güvenliğini sağlamak için bağlı bulundukları zeminlere sabitlenmelidir.