1.AMAÇ

Bu politika; Hakkari Üniversitesi, bilgi sistemleri ve ağ altyapısındaki güvenlik açıklarını, hataları ve performans iyileştirmelerini gidermek için gerekli yama yönetim süreçlerini tanımlamaktır.

2.KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında yürütülmesi, tüm bilgi sistemleri, ağ cihazları, sunucular, masaüstü ve dizüstü bilgisayarlar, mobil cihazlar,yazılımlar ile bilgi güvenliği yönetim sisteminin gerekliliklerinin Yama Yönetimi süreçlerinin sağlanmasını 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.Erişim: Herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı kazanılmasını,

3.9.Yama Yönetimi: İşletim sistemleri, uygulama yazılımları, veritabanları, ağ cihazları ve benzeri bilgi

teknolojileri varlıklarında bulunan açıklıklara karşı önlem almak.

3.10. Zafiyet: Zafiyet, bir sistemin veya varlığın, bir tehdidin zarar vermesine olanak tanıyan zayıf noktasıdır.

3.11. Sızma Testi: Sistemin güvenliğini değerlendirmek üzere bir bilgisayar sistemi üzerinde gerçekleştirilen yetkilendirilmiş temsili bir siber saldırıdır.

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/Kullanıcı: Politika içinde belirtilen faaliyetlerin gerçekleştirilmesinden sorumludur.

5. UYGULAMA

5.1. Güvenlik güncellemeleri başta olmak üzere işletim sistemlerine yönelik güncellemelerin ve yamaların üreticisi tarafından bildirilen en kararlı, güncel ve güvenilir sürüm dikkate alınarak yapıldığı, otomatik yazılım güncelleme araçları ile kontrol edilmelidir.

5.2. Yama Yönetiminde; mevcut varlıkların envanterlerinin çıkarılması, yeni yazılım güncellemeleri için kaynakların belirlenmesi,mevcut yazılım dağıtım altyapısının değerlendirilmesi, yama yönetim etkinliğinin değerlendirilmesi gerçekleştirilmelidir.

5.3. Üretici tarafından desteklenmeyen sistemler zafiyet içerebileceğinden, veri tabanı bilinen en kararlı versiyon ile kullanılmalıdır. Bu kapsamda, belirli periyotlar ile sistemlerin güncelliği kontrol edilmeli ve gerekli güncelleştirmeler gerçekleştirilmelidir.

5.4. Güvenlik yamaları, yayımlandıktan sonra mümkün olan en kısa zamanda ilgili sistemlere yüklenmelidir.

5.5. Üniversite bilişim altyapısında yer alan ağ ve sistemler ile kritik veri işleyen uygulamalara güvenlik açıklarının zamanında tespit edilmesi için yılda en az 1 (bir) defa teknik sızma testleri yapılmalıdır.

5.6. Dış Taraflarca Yapılan Açıklık Taramasında, alınan hizmet kapsamında sistem açıklık raporu hazırlanır ve gerekli aksiyonların alınması için ilgili ekiplere bilgilendirme yapılmalıdır. Bu durumda Bilgi İşlem Daire Başkanlığı tarafından;

5.6.1. Test kapsamı ve testi yapılacak sistemlerin gerekli bilgileri belirlenir.

5.6.2. Sızma testi ve/veya açıklık taramasını yapacak firma çalışanlarının yetkinlik belgeleri istenir.

5.6.3. Sızma testi ve/veya açıklık taraması için iş planları ve kullanacakları araçların listesi istenir. Kullanılacak açıklık tarama araçlarının sektörde kabul görmüş lisanslı araçlar olup olmadığı kontrol edilir.

5.6.4. Yapılacak çalışmanın takvimi hakkında Üniversite Yönetimi bilgilendirilir.

5.6.5. Çalışmayı yapacak firma çalışanlarına test ve taramalar için kullanıcı hesabı oluşturulur. Tarama bitiminde kullanıcı hesapları pasif hale getirilir.

5.6.6. Teknik açıklık taramalarının karşılıklı gizliliğini sağlamak amacıyla gerekli eklemelerle Gizlilik Sözleşmesi imzalanır.

5.7. Üniversite ağında daha fazla güvenlik gerektiren sistemler/sunucular ayrı bir ağda tutulmalıdır.

5.8. Üniversite kaynakları ile geliştirilen uygulamalara ilişkin güncellemeler ve yamalar Bilgi İşlem Daire Başkanlığınca gerçekleştirilir ve yürütülür.

5.9. Tedarikçiler tarafından geliştirilen uygulamalarda güncelleme ve yamalar tedarikçi tarafından gerçekleştirilir. Yapılan değişiklikler kayıt altına alınır ve Bilgi İşlem Daire Başkanlığına sunulur.

5.10. Bilgisayar ve taşınabilir cihazlar üzerindeki işletim sistemi ve uygulamaların yüklenmesi ve güncellenmesi kullanıcının sorumluluğundadır.

5.11. Güncelleme ve yamalar sadece üretici kaynaklarından temin edilmelidir.

5.12. Sistemlerde yeni yamalarının takip edilmesi, bu yamaların mevcut sisteme dağıtımından önce test edilmesi, yamaların ilgili bilgi varlıklarına dağıtılması Ağ ve Sistem Hizmetleri Şubesi tarafından yürütülmelidir.

5.13. Eksik yama ve güncellemeler canlı ortamda bulunan sistemlere kurulmadan önce test ortamında kurulmalıdır. Testten başarı ile geçen güncellemelerin canlı ortama kurulması için gerekli planlama yapılır. Acil olmayan güncellemeler mesai saatleri sonrasında gerçekleştirilebilir. Acil olan güncellemeler yönetimin izni ile gün içinde gerçekleştirilmelidir.

5.14. Hedef bilgisayarlarda güncellemenin yüklenmesi, dağıtım ve dağıtım sonrası bilgisayar durumları kontrol edilmelidir.

5.15. Uygulanan yamalar, tarihleri ve ilgili sistemlerle birlikte Ağ ve Sistem Hizmetleri Şubesi kontrolünde arşivlenir.