1.AMAÇ

Bu politikanın amacı, Üniversitemiz kullanıcılarının tüm bilgi sistemleri uygulamalarında ve kurumsal e-posta hesaplarında kullanılacak olan parolaların üretilmesi, korunması, kullanılması ve değiştirilme sıklığı hakkında kurumsal bir standart oluşturmaktır.

2.KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında kullanıcıların kullandıkları parola ile korunan bilgi varlıklarını 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.Kullanıcı: Hakkari Üniversitesi bilgi sistemlerine erişim yetkisi olan kullanıcılar.

4.SORUMLULAR

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

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

4.3.Rektör: Politikanın onaylanması ve yürürlüğe konulmasından sorumludur.

4.4.Kalite Yönetim Temsilcisi: Politikanın KYT-PRD-01 Dokümanların Kontrolü prosedürüne göre kontrol edilmesinden, politikaya doküman kodu verilmesinden, prosedür revizyona uğrarsa takibinden ve revizyon numarasının verilmesinden, prosedürün güncel doküman listesine eklenmesinden ve listenin takibinden sorumludur.

4.5.Kullanıcı: Politika içinde belirtilen faaliyetlerin gerçekleştirilmesinden sorumludur.

5.UYGULAMA

5.1.Parola Oluşturma Kuralları

5.1.1. Parolalar en az 8 karakter uzunluğunda olmalıdır ve bu karakterlerin en az bir tanesi sayılardan (örn: 1234567890), bir tanesi büyük harften (örn: ABCDEF...), bir tanesi küçük harften (örn: abcdef ...) ve bir tanesi de noktalama işaretinden (örn: !?., vb.) veya özel karakterden (örn: @#$%^&*()_+|~-=\`{}[]:";'<>/ vb.) oluşmalıdır.

5.1.2. Parola içeriği aile bireylerinin isimleri, doğum tarihleri, telefon numarası veya adres bilgileri gibi kişisel bilgiler içermemelidir.

5.1.3. Parolada "aaabbb, qwerty, zyxwvuts, 12345678, 123321..vb" gibi kelime veya rakam dizileri kullanılmamalıdır.

5.1.4. Oluşturulacak parola içerisinde Türkçe karakter (i,ö,ş,ü ..vb) bulunmamalıdır.

5.2.Parola Yönetimi ve Kullanımı

5.2.1.Üniversite çalışanları, kendilerine verilmiş olan kullanıcı adı ve parolaların sadece kendileri tarafından

kullanılması ilkesini koruma sorumluluğuna uymalıdırlar. Bu ilkenin ihlali durumda çalışan sorumlu olacaktır.

5.2.2. Kullanıcı hesaplarına ait parolalar (e-posta, web, masaüstü bilgisayar vs.) 6 (altı) ayda bir değiştirilmelidir.

5.2.3. Kullanıcı, yeni parola için, son kullanılan 3 paroladan farklı bir parola kullanmalıdır.Bilgi sistemlerinin şifre değiştirmede son 3 parolanın tekrar kullanılmasına izin vermeyecek şekilde yöntem geliştirmesi gerekmektedir.

5.2.4. Kullanıcı, sahip olduğu parolaları bağlı olduğu Daire Başkanlığı ve iş arkadaşları dâhil olmak üzere hiç kimse ile paylaşmamalıdır.

5.2.5. Kullanıcı, tarayıcılarda (Google Chrome, Firefox..vb) parola hatırlatma kullanmamalı veya üçüncü kişilerin erişebileceği şekilde kayıt altına almamalı ve paylaşmamalıdır.

5.2.6. Ağ ve Sistem Hizmetleri Şubesi çalışanları, kendi yönetimindeki sistem ile kendi kullanıcı hesapları için farklı parolalar kullanmalıdır.

5.2.7. Üniversite hesaplarına ait parolalar, hatırlamak amacıyla görünür ortamlarda (kağıt, bilgisayar, cep telefonu vb.) kayıt edilmemelidir.

5.2.8. Kullanıcılar, kullanmaya kısa süreli ara verdikleri bilgisayarları parola korumalı ekran koruyucu gibi özellikler kullanarak güvenlik altına almakla yükümlüdürler.

5.2.9. Kullanıcılar bilgisayar başından kalktığı zaman mutlaka Windows+L yaparak oturumlarını kilitlemelidirler. Genel kullanıcı bilgisayarları kullanılmadığı zaman otomatik olarak 5 dakika içerisinde şifreli ekran korumasına girecektir.

5.2.10. Hakkari Üniversitesi Bilgi İşlem Daire Başkanlığı Ağ ve Sistem Hizmetleri Şubesi tarafından size oluşturulan parolaları hemen değiştirmeniz gerekmektedir.

5.2.11. Bir kullanıcı hesabı birden çok kişi tarafından kullanılmamalıdır.

5.2.12. Üniversite çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının parolaları da kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

5.2.13. Kişisel Verilerin Korunması Kanunu ‘na istinaden kullanıcının bizzat kendi talebi olmaksızın parolası

sıfırlanamaz veya değiştirilemez.Eğer kullanıcının parola sıfırlama veya değiştirme talebi olursa BLG-PRS-XXX E-Posta Destek Talep prosesine uygun işlem yapılır.

5.2.14. Üniversitenin sağladığı kullanıcı hesaplarını kullanan tüm paydaşlar bu politikanın hükümlerini anlamak ve uygulamakla yükümlüdür.

5.2.15. Bu politikanın ihlal edilmesi durumunda BGYS komisyon başkanı tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel, Ağ ve Sistem Hizmetleri Şubesi çalışanları tarafından e-posta üzerinden yazılı olarak uyarılır. Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa "BLG-PRD Bilgi Güvenliği İhlal Olayları Prosedürü" gereğince işlem yapılır.

6.İLGİLİ DOKÜMANLAR

KYT-PRD-01 Dokümanların Kontrolü

BLG-PRS-XXX E-Posta Destek Talep Prosesi

BLG-PRD Bilgi Güvenliği İhlal Olayları Prosedürü