T.C.
İSTANBUL
KÜLTÜR
ÜNİVERSİTESİ

İKÜ BST

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

ŞİFRE YÖNETİMİ POLİTİKASI (ŞYP)

HAZIRLAYANLAR	KONTROL EDEN	ONAYLAYAN
Ufuk Dikme	İsmail Koç	
Bilgi Güvenliği Yönetim Müdürü	Bilgi Sistemleri ve Teknolojileri Daire Başkanı	Rektörlük Temsilcisi

İÇİNDEKİLER

1. AMAÇ 2
2. KAPSAM 3
3. DAYANAK 3
4. TANIMLAR VE KISALTMALAR 3
5. SORUMLULUK VE YETKİ TANIMLARI 4
6. İLGİLİ DOKÜMANLAR 5
7. ŞİFRE POLİTİKASININ HEDEFLERİ VE PRENSİPLERİ 5
8. ŞİFRE BELİRLEME KURALLARI 6
9. ŞİFRE KULLANIM POLİTİKASININ YAPTIRIMLARI 7
10. REVİZYON BİLGİSİ 7

1. AMAÇ

Bu politikanın amacı, T.C. İstanbul Kültür Üniversitesi kaynaklarına erişimde kullanılan şifrelerin üretilmesi, korunması, kullanılması ve değiştirilme sıklığı hakkında kurumsal bir standart oluşturmaktır. Şifreleme; bilgi güvenliği ve bilgi

kaynaklarına erişim kontrolü için kullanılan önemli bir yöntemdir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre, ağ güvenliğini tümüyle riske atabilir. Yetkisiz kişilerin bilgi kaynaklarına erişimi; bilginin gizliliği, güvenilirliği, bütünlüğü ve erişilebilirliğini riske atarak; İKÜ için güven kaybına ve maddi kayıplara sebep olabilir. Bu politika ile İKÜ 'de bilgi sistemleri ortamlarına erişirken kullanılan şifrelerin standartlara uygun biçimde oluşturulması, korunması, kullanılması ve değiştirilmesi, tanımlanan şifreler konusunda çalışanların bilgilendirilmesi ve şifre işlemlerinin İKÜ riskini en aza indirecek ve en güvenli şekilde yapılmasını sağlamak amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika, İKÜ 'nün sahip olduğu ve BSTDB tarafından yönetilen bilgi, sistem, iletişim ağı, uygulama ve diğer ortamlara erişim için gerekli tüm şifreleri kapsayarak, şifre verilen tüm İKÜ personeli, sözleşmeli personel, geçici personel ve İKÜ tarafından bilgiye erişim hakkı verilen 3. şahıslar ve İKÜ tarafından bilgiye erişim hakkı verilmiş herkes için geçerlidir.

3. DAYANAK

- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Ek.A.5.1.1, Ek.A.7.1.2, Ek.A.9.1, Ek.A.9.2, Ek.A.9 ve Ek.A.9.4 maddeleri.
- 15.03.2018 tarihli ve 19924119-719-E.21240 sayılı "2016-2019 Ulusal Siber Güvenlik Eylem Planı" konulu YÖK yazısında, üniversitelerin ISO27001 Bilgi Güvenliği Yönetim Sertifikası alması ve iş süreçlerini bu şekilde yapılandırması gerektiği ifade edilmiştir.

4. TANIMLAR VE KISALTMALAR

KISALTMALAR	TANIMLAR
BGYS	Bilgi Güvenliği Yönetim Sistemi: Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, sözleşmeleri, talimatları, prosedürleri, prosesleri ve tüm kaynakları içerir.
BSTDB	Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı
E-POSTA	Elektronik Posta
İKÜ	T.C. İstanbul Kültür Üniversitesi
KULLANICI	T.C. İstanbul Kültür Üniversitesi bünyesinde çalışan, akademik ve idari tüm çalışanlar ve sözleşme ile bağlayıcılığı sağlanmış dış firma çalışanları.

KULLANICI HESABI	Kullanıcının İKÜ bilgisayar sistemlerine giriş için kullandığı, tüm işlemlerde kullanıcıyı temsil eden ve kendisine tanımlanan şifre ile sisteme girişin mümkün olduğu sayısal, alfabetik kod veya alfa nümerik kişiye özel koddur.
ROOT, ADMINISTRATOR	Tam Yetkili Kullanıcı, Sistem Yöneticisi
ŞİFRE	Kullanıcının, bilgisayar sistemine veya uygulamaya kullanıcı hesabı ile birlikte kendisini tanıtmasını ve işlem yaratma ve/veya sonuçlandırmasını sağlayan, sadece kendisinin bildiği ve dilediğinde değiştirebileceği alfa numerik karakterlerden oluşan tanımdır
WORD WIDE WEB	Birbiriyle bağlantılı, internet üzerinde çalışan ve "www" ile başlayan adreslerdeki sayfaların görüntülenmesini sağlayan servistir.

5. SORUMLULUK VE YETKİ TANIMLARI

Bölüm/Rol/Unvan/Görev	Sorumluluklar	Yetkiler
Kullanıcılar (İKÜ personeli, sözleşmeli personel, geçici personel ve İKÜ tarafından bilgiye erişim hakkı verilen 3. şahıslar ve İKÜ tarafından bilgiye erişim hakkı verilmiş herkes)	-Kullanıcı şifrelerinin belirlenmiş kurallara göre tanımlanması ve şifre belirleme kurallarına uyulması. -Kullanılan şifrelerin gizliliğinin sağlanması ve hiç kimseyle paylaşılmaması. -Kendilerine iletilen geçici şifrelerin sisteme veya uygulamaya ilk girişte değiştirilmesi. -Şifrelerin kâğıda basılı olarak, elektronik dosyalarda veya cep telefonu gibi el cihazlarında tutulmaması. -Şifrenin güvenliği ile ilgili bir sorun hissedildiğinde şifrenin değiştirilerek konu ile ilgili Bilgi Sistemleri Departmanına haber verilmesi.	Kendi şifrelerini kurallar doğrultusunda belirlemesi.
İKÜ Bilgi sistemleri ve Teknolojileri Daire Başkanlığı	-BSTDB tarafından yönetilen tüm sistemler, sunucular, uygulamalar, servisler ve ağ sistemleri yönetici ve servis şifrelerinin üretilmesi ve korunması.	-Sorumluluğunda olan kullanıcı şifrelerinin oluşturulması ve kullanıcı hesaplarındaki blokelerin kaldırılması.

	-Geçici kullanıcı şifrelerinin belirlenmesi ve kullanıcılara iletilmesi. -Bloke olan veya unutulan şifreleri üzerindeki blokelerin kaldırılması ve geçici şifrelerin tanımlanarak kullanıcılara iletilmesi, kullanıcılara bu tip durumlar için bir platform sunarak kullanıcının da bu işlemleri yapabilmesinin sağlanması. -Üretici firma tarafından tanımlanmış şifrelerin değiştirilmesi.	-Kullanıcılara şifre değiştirmesi veya şifrenin unutulması durumunda bir platform sunarak kullanıcının bu işlemleri yapabilmesinin sağlanması.
Üst Yönetim ve BSTDB	-Şifre yönetim politikalarının belirlenmesi için gerekli olan koordinasyonun sağlanması. -BGYS'de alınan kararlar doğrultusunda uygulanmanın koordinasyonu. -Şifre güvenliği ile ilgili iletilen sorun veya şüphelerin yönetilerek giderilmesi.	Şifre uygulamalarının kontrol (Audit) edilmesi.

6. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR
1	IKU BSTDB BGYS Politikası
2	IKU BSTDB Bilgi Güvenliği Disiplin Politikası
3	IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü

7. ŞİFRE POLİTİKASININ HEDEFLERİ VE PRENSİPLERİ

8.1. Kullanıcı hesaplarına ait şifreler en geç 6 (altı) ayda bir değiştirilir.

8.2. Administrator yetkisine sahip kullanıcılar, kendi yönetimindeki sistemlere erişimde kullandığı Administrator hesabı ile kendi kullanıcı hesapları için farklı şifreler kullanır.

8.3. Şifrelerin e-posta iletilerine veya herhangi bir elektronik forma eklenmesi yasaktır.

8.4. Kullanıcı, yetkilerini ve/veya görevlerini kendi bölümündeki bir arkadaşına devretmek suretiyle izne çıkacağı zaman bile kendisine ait olan şifreyi bir başkası ile paylaşamaz. İzinde iken kendi adına bir başkası tarafından kullanıcı adı ve şifresi girilerek işlem yapılamaz, talep edilemez.

8.5. Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda BGYS Birimi tarafından yapılan farkındalık eğitimleri ve farkındalık e-postaları ile düzenli aralıklarla bilgilendirilir.

8.6. Kurum çalışanı olmayan, sözleşme ile bağlayıcılığı sağlanmış dış firma çalışanları için süreli olarak açılan kullanıcı hesapları da bu yönergenin ilgili maddelerinde belirtilen şifre oluşturma özelliklerine uygun olmak zorundadır.

8.7. Bütün şifreler İKÜ 'ye ait gizli bilgi niteliğindedir. Paylaşılamaz, kâğıtlara ya da elektronik ortamlara yazılamaz.

8.8. Web tarayıcısı ve diğer şifre hatırlatma özelliği olan uygulamalardaki "şifre hatırlama" seçeneği kullanılamaz. Bu durum bilgi güvenliği açısından sakıncalı olup, kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.

8.9. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile güvenlik tatbikatlarında gerçekleştirilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıdan şifresini değiştirmesi talep edilir.

8.10. Kullanıcının yeni şifresini belirlerken daha önce vermiş olduğu son 3 şifreyi yeniden atayamaz. Tekrar aynı şifreyi kullanması durumunda sistem tarafından otomatik olarak engellenir.

8.11. Sisteme yeni ürün kurulumlarında üretici firmaların tanımladığı varsayılan şifreler, sistem ve yazılımların kurulumunu takiben hemen değiştirilir.

8.12. Kullanıcı şifresinin güvenliği ile ilgili bir sorun hissettiğinde, kullanıcı şifresini hemen değiştirilerek konu ile ilgili BSTDB 'ye haber verir. Kullanıcının, şifresini değiştirecek imkânı yoksa, şifre değişimi için BSTDB Destek Birimine hızlıca bilgi vermesi gerekir.

8.13. İş amacıyla ve/veya iş dışı kullanımda aynı şifre/şifreler kullanılamaz.

8.14. Kurumsal bilgiye erişilebilen mobil cihazlar için ekran kilidi kullanımı zorunludur. Ekran kilidini açmak için kolay tahmin edilemeyen PIN kodu, şifre veya desen kullanılır.

8.15. Kurumda kullanılan şifreler; doğum tarihi, kimlik numarası, telefon numaraları gibi kişisel bilgilerden oluşturulamaz.

8.16. Her kullanıcı kendi hesabından ve şifresinden sorumludur.

8. ŞİFRE BELİRLEME KURALLARI

9.1. En az 10(on) karakterli olmalıdır.

9.2. İçerisinde en az 1(bir) tane büyük, en az 1(bir) tane küçük harf, en az 1(bir) alfa numerik ve en az 2(iki) rakam bulunmalıdır. En az 3(üç) tane harf bulunmalıdır.

9.3. Başlangıç karakterleri "qwertyuiopasdfghjkzxcvbnmQWERTYUPASDFGHJKLZXCVBNM0123456789" dışında karakter olamaz.

9.4. Bazı özel karakterlere ("'^/ () =`|~%&#$IIO_, @; \) izin verilmemektedir.

9.5. Aynı karakterler peş peşe kullanılamaz. (aaa, 111, XXX, ababab...).

9.6. Sıralı karakterler kullanılamaz. (abcd, qwert, asdf,1234,zxcvb...).

9.7. Kullanıcı Adı ve Kullanıcı ID 'si şifre olarak kullanılamaz.

9.8. Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş şifreler kullanılmamalıdır.

9. ŞİFRE KULLANIM POLİTİKASININ YAPTIRIMLARI

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla "IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü" ve "IKU BSTDB Bilgi Güvenliği Disiplin Politikası" belgelerinde belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır. Bu belgenin yetersiz kaldığı durumlar üniversite makamlarınca değerlendirilir.

10. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar