1. AMAÇ

Bu politikanın amacı, bilgi güvenliğini sağlamak, yetkisiz erişimleri önlemek ve üniversitenin bilgi varlıklarının korunmasını sağlamaktır.

2. KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında Üniversite bilgi sistemlerine erişim sağlayan tüm cihaz ve kullanıcılarını kapsamaktadır.

3. TANIMLAR VE KISALTMALAR

BGYS: Bilgi Güvenliği Yönetim Sistemi'nin kısaltmasıdır.

Bilgi Güvenliği Yönetim Sistemi: Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, risk yaklaşımına dayalı yönetim sistemidir.

Kimlik Doğrulama: Bildirilen bir kimliğin gerçekten bildiren şahsa ait olduğuna dair güvence sağlayan mekanizma.

Kullanıcı Hesabı: Kullanıcının, kuruluş sistemlerine giriş için kullandığı, tüm işlemlerde kullanıcıyı temsil eden ve kendisine tanımlanan parola ile sisteme girişin mümkün olduğu tekil ve kişiye özel karakterler bütünü.

Parola: Kullanıcının, sistemine kullanıcı adı ile kendisini tanıtmasını ve işlem yaratma ve/veya sonuçlandırmasını sağlayan, sadece kendisinin bildiği ve belirli dönemlerde değiştirilmesi zorunlu kılınan gizli karakterler dizisi.

4. SORUMLULUKLAR

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

Bilgi İşlem Daire Başkanı: Politikanın kontrolü ve uygulanabilirliğinin sağlanmasından sorumludur.

Rektör: Politikanın onaylanması ve yürürlüğe konulmasından sorumludur.

İlgili Personel: Politika içinde belirtilen faaliyetlerin gerçekleştirilmesinden sorumludur.

5. UYGULAMA

a) Üniversite sistemlerine erişecek tüm kullanıcıların hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.

b) Üniversite sistemlerine erişmesi gereken kullanıcılara yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacaktır.

c) Üniversite bünyesinde kullanılan ve merkezi olarak erişilen uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli ve denetim altında tutulmalıdır.

d) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.

e) Kullanıcılar, Üniversite tarafından kullanımlarına tahsis edilen sistemlerin güvenliğinden sorumludur.

f) Sistemlerin başarılı ve başarısız erişim logları düzenli olarak tutulmalıdır.

g) Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.

h) Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve kayıt alınmalıdır.

i) Kullanıcı hatalarını kaydetmek ve takip etmek amacıyla olay ihlal formu açılmaktadır.

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