İÇİNDEKİLER

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

1 Amaç

Bu politikanın amacı, ESOGÜ bünyesinde yer alan bilgi sistemlerinin genel kullanım esaslarının tanımlanmasıdır.

2 Kapsam

ESOGÜ bünyesinde çalışan tüm personel bu politika kapsamındadır.

3 Tanım ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi
BİDB: Eskişehir Osmangazi Üniversitesi Bilgi İşlem Daire Başkanlığı
BGYS: Bilgi Güvenliği Yönetim Sistemi

4 Sorumlular

Bu politikanın oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Politikanın uygulanmasından tüm ESOGÜ personeli sorumludur.

5 Kurallar

5.1 Genel Kurallar

- Kurum bünyesinde oluşturulan tüm veriler Kurum mülkiyetindedir.
- Güvenlik sistemlerinin kontrolü amacıyla yetkili kişiler cihazları, sistemleri ve ağ trafiğini *Güvenlik Açıkları Tespit Etme Prosedürü* çerçevesinde gözlemler.
- BİDB bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
- BİDB'nin bilgisi olmadan Yerel Ağda sunucu (web hosting servisi, e-posta servisi) nitelikli bilgisayar bulundurulamaz.
- Bilgi sistemlerindeki değişiklikler *Değişiklik Yönetim Prosedürü* kapsamında yapılmaktadır.
- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamaktadır, kaynakların paylaşıma açılması halinde bu süreç kontrollü olarak uygulanmakta, PL.04 - ERİŞİM KONTROL VE UZAKTAN BAĞLANTI POLİTİKASI dikkate alınmaktadır.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

- Fikri mülkiyet hakları gereğince kurum içinde kullanılan ve kurulum gerektiren tüm programlar, yazılımlar lisanslıdır. (Açık kaynak kodlu yazılımlar hariçtir)
- Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim yetkileri tanımlanmıştır, PL.04 - ERİŞİM KONTROL VE UZAKTAN BAĞLANTI POLİTİKASI dikkate alınır.
- Tüm parolalar "PL.12 - PAROLA POLİTİKASI "ne uygun şekilde oluşturulmuş ve kullanılmaktadır. Parolalar Başkalarıyla paylaşılmaz.
- Bütün bilgisayar ve benzeri araçlar otomatik olarak en fazla 3 dakika içerisinde parolalı ekran korumasına geçer.
- Kullanıcılar bilinmeyen kaynaklardan gelen dosyaları açarken çok dikkatli olmalıdır. Çünkü bu dosyalar virüs, truva atı gibi zararlı kodları ve kötücül yazılımları içerebilirler.
- Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamakta/kopyalanmamaktadır.
- Bilgisayarlar üzerinde ve kurumsal e-posta kullanımında iş ile ilgili dosyalar, uygulamalar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamaktadır.

5.2 Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler kesinlikle yapılmamalıdır:

- Herhangi bir kişinin veya Kurumun uygulamalarını izinsiz kopyalamak, ticari sır, patent veya diğer şirket bilgileri, yazılım lisanları vs. haklarını çiğnemek.
- Kitapları izinsiz kopyalamak, magazinlerdeki fotoğrafların dijital formata dönüştürmek, lisans ve telif gerektiren yazılımları kopyalamak.
- Zararlı programları (örnek: virus, solucan, truva atı, e-mail bombaları vs) ağa veya sunuculara bulaştırmak.
- Kurum kaynaklarını kullanarak herhangi bir yasadışı aktivitede bulunmak,
- Kişisel hesap şifrelerini başkalarına vermek veya kişisel hesaplarını kullandırtmak.
- Kurum bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmak.
- Ağ güvenliğini etkilemek (örnek: bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (paket spoofing, denial of service vs.).
- BİDB'nin bilgisi dışında port veya ağ taraması yapılmaz.
- Birim yöneticisinin bilgisi dışında gizlilik, bütünlük veya erişilebilirlik değeri yüksek veya daha üstü olan cihaz, yazılım veya bilgiyi izinsiz olarak kurum dışına çıkarılmaz.

5.3 Diğer Bilgi Sistem Aktiviteleri

- Cep telefonu ve Kurum telefonlarıyla iletişimdeyken karşıda konuşulan kişinin o olduğuna dikkat etmek
- Kalabalık ve geniş kitleli ortamlarda telefonla yapılan iletişim esnasında başkaları tarafından duyulmaması gerekli bilgileri konuşmamak
- Mobil cihaz üzerinden kullanılan iletişim uygulamaları (örn: whatsapp, skype, turkcell bip vb) üzerinde paylaşılan bilgiler için de Bilgi Güvenliği Politikalarına uyum sağlamak
- Yazıcı, tarayıcı vb. sistemler üzerinden yapılan her türlü kullanımlarda Bilgi Güvenliği Politikalarına uyum sağlamak.

5.4 Windows İşletim (Domain) Sistemi Sıkılaştırma Tedbirleri

- Kullanıcı hakları en az yetki prensibi göz önünde bulundurularak sadece ihtiyaç duyulan kullanıcı ve gruplara verilmelidir.
- Tüm kullanıcı makinelerinde otomatik güncelleme özelliği aktif hale getirilmelidir.
- Windows işletim sistemlerinde SMB versiyon 1 protokolü yerine daha güvenli ve güncel SMB protokol versiyonları kullanılmalıdır.
- Gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesapları devre dışı bırakılmalıdır. Gerekli kullanıcılar için varsayılan olarak aynı tanımlanan yerel yönetici hesaplarının parolaları değiştirilmelidir.
- Etki alanı yöneticisi (Domain Admin) ve diğer yetkili hesapların (Enterprise Admin, Backup Admin ve Schema Admin) sayısı sınırlandırılmalıdır.
- Yetkili hesapların parola özetlerinin çalınmasının engellenmesi için: Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında gerekli olmadıkça işlem yapılmamalı, işlem yapıldığı durumlarda kullanıcı bilgisayarlarının yeniden başlatılması sağlanmalıdır. Yerel bilgisayarlarda parola özetleri tutulma sayısı 0 yapılmalıdır. Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) grubuna alınmalıdır.
- Aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarını tespit etmek için bir yordam tanımlanmalıdır.
- Sistemlerde yer alan varsayılan yönetici ve misafir hesapları pasif hale getirilmelidir.
- Standart kullanıcıların betik çalıştırma motorlarına (Windows Script Host, Powershell, Command Prompt ve Microsoft HTML Application Host vb.) erişimi engellenmeli veya kısıtlanmalıdır.
- Aktif dizin sorguları LDAP protokolü yerine güvenli LDAPs protokolü ile yapılacak şekilde konfigüre edilmelidir.

- Ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ve oturum açma kapama işlemleri izlenmelidir.
- Yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu konumlandırılmalı, ek yazılım veya rol yüklenmemeli, eposta, internet vb. erişimleri için kullanılmamalıdır.
- Aktif dizinde devre dışı bırakılan kullanıcı hesabı için activesync mail erişimi hemen kesilmelidir.

6 Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi 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 BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

7 İlgili Dokümanlar

PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ
PR.19 - DEĞİŞİKLİK YÖNETİM PROSEDÜRÜ
PR.11 - GÜVENLİK AÇIKLARINI TESPİT ETME PROSEDÜRÜ
PL.04 - ERİŞİM KONTROL VE UZAKTAN BAĞLANTI POLİTİKASI

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI