İÇİNDEKİLER

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	ÖMER TANBERK

1 Amaç

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

2 Kapsam

ESOGÜ BİDB bünyesinde çalışan tüm personel bu politika kapsamındadır.

3 Sorumlular

Bu prosedürün oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Politikanın uygulanmasından tüm ESOGÜ BİDB personeli sorumludur.

4 Kurallar

4.1 Genel Kurallar

- Kurum bünyesinde oluşturulan tüm verilerin Kurum mülkiyetinde olduğu düşünülmelidir.
- Güvenlik sistemlerinin kontrolü amacıyla yetkili kişiler cihazları, sistemleri ve ağ trafiğini *Güvenlik Açıkları Tespit Etme Prosedürü* çerçevesinde gözlemleyebilir.
- Kurum bu prosedür çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
- Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/kopyalanmamalıdır.
- Bilgisayarlar üzerinden iş ile ilgili dosyalar ve uygulamalar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
- İT Yöneticisi bilgisi olmadan Ağ sisteminde sunucu (web hosting servisi, e-posta servisi vb.) nitelikli bilgisayar bulundurulmamalıdır.
- Bilgi sistemlerindeki değişiklikler ancak *Değişiklik Yönetim Prosedürü* kapsamında yapılmalıdır.
- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde bu süreç kontrollü olarak uygulanmalıdır.
- Fikri mülkiyet hakları gereğince kurum içinde kullanılan ve kurulum gerektiren tüm programlar, yazılımlar lisanslı olmalıdır. (Açık kaynak kodlu yazılımlar hariçtir)
- Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim yetkileri tanımlanmalıdır.

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	ÖMER TANBERK

- Parolalar güvenli bir şekilde tutulmalı ve hesaplar başka kimselerle paylaşılmamalıdır.
- Sistem seviyeli şifreler 6 ayda bir kullanıcı seviyeli şifreler ise 2 ayda bir değiştirilmelidir.
- Bütün bilgisayar ve benzeri araçlar otomatik olarak en fazla 3 dakika içerisinde parolalı ekran korumasına geçebilmelidir.
    - Bu noktada mevcut yapı buna izin vermemekle beraber, kullanıcılara bilgilendirme niteliğinde e-posta gönderilmiştir.
- Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar. Çünkü bu mailler virus, e-mail bombaları ve truva atı gibi zararlı kodları ve kötücül yazılımları içerebilirler.
- Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve gerekirse dosyaların sıkıştırılması sağlanmalıdır.
- Mail gönderiminde birbirini görmesi gerekmeyen toplu maillerde TO yerine BCC yapılarak gizli gönderim sağlanmalıdır.

4.2 Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler kesinlikle yasaklanmıştır.

- 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 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 kullandırmak.
- Kurum bilgisayarlarını kullanarak taciz veya yasadışı olaylara karıştırmak.
- Ağ güvenliğini etkilemek (örnek: bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (paket spoofing, denial of service vs.).
- BGYS Yöneticisi ve IT Yöneticisi bilgisi dışında port veya ağ taraması yapmak.
- Kullanıcı kimlik tanıma yöntemlerinden kaçmaya çalışmak.
- Program/script/komut kullanarak kullanıcının bağlantısını etkilemek.

- Kurum bilgilerini, Kişisel Verilerin Korunumu Kanunu çerçevesinde tanımlanmış kişisel verileri Kurum dışından üçüncü şahıslara iletmek.
- BGYS Yöneticisi bilgisi dışında gizlilik, bütünlük veya erişilebilirlik değeri yüksek veya daha üstü olan cihaz, yazılım veya bilginin izinsiz olarak kurum dışına çıkarmak.

4.3 E-mail ve Haberleşme Aktiviteleri

Aşağıdaki aktiviteler hiçbir istisna olmadan kesinlikle yasaklanmıştır.

- Güvenliğinden emin olunmayan bir bilgisayardan web e-posta sistemini kullanmak.
- İstenilmeyen e-posta mesajlarının iletmek (Bunlar karşı tarafın özellikle istemediği reklam mesajlarını içeren e-postalar, spam e-postalar olabilir).
- E-posta veya telefon vasıtası ile taciz etmek.
- E-posta başlık bilgilerini yetkisiz kullanmak veya değiştirmek.
- Zincir e-postaları oluşturmak veya iletmek.
- İş ile alakalı olmayan mesajları birçok haber gruplarına iletmek.

4.4 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 içinde BGYS kriterlerine uyum sağlamak
- Yazıcı, tarayıcı vb. sistemler üzerinden yapılan her türlü kullanımlarda BGYS kriterlerine uyum sağlamak

5 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.

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	ÖMER TANBERK

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.

6 İlgili Dokümanlar

PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ
PR.19 - DEĞİŞİKLİK YÖNETİM PROSEDÜRÜ
PR.11 - GÜVENLİK AÇIKLARINI TESPİT ETME PROSEDÜRÜ

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	ÖMER TANBERK