1 AMAÇ

Bu politikanın amacı, Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde yer alan bilgi sistemlerinin genel kullanım esaslarının tanımlanmasıdır.

2 KAPSAM

Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde çalışan tüm personel bu politika kapsamındadır.

3 SORUMLULAR

Bu prosedürün oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Politikanın uygulanmasından tüm Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı 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.
- Sistem ve Ağ sorumlusunun 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.
- Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim yetkileri tanımlanmalıdır.
- Parolalar güvenli bir şekilde tutulmalı ve hesaplar başka kimselerle paylaşılmamalıdır.
- Sistem seviyeli şifreler en fazla 1 yıl, kullanıcı seviyeli şifreler ise en fazla 6 ayda bir değiştirilmelidir.
- Bütün bilgisayar ve benzeri araçlar otomatik olarak en fazla 3 dakika içerisinde parolalı ekran korumasına geçebilmelidir.

- 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 fotoğrafları 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 Sistem ve Ağ sorumlusu 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 YAPTIRIM

Bu politikanın ihlal edilmesi durumunda Disiplin Prosedürü uygulanacaktır.

6 İLGİLİ DOKÜMANLAR

EYS-PO.021 - DİSİPLİN PROSEDÜRÜ