P01 BİLGİ SİSTEMLERİ GENEL KULLANIM POLİTİKASI

1.1 Genel Bakış

Kurumumuz bilgi paylaşımı ve güvenliği konularında tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmek amacıyla "Bilgi Güvenliği Politikalarını" hazırlamıştır. Bilişim ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir güvenlik bütün çalışanların içerisine dahil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

1.2 Amaç

Bu politikanın amacı kurum bünyesindeki bilişim cihazlarının ve yazılımlarının uygun kullanımı hakkında standart oluşturmaktır. Uygunsuz kullanım kurumu virüs saldırılarına, ağ sistemlerinin çökmesine hizmetlerin aksamasına ve bunların yaptırımlara dönüşmesine sebep olabilir.

1.3 Kapsam

Bu politika kurumun bütün çalışanları, sözleşmelileri, kurum adı altında çalışan bütün kişiler ve aynı zamanda kurumun sahip olduğu ve kiraladığı bütün cihazları kapsamaktadır.

1.4 Politika

Genel Kullanım ve sahip olma ile güvenlik ve kişiye ait bilgiler aşağıdaki gibi açıklanmıştır.

1.4.1 Genel Kullanım ve Sahip Olma

a) Kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da kurumun bünyesinde oluşturulan tüm veriler kurumun mülkiyetindedir.
b) Çalışanlar bilgi sistemlerinden kendi kişisel kullanımı için makul seviyede yararlanabilirler.
c) Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmelidir.
ç) Güvenlik ve ağın bakımı amacı ile yetkili kişiler cihazları, sistemleri ve ağ trafiğini burada tanımlanan politikalar çerçevesinde gözlemleyebilir. Kurum, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
d) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalıdır ve kopyalanmamalıdır.
e) Bilgisayarlar üzerinden işle ilgili belgeler, resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
f) Bilgisayarlara hiçbir surette lisanssız program yüklenmemelidir.
g) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre politikasına göre hareket edilmelidir.

1.4.2 Güvenlik ve Kişiye Ait Bilgiler

a) Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları tanımlanmalıdır.
b) Şifreleri güvenli bir şekilde saklamalı ve hesap bilgileri başka kimselerle paylaşılmamalıdır. Sistem seviyeli şifreleri en az yılda bir kullanıcı seviyeli şifreler ise en az yılda bir değiştirilmelidir.
c) Bütün PC ve Laptoplar otomatik olarak 20 dakika içerisinde şifreli ekran korumasına geçebilmelidir.
ç) Laptop bilgisayarlar güvenlik açıklarına karşı korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır.
d) Laptop bilgisayarın çalınması / kaybolması durumunda, durum fark edildiğinde en kısa zamanda yetkili kişiye haber verilmelidir.
e) Kuruma ait cep telefonu, tablet ve el terminali cihazlarının gerekli güvenlik tedbirlerini almaktan cihaz kullanıcısı sorumludur.
f) Çalışanlar tarafından gönderilen maillerde şöyle bir açıklama olmalıdır.

Türkçe metin:
"Bu e-posta mesajı ve ekinde bulunabilecek dosyalar yalnız mesajın alıcı hanesinde kayıtlı kullanıcı(lar) içindir. Mesajın alıcısı değilseniz, lütfen hemen göndericiyi uyarınız. Mesajı dağıtmayınız, kopyalamayınız, içeriğini açıklamayınız ve çıktı almaksızın siliniz. Bu mesajda kayıtlı görüş ve düşünceler hiçbir şekilde Erzurum Teknik Üniversitesi atfedilemeyeceği gibi, kurumumuz açısından bağlayıcı da değildir. Virüs ve kötü amaçlı yazılımların bu mesajda yerleşmesinin engellenmesi amacıyla gerekli tüm önlemler alınmış olsa da bu mesajın sisteminizde yaratabileceği kayıp ve zararlardan dolayı kurumumuz hukuken sorumluluk kabul etmez. Erzurum Teknik Üniversitesinin alanında dünya çapında yürüttüğü faaliyetlere ilişkin bilgi almak için internet sitemizi (www.erzurum.edu.tr) ziyaret edebilirsiniz. "

g) Çalışanlar bilinmeyen kimselerden gelen dosyaları açmamalıdırlar. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler.
ğ) Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve gerekirse dosyaları sıkıştırılmalıdır.

1.4.3 Uygunsuz Kullanım

Genel olarak aşağıdaki eylemler yasaklanmıştır. Sistem yöneticileri bu kapsamın dışında olabilir. Herhangi bir kullanıcı kurumun kaynaklarını kullanarak hiçbir şart altında herhangi bir yasadışı aktivitede bulunamaz.

1.4.3.1 Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler hiçbir istisna olmadan standartlaştırılmıştır.

a) Herhangi bir kişi veya kurumun izinsiz kopyalama, devlet sırrı, patent veya diğer kurum bilgileri, yazılım lisansları vs. haklarını çiğnemesi,
b) Kitapların izinsiz kopyalanması, magazinlerdeki fotoğrafların dijital formata dönüştürülmesi, lisans gerektiren yazılımların kopyalanması,
c) Zararlı programların ağa veya sunuculara bulaştırılması,
ç) Kendi hesabınızın şifresini başkalarına vermek veya kendi hesabınızı kullandırması,
d) Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışması,
e) Ağ güvenliğini etkilemek, ağ haberleşmesini bozması,
f) Kullanıcı kimlik tanıma yöntemlerinden kaçması,
g) Program/script/komut kullanarak kullanıcının bağlantısını etkilemesi,
ğ) Kurum bilgilerini kurum dışından üçüncü şahıslara iletmesi,
h) Kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programları kurmak ve kullanmak yasaktır.

1.4.3.2 E-mail ve Haberleşme Aktiviteleri

a) Kurum dışından web posta sistemini güvenliğinden emin olunmayan bir bilgisayardan kullanması,
b) İstenilmeyen e-posta mesajlarının iletilmesi. (Bunlar karşı tarafın özellikle istemediği reklam mesajlarını içeren mailler olabilir),
c) E-posta veya telefon vasıtası ile taciz etmesi,
ç) E-posta başlık bilgilerini yetkisiz kullanması veya değiştirmesi,
d) Zincir e-postaları oluşturması veya iletmesi,
e) Yetkili kişilerin izni olmadan haber gruplarına iletmesi yasaktır.