**STEP MEDİA REKLAM ve PAZARLAMA DANIŞMANLIĞI**

**PERSONEL BİLGİ GÜVENLİK POLİTİKASI**

1. **Bilgi Sistemlerinin Genel Kullanımı**
   1. Bütün PC ve laptoplar beklemedeyken otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçmelidir.
   2. Laptop bilgisayarın çalınması veya kaybolması durumunda en kısa zamanda Bilgi İşlem bölümüne haber verilmelidir.
   3. Kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek kuruma veya kişiye yönelik saldırılarda (örnek, elektronik bankacılık vs.) sistemin kullanıcısı sorumludur.
   4. Ağ güvenliğini (örnek, bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozan (paket sniffing, paket spoofing, denial of service vs.) veya ortadan kaldıran eylemlere girişilmemelidir.
   5. Şirket bilgileri kurum dışındaki üçüncü şahıslara iletilmemelidir.
   6. Kullanıcıların bilgisayarları üzerine Bilgi İşlem bölümünün onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
   7. Cihaz, yazılım ve veri izinsiz olarak şirket dışına çıkarılmamalıdır.
   8. Kullanıcılar şirketin kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları kurmamalı ve kullanmamalıdır.
   9. Bilgisayarlar üzerinde oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır. Bilgi işlem personeli dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımlar vb. üzerinde mevcut yapılan düzenlemeleri hiçbir şekilde değiştirilmemelidir.
   10. Bilgisayarlara herhangi bir şekilde lisanssız yazılım yüklenmemelidir.
2. **E-POSTA KULLANIMI**
   1. E-posta göndermeden önce alıcının kimliği ve bu mesajı almaya yetkili olup olmadığı dikkatle kontrol edildikten sonra gönderim yapılmalıdır.
   2. E-postası değişen ve işten ayrıldığı anlaşılan kullanıcıların adresleri derhal güncellenmeli ve düzeltilmelidir.
   3. Toplu e-posta gönderimi konusunda KVKK ve Elektronik Ticaret Kanunu ve mevzuatı hükümlerine uygun hareket edilmelidir.
   4. Birden fazla kişiye mail gönderilmesi durumunda, bunların adres listeleri özenle kontrol edilmeli ve güncellenmelidir.
   5. Kurumun e-posta sistemi taciz, suiistimal veya herhangi bir şekilde kanunlara aykırı öğeler içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
   6. Toplu e-posta yolu ile Kurum çalışanlarına veya üçüncü şahıslara yönelik siyasi, din, ırk, cinsiyet, politik içerik taşıyan mesajlar gönderilmesi kesinlikle yasaktır.
   7. E-posta gönderilirken “CC” kullanımına özen gösterilmelidir. İşin görülmesi sürecinde bireysel düzeyde, şahsi diyalog ile halledilmesi gereken konulara Kurumun üst düzey yöneticileri ile ilgisiz birimler “CC” yapılarak karıştırılmamalı, bireysel ihtilafların içine çekilmemelidir. Aynı şekilde konu ile doğrudan ilgili kişiler “CC” kapsamı dışında bırakılmamalıdır.
   8. Kişiler ile ilgili soruşturmaların yürütülmesi, savunma istenmesi gibi konuların gizlilik içinde yapılması esas olup, bu konuların e-posta veya “CC”, “BCC” yolu ile yayılması yasaktır.
   9. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-posta alındığında hemen silinmeli ve başkalarına iletilmemelidir.
   10. Kişisel kullanım için internetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
   11. Spam, zincir e-posta, sahte e-posta ve benzeri e-postalara yanıt yazılmamalıdır.
   12. Kullanıcıların kullanıcı kodu ve şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak herhangi bir işlem yapılmaksızın silinmelidir.
   13. Çalışanlar, e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb.) gönderemezler.
   14. Çalışanlar, kurumsal e-postaları kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.
   15. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar açılmamalı ve silinmelidir. Çünkü bu mailler virüs, e-mail bombaları ve truva atı gibi zararlı kodları içerebilirler.
   16. Şirket dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.
   17. Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak sorunlardan sorumludurlar.
   18. Kullanıcıların Şirket e-postalarını iş amaçlı olarak kullanmaları esastır. Buna göre özel amaçlı olarak e-posta kullanılamaz. Özel yazışmaların özel e-posta adreslerinden yapılması gerekir.
   19. E-postaların Şirketin denetim ve gözetimine tabi olup, Çalışan bu konuda bilgilendirilmiş ve aydınlatılmıştır.
3. **İNTERNET KULLANIMI**
   1. Kullanıcılara, görevleri çerçevesinde internet erişim olanağı sağnabilir. işveren güvenlik nedeniyle bazı sitelere erişimi yasaklayabilir, ya da kısıtlayabilir.
   2. Kullanıcılar, peer-to-peer bağlantı yoluyla internetteki servisleri kullanmamalıdır.
   3. Kullanıcılar internet üzerinden Multimedia Streaming (online video izlemek ve müzik dinlemek) yapmamalıdır.
   4. İş ile ilgili olmayan müzik, video dosyaları gönderilmemeli veya indirilmemelidir.
   5. İnternet üzerinde şirket Bilgi İşlem bölümü tarafından onaylanmamış yazılımlar indirilmemeli ve şirket sistemleri üzerine bu yazılımlar kurulmamalıdır.
   6. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerin girilmemelidir.
   7. Üçüncü şahısların kurum içerisinden interneti kullanmaları Bilgi İşlem sorumlusunun izni ve bu konudaki kurallar dahilinde gerçekleştirilecektir.
   8. Şirket, iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir.
4. **ŞİFRE KULLANIMI**
   1. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
   2. Şifreler başkalarıyla paylaşılmamalı, kağıtlara yada elektronik ortamlara yazılmamalıdır.
   3. Şifrelemede, küçük ve büyük karakterlere (örnek, a-z, A-Z) hem dijit hem de noktalama karakterleri ve ayrıca harflere (örnek 0-9, !, $, #, %) sahip olmalıdır.
   4. En az altı karaktere, en az bir sayısal ve alfabetik karaktere sahip olmalıdır.
   5. Herhangi bir dildeki sözlük anlamı olan kelime olmamalıdır.
   6. Ailedeki bireylerin isimleri, doğum tarihleri, telefon numaraları gibi şahsi bilgileri içermemelidir.
   7. Herhangi bir kişiye telefonda şifre verilmemelidir.
   8. Şifreler aile bireyleriyle ve arkadaşlarla paylaşılmamalıdır.
   9. Şifreler işten uzak olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.
5. **ANTİ-VİRÜS** 
   1. Bütün bilgisayarlarda şirketin lisanslı anti virüs yazılımı yüklü olmalıdır ve otomatik olarak güncellenmelidir. Aksi durumlarda Bilgi İşlem sorumlusuna bilgi verilmelidir.
   2. Kullanıcılar herhangi bir sebepten dolayı anti virüs programını sistemden kaldıramaz.
   3. Kullanıcılar bilgisayarlarına harici olarak USB bellek, harici disk, memory stick gibi veri depolama aygıtlarını takmaları yasaktır.
   4. Zararlı programları şirket bünyesinde oluşturmak ve dağıtmak yasaktır.
6. **YAPTIRIMLAR**
   1. Bilgi güvenlik politikasına aykırılık durumunda, İşveren ihlalin ağırlığına göre iş sözleşmesinin haklı nedenle tazminatsız olarak feshi de dahil olmak üzere, disiplin cezası uygulama yetkisine sahiptir.
   2. İşverenin, Bilgi güvenliği ihlalleri nedeniyle ortaya çıkan zararı çalışana rücu hakkı saklıdır.