E-POSTA KULLANIMI; Kuruluşumuzda e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.

Mesajların, gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilir

İş ile ilgili olmayan sosyal mesajlar içeren zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında, hemen silinir ve kesinlikle başkalarına iletilmez.

Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmaz.

Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikrim mülkiyeti içeren malzeme vb.) gönderemez.

ERİŞİM POLİTİKASI; Kuruluşumuzda Tüm çalışanların aynı yöntemle oluşturulmuş kullanıcı isimleri bulunmakla birlikte, kurum ağ ve sistemlerine giriş izni veren parolaların gizli tutulur.

Geçici çalışanlara veya tedarikçilere geçici olarak verilmiş olan kullanıcı isimlerinin bir son kullanma tarihi olmakla birlikte, örn: 30 gün. İlgili kayıtlar kullanım bitiş tarihinden itibaren iki hafta süre ile saklanır

Bir çalışanın işten ayrılması durumu ortaya çıkar çıkmaz, tüm ayrıcalıkları ve yetkileri kapatılır.

Organizasyonda hangi kullanıcıların hangi kullanıcı isimlerini hangi sistemlerde kullanmakta olduklarına yönelik listeler bulunur.

Kullanıcılar sistemi kullanarak parolalarını başkalarına iletemez.

Parolasını unutan veya diğer kişilere söyleyen kullanıcılar yeni şifre oluşturur.

Tüm bilgisayar kullanıcıları, kurumun networküne bağlanmadan önce kurum tarafından onaylı bir Anti-virüs programı tarafından taratılır.

AĞ GÜVENLİĞİ ERİŞİM POLİTİKASI; Kuruluş içi ağlar, organizasyonun güvenli bölgelerine göre bölünür.

İnternet erişimi olan server'lar, firewall ile korunur.

Kuruluşumuz ağına bağlı bir iş istasyonundan, güvenlik alt yapısını devre dışı bırakarak internete bağlanmak yasaktır.

Bir sistem yöneticisine uzaktan bağlanabilmek için tek bir kullanım parolası gerekir.

Uzaktan bağlantı kurmuş kullanıcıları onaylamanın bir yolu da internet kullanımı yoluyladır.

Diagnostic Portlara erişebilmek için onay gereklidir.

ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI; Kurum dışından gelen bakım ve tamir çalışanları, diğer tedarikçilerde de olduğu gibi kurum içinde olduğu süre boyunca bir gizlilik anlaşması imzalamalıdır.

Tedarikçilerin finansal durumu senelik olarak gözden geçirilmelidir. Bazı sektörlerde iflas, batak, dolandırıcılık gibi olaylar çok sık gerçekleşmektedir.

Kuruluş içinde kullanılan telefon rehberleri, üçüncü tarafların eline geçmemelidir. Üçüncü taraflar, kendi kuruluşlarına transfer olabilecek çalışanlarımızı görmemelidir.

Sadece uygun yetkileri almış olan çalışanların, organizasyonun bilgi veya iletişim sistemlerine erişimi vardır.

Üçüncü taraflarla herhangi bilgi alışverişi yapılmadan önce bir gizlilik anlaşması yapılmalıdır.

Üçüncü taraflara kurumun Network 'üne erişim izni verilmeden önce, bilgisayarlarını güvenliğe almaları gerekir. Kuruluş, üçüncü taraflara herhangi bir uyarıda bulunmadan ağa olan erişimlerini kesebilir.

Anlaşma sona erdiğinde, tarafların elde ettiği dokümanları geri vermesi gerekir.

İNTERNET ERİŞİM POLİTİKASI; Kuruluşumuzda, bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkar.

Kuruluşumuz ihtiyacı doğrultusunda, içerik filtreleme sistemleri kullanılır.

İstenilmeyen siteler (kumar, şiddet vs.) yasaklanmıştır.

Kuruluşumuzda bilgi sistemlerinde oluşabilecek hatalar yâda doğal afetler karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için sistem ve kurumsal verileri düzenli olarak yedeklenir.

Veriler offline ortamlarda en az kanunlarda belirtilen yasal süreler boyunca saklanır.

ŞİFRE GÜVENLİĞİ POLİTİKASI; Kuruluşumuzda her sistem için mümkün olduğunca farklı şifreler kullanılır

Şifreler, e-posta iletilerine veya herhangi bir elektronik forma eklenmez.

Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması açık bir şekilde masalara, monitörüstlerine konulmaması konusunda bilinçlendirilir.

TAŞINABİLİR CİHAZ POLİTİKASI; Kuruluşa ait bilgi içeren taşınabilir cihazlar, ilgili kişiye zimmetlenerek teslim edilir.

Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur. Mobil cihazlara açılış veya ekran şifreleri koyulması gerekmektedir.

Kuruluşa ait cep telefonu hatları için standart fatura istenir. Detay Dökümlü Fatura hangi yöntemle olursa olsun (Kâğıt, Web Paneli, Taşınabilir Materyal vb.) sadece Genel Müdür onayı ile incelenebilir

Kuruluşa ait bilgisayar, taşınabilir bellek ve PDA cihazlara dışarıdan herhangi bir yazılım, siyasi propaganda, ırkçılık, şiddet, pornografi veya erotizm içeren resim, film veya müzik kopyalanamaz ve cihaz içerisinde bulundurulamaz.

Bilgisayarlar ve PDA cihazlar üzerindeki anti-virüs programları hiçbir nedenle devredışı bırakılamaz.

Taşınabilir bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar mutlaka ağ üzerinde ilgili adrese kaydedilmelidir.

İletişim: Bilgi Güvenliği ile ilgili Dilek, İstek ve Şikayetlerinizi **0342 337 18 36 numaralı telefon numarasına ve etik@sirmacarpet.com e-mail** adresine bildirebilirsiniz.

YÖNETİM KURULU BAŞKANI

HANİFİ ŞİRECİ