ÇAĞDAŞ İŞİTME CİHAZLARI	**VERİ GÜVENLİĞİ**	Düzenleme Tarihi	:	18.01.2022
			:	
			:	

ÇAĞDAŞ İŞİTME CİHAZLARI VERİ GÜVENLİĞİ İLE İLGİLİ YAPILMASI GEREKENLER

- Ağınızın güvenliği için internete bağlanacak cihazlar belirlenmeli ve belirlenen bu cihazlar dışında interneti kablolu yada kablosuz kullanmak isteyen yabancı cihazlar(3. Şahıslar) mac filtrelemesi ile engellenmelidir. (internete yalnızca belirlenen cihazlar çıkabilmelidir.)
- İnternet üzerinden gelebilecek tehlikelere karşı kullanıcı güvenlik duvarlarının ips/ids ayarları aktif edilmelidir.
- İnternete erişim loglarının 5651 kanununa uygun şekilde tutularak 2 yıl süreyle kayıt altına alınması gerekmektedir.
- İnternet üzerinden genel ahlak kurallarına aykırı (şiddet, uyuşturucu vb.) ve kişisel veriler açısından tehdit teşkil eden internet sitelerine erişimler şirket ağ geçidinden engellenerek yasaklanmalıdır.
- Kullanıcıların admin yetkisinden arındırılarak bilgisayarlar üzerinde mecbur kalınmadığı sürece (kullanılan programların tam yetki istemesi gibi durumlar dışında) tam yetki sahibi olmaması, user olarak erişim yetkilerinin kısıtlanması gerekmektedir.
- Formatlama ile veri kaybı yaşanması ihtimaline karşı bilgisayarların biosları şifrelenmeli ve boot aygıtları kapatılmalıdır. Formatlama işlemi kontrollü olarak yetkili kişi tarafından yapılmalıdır.
- Bilgisayarların çökme ihtimaline karşı veri kaybı yaşanmaması adına bilgisayarda depolanan kişisel veriler (örn; randevu bilgileri) düzenli olarak yedeklenmelidir. (otomatik yedekleme kurulması tavsiye edilir.)
- Kullanıcı bilgisayarlarında zararlı yazılımlara karşı antivirüs programı eksiksiz kurulu olmalı, güncel tutulmalı ve kullanıcıların antivirüs programını kaldırma yada durdurması engellenmelidir.

- Kullanıcıların yetkilendirildikleri alanlara(bilgisayara, eposta hesabına vb.) erişimleri her kullanıcıya özel kullanıcı adı ve şifre ile yapılmalı, şifreler en az 8 karakter uzunluğunda karmaşık kombinasyon yapısına(büyük/küçük harf, rakam ve sembol içeren yapı) sahip olmalıdır. Şifre girişlerinde kaba kuvvet algoritması(BFA) gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısını sınırlandıran algoritma kullanılmalı, şifrelerin en az 6 ayda bir olmak üzere düzenli aralıklarla değiştirilmesi sağlanmalıdır.
- Kullanıcıların ağ üzerinde paylaşım yetkileri kısıtlanmalı, kontrolsüz şekilde dosya yada herhangi bir veri paylaşımı yapılmasına müsaade edilmemelidir.
- Sistemden dışarıya veri aktarılması sınırlandırılmalıdır. (USB, CD/DVD v.s.)
- Sistemde süresi geçmiş veya eski sürüm(yayıncısı tarafından desteği bitmiş) yazılım ve servislerin potansiyel güvenlik açığı oluşturmalarından dolayı kullanılmaması ya da güncel versiyonlarına yükseltilmesi, atıl olan veya kullanılmayan yazılım ve servislerin ise silinmesi gerekmektedir. (Örn; Windows 7, Office 2007, Office 2010)
- Sistemde yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilerek olası güvenlik açıklarının kapatılması için yama yönetimi ve yazılım güncelleme denetimi yapılmalıdır.
- Sistemde dijital yada kağıt her türlü veri aktarımlarında, aktarılacak belgede karşı tarafın görmemesi gereken kısımlar var ise, bu alanlar maskelenerek yalnızca ihtiyaç duyulan verilerin gönderilmesi sağlanmalıdır.(veri maskeleme),
- Firma ile ilişkisi kesilen çalışanların zaman kaybetmeden hesaplarının silinerek yetkilerinin kaldırılması ve erişimlerinin sınırlandırılması gerekmektedir. İşten ayrılma sonrasında internet gibi ortak kullanım şifreleri değiştirilmelidir.
- Arızalandığı ya da bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazların harddiskleri veya veri içeren ortamları sökülerek sadece arızalı parçaların gönderilmesi sağlanmalıdır.
- Mail hizmeti olarak yaygın şekilde kullanılan gmail, hotmail, onedrive, googledrive, azure, office3665 vb. hizmetlerininKvkk'nın 9. Maddesine uygun olmaması sebebiyle tercih edilmemesi, kullanılıyorsa yurtiçine taşınması gerekmektedir.
- Taşınabilir cihazlar varsa(örn; dizüstü bilgisayar) BIOS'u şifrelenmeli ve boot aygıtları engellenmelidir. Antivirüs yazılımı ve firewall ile şirket içi kurallar taşınabilir cihazlar için özel olarak oluşturulmalı ve network dışında da aktif edilmelidir.

- Çalınma durumlarına karşı taşınabilir cihazların bellekleri şifrelenerek anahtar güvenliği sağlanmalıdır.
- Ağ cihazlarının (örn; modem, switch vb.) fiziksel güvenliğinin sağlanabilmesi için yalnızca yetkili kişinin erişebileceği şekilde kilitli dolap yada odada muhafaza edilmesi gerekmektedir.
- Bilgisayarlara fiziksel olarak yetkisiz erişimlerin engellenmesi için mutlaka oturum açma şifresi ile şifrelenmesi, ekranı açık şekilde bırakılmaması, ekrandan ayrılma durumu halinde Windows Tuşu + L tuşu ile ekranın kilitlenmesi, ekranda işlem yapılmaması halinde ise otomatik olarak kararma ve kilitleme özelliklerinin aktif edilmesi gerekmektedir.
- Cihazların(bilgisayarların, modemin vb.) bulunduğu alanlara yetkisiz giriş çıkışlar engellenmeli, cihazlara erişimler takip edilmelidir.