**C.34.2.** Sosyal medya hesaplarına gönderilen mesajlar, kuruma ait bilgiler sözlü ya da yazılı olarak hiçbir platformda kullanılmamalıdır.
**C.34.3.** Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcılar, hesapların şifrelerini kurum içi şifrelendirme sisteminden farklı düzenlemelidir.
**C.34.4.** Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcılar, hesapların şifrelerini kimseyle paylaşmamalıdır.
**C.34.5.** Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcılar, şifreleri belirli aralıklarla güncellemeli ve şifrelerin en az 8 karakterden oluşmasına dikkat etmelidir.
**C.34.6.** İnternet sitesi (web) Basın Yayın ve Halkla İlişkiler Müdürlüğü sorumluluğunda olmakla birlikte, Bilgi İşlem Müdürlüğü tarafından görevlendirilecek 1 (bir) personel de teknik destek vermelidir.
**C.34.7.** Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcıların, bilgisayarlarını kullanmadıkları zamanlarda kapatmaları veya kilitlemeleri gerekmektedir.
**C.34.8.** Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcılar, içerik paylaşılmadan önce Basın Yayın ve Halkla İlişkiler Müdüründen onay almalıdırlar.
**C.34.9.** Sosyal medya hesaplarında ve internet sitesinde (web) paylaşılması istenen tüm verilerin ilgili müdürlükler tarafından en az 1 (bir) gün önce Basın Yayın Halkla İlişkiler Müdürlüğü'ne yazıyla bildirilmelidir.

## D. KISALTMALAR

T.C. : Türkiye Cumhuriyeti

BG: Bilgi Güvenliği

BGYS: Bilgi Güvenliği Yönetim Sistemi

BT: Bilgi Teknolojileri

BSI: British Standarts Institute, İngiliz Standartları Enstitüsü

ÇKYS: Çekirdek Kaynak Yönetimi Sistemi

DTVT: Devlet Teşkilatı Veri Tabanı

IEC: International Electrotechnical Commission, Uluslararası Elektroteknik Komisyonu

ISO: International Organization for Standardization, Uluslararası Standartlar Teşkilâtı

Coso Modeli

## E. SÖZLÜK

Açılır Pencere Engelleyicisi (Popup Blocker): Açılır Pencere Engelleyicisi, istenmeyen çoğu açılan pencerenin görüntülenmesini engeller.

ADSL: Asimetrik Sayısal Abone Hattı anlamına gelen hızlı internet erişim teknolojisidir.

Ağ (Network): Ağ birbirine kablolarla veya kablosuz bağlanmış sunucu, yazıcı, bilgisayar, modem gibi birçok haberleşme cihazlarının en ekonomik ve verimli yoldan kullanılmasıdır.

Aldatmaca e-posta (Hoax): Elektronik posta adresi toplamak veya markaları karalamak için oluşturulan yalan haber (asparagas) içeren e-postalardır.

Anti virüs (Virüsten Korunma ): Bilgisayarınızı ya da sisteminizi bilgisayar virüslerinden korumaya ve bilgisayar virüslerini temizlemeye yarayan yazılımdır.

Bağlantı Noktası (Port): Bir elektronik devreye, şebekeye veya sisteme giriş ve bağlantı noktasıdır.

Bilgisayar Korsanı (Hacker): Bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren ve onları kullanabilen kişidir. Amaçlarına göre farklı adlandırılırlar:

Siyah Şapkalılar: Her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabilen bu en bilindik hackerlar, sistemleri kullanılmaz hale getirir veya gizli bilgileri çalar. En zararlı hackerlar siyah şapkalılardır.
Beyaz Şapkalılar: Beyaz şapkalılar da her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabiliyor ancak kırdığı sistemin açıklarını sistem yöneticisine bildirerek, o açıkların kapatılması ve zararlı kişilerden korunmasını sağlıyorlar.

Bilgisayar Solucanı (Computer Worm): Bilgisayar solucanı kendi kendini çoğaltabilen ve kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmış kötücül (malware) yazılımdır. Bilgisayar virüsünden farkı bunu otomatik olarak yapmasıdır.

Bilgisayar Virüsü (Computer Virus): Veri girişi yoluyla bilgisayarlara yüklenen, sistemin veya programların bozulmasına, veri kaybına veya olağandışı çalışmasına neden olan yazılım.

Bilişim (Informatics): İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi.

Bilmesi Gereken Prensibi (Need to Know Principle): Gizlilik dereceli bir ilgiyi, belgeyi, projeyi veya malzemeyi ancak görevi gereği öğrenme ve kullanma sorumluluğu olma ve uygun gizlilik dereceli Şahıs Güvenlik Derecesine sahip olma durumudur.

BIOS (Basic Input/Output System): Temel Giriş/Çıkış Sistemi, bilgisayarın ilk açılma işlevini yerine getiren yazılımdır.

Casus Yazılım (Spyware): Casus yazılım, en başta gelen bir kötücül yazılım (malware) türüdür. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır.

Disk Biçimlendirme (Disc Partitions): Diskinizi biçimlendirmek demek diskinizi farklı mantıksal disk bölümlerine ayırmak anlamına gelir.

EFS: Veri Şifreleme Sistemi anlamına gelen bir bilgisayar terimi kısaltmasıdır.

Ekran Koruyucusu (Screen Saver): Bilgisayarda monitörün uzun süre kullanılmadan açık kalması durumunda devreye giren, monitörün ömrünün azalmasını ve parola ile korunduğunda yetkisiz erişimi engelleyen yazılımdır.

Elektronik Sertifika (Electronic Certificate): Elektronik Sertifika, yani elektronik kimlik, sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisini taşıyan ve taşıdığı açık anahtar bilgisinin, belirtilen kişi veya kuruma ait olduğunu garanti eden belgedir. Elektronik kimlik belgesi kişilere ait olabildiği gibi kurumlara veya web sunucularına ait olabilir.

Exe: Çalıştırılabilir dosya tiplerinin dosya uzantısıdır.

FTP: Dosya aktarım iletişim kuralı, (File Transfer Protocol; FTP), bir dosyayı ağ üzerindeki başka kullanıcıya o ağdaki bilgisayarda geçerli bir kullanıcı ismi ve şifresi ile yollamak için kullanılmaktadır.

Güvenlik Duvarı (Firewall): Güvenlik duvarı kurulduğu sisteme gelen ve giden ağ trafiğini kontrol ederek yetkisiz veya istenmeyen yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır.

Hata (Bug): Bir yazılım ya da donanımda var olan, meydana gelen hata, kod hatasıdır.

Hizmet Paketi (Service Pack): Piyasaya sürülen bilgisayar yazılımlarının, ortaya çıkan hata ve

açıklıklarını giderecek, varsa yeni özelliklerini ortaya çıkaracak yama tabir edilen programcıkların tek bir paket halinde toplandığı yazılımdır.

HDD: Sabit disk ya da Hard disk kısaca HDD ya da Türkçesi ile sabit disk sürücüsü veri depolanması amacı ile kullanılan manyetik kayıt ortamlarıdır. Önceleri büyük boyutları ve yüksek fiyatları nedeni ile sadece bilgisayar merkezlerinde kullanılan sabit diskler, cep telefonları ve sayısal fotoğraf makineleri içine sığabilecek kadar küçülen boyutları ile günlük hayatımıza girmişlerdir. Sabit disklerin en yoğun kullanım yeri bilgisayarlardır. Ses, görüntü, yazılımlar, veri tabanları gibi büyük miktarlarda bilgi, gerektiğinde kullanılmak üzere sabit disklerde saklanır.

HTTP : HTTP (Hypertext Transfer Protocol, Türkçe Hipermetin Aktarma İletişim Kuralı) bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiper ortam bilgi sistemleri için uygulama seviyesinde bir iletişim kuralıdır.

HTTPs : HTTPS (Secure Hypertext Transfer Protocol, güvenli hipermetin aktarım iletişim kuralı) hipermetin aktarım iletişim kuralının (HTTP) güvenli ağ protokolü ile birleştirilmiş olanıdır. Klasik HTTP protokolüne SSL protokolünün eklenmesi ile elde edilir.

ICMP: Internet Kontrol Mesaj İletişim Kuralı, ICMP(Internet Control Message Protocol), hata mesajları ve TCP/IP yazılımının bir takım kendi mesaj trafiği amaçları için kullanılır. Kontrol amaçlı bir protokoldür.

IEEE: (Institute of Electrical and Electronics Engineers, Elektrik ve Elektronik Mühendisleri Enstitüsü) elektrik, elektronik, bilgisayar, otomasyon, telekomünikasyon ve diğer birçok alanda, mühendislik teori ve uygulamalarının gelişimi için çalışan, kar amacı olmayan, dünyanın önde gelen teknik organizasyonudur.

IEEE 802.1x: Bağlantı noktası tabanlı ağ erişim kontrolü için bir IEEE standartıdır. Bu, ağ protokolleri IEEE 802.1 grubunun bir parçasıdır. Bir LAN veya WLAN eklemek isteyen cihazlara kimlik doğrulama mekanizmasını sağlar.

İç Ağ (Intranet): Kuruluşların, kurumun veya herhangi bir grubun, bilgisayarları arasında güvenli bir şekilde bilgi paylaşması için oluşturulmuş büyük çaplı yerel ağ yapısıdır.

IP adresi: IP (Internet Protokol) adresi, interneti protokolünü kullanan diğer ağlara bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adrestir.

İstenmeyen e-posta (Spam): Talep edilmeyen veya istenmeyen e-posta mesajıdır.

İşletim Sistemi (Operating System): İşletim sistemi, bilgisayar donanımının doğrudan denetimi ve yönetiminden, temel sistem işlemlerinden ve uygulama yazılımlarını çalıştırmaktan sorumlu olan sistem yazılımıdır.

Kırılmış (Crack): Ücretli yazılımları ücretsiz kullanmayı sağlayan, program kırıcıları (cracker) tarafından yazılmış programcıkları ve korsan yazılımları ifade eder.

Kriptoloji: Şifre bilimidir. Çeşitli iletilerin, yazıların belli bir sisteme göre şifrelenmesi, bu mesajların güvenlikli bir ortamda alıcıya iletilmesi ve iletilmiş mesajın deşifresiyle uğraşır. Kriptoloji=Kriptografi + Kriptoanaliz Kriptoloji bilmi kendi içerisinde iki farklı branşa ayrılır. Kriptografi ; şifreleri yazmak ve Kriptoanaliz ;şifreleri çözmek ya da analiz etmekle ilgilenir.

Kriptografi: Gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi -dolayısıyla bilgi ile beraber bilginin göndericisi ve alıcısını da- koruma amacı güderler. Bir başka deyişle kriptografi, okunabilir durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan tekniklerin tümü olarak da gösterilir.

Korsan (Warez): Telif yasaları çiğnenerek ticareti yapılan telif hakkı saklı materyallere denir. Telifli ürünlerin kopyalanmasını, çoğaltılmasını ve dağıtımını yapan kişilere korsan, yapılan işe korsancılık denmektedir.

Kötücül Yazılım (Malware): Kötücül yazılım (malware: İngilizce "malicious software"in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır.

Linux: Unix'e fikirsel ve teknik anlamda atıfta bulunarak geliştirilmiş; açık kaynak kodlu, özgür ve ücretsiz bir işletim sistemi çekirdeğidir. Çekirdeğin kaynak kodları GNU Genel Kamu Lisansı çerçevesinde özgürce dağıtılabilir, değiştirilebilir ve kullanılabilir. Linux'un Unix ile herhangi bir kod ortaklığı bulunmamaktadır yani Linux'un kodları sıfırdan başlanılarak yazılmıştır.

MAC Adresi: MAC adresi (Media Access Control, yani Ortam Erişim Yönetimi) bir cihazın ağ donanımını tanımaya yarar, bir anlamda fiziksel adresidir.

Modem: Bilgisayarınızın telefon ya da internet hattına bağlanarak diğer bilgisayarla bağlantı kurmasına yarayan cihazdır.

NTFS: (New Technology File System; Yeni Teknoloji Dosya Sistemi), Windows NT'nin standart dosya sistemidir ve Windows 2000, Windows XP, Windows Server 2003 ve Windows Vista'da da standart olarak kullanılmıştır. Microsoft'un önceki FAT dosya sisteminin yeniden yapılandırılmasıyla oluşmuştur.

Olay Kayıtları (Event Logs): Bir işletim sisteminin tuttuğu kayıtları ifade eder. Olay günlüğü kayıtları, sorunları incelerken ve çözerken size önemli bilgiler sağlar.

Oltalama (Phishing): Yasal bir e-posta gibi görünen ve kişisel bilgilerinizi talep eden bir e-posta mesajıdır. İkna yöntemiyle gizli bilgilerin elde edilmesini amaçlayan bir sosyal mühendislik metodudur.

Otomatik Çalıştır (Autorun): Autorun, taşınabilir disklerin bilgisayara takıldığında istenilen programı veya programları otomatik olarak çalıştırması için kullanılan bir uygulamadır.

Paylaştırılmış Klasör (Shared Folder): Paylaştırılmış klasörler başkasının erişimine izin verdiğiniz ve çoğu zaman dosya paylaşmak amacıyla kullandığımız klasörlerdir.

Privilege: Ayrıcalık, imtiyaz, özel hak.

Rar: Bir dosya sıkıştırma ve arşivleme formatıdır. Eugene Roshal tarafından oluşturulmuş ve oluşturucusunun soyadını almıştır. RAR uzantılı dosyalar .rar şeklinde gözükür.

Robot (Bot): Bot, bilişim dünyasında "robot" anlamında kullanılan yaygın bir terimdir.
Pek çok bilgisayar işlemini yarı-otomatik olarak yapabilen robotlar anlamında kullanılır.

TCP/IP: İnternet protokol takımı, İnternet'in çalışmasını sağlayan bir iletişim protokolleri bütünüdür. Bazen TCP/IP protokol takımı olarak da adlandırılır. TCP (Transmission Control Protocol ) ve IP (Internet Protocol) ün kısaltmalarıdır.

Truva Atı (Trojan): Bilgisayar yazılımı bağlamında Truva atı zararlı program barındıran veya yükleyen programdır. Terim klasik Truva Atı mitinden türemiştir. Truva atları masum kullanıcıya kullanışlı veya ilginç programlar gibi görünebilir ancak çalıştırıldıklarında zararlıdırlar.

Tuş Kaydedici (Keylogger): Bilgisayarda yazılanları siz farkında olmadan kaydedebilen yazılım veya donanımlardır.

Sabit disk (Hard Disk): Sabit Disk ya da Hard disk kısaca HDD, veri depolanması amacı ile kullanılan manyetik kayıt ortamlarıdır.

SMS: (İngilizce Short Message Service; Kısa Mesaj Hizmeti), cep telefonu aracılığı ile yazılan mesajın bir cep telefonundan diğer bir cep telefonuna gönderilmesi, mesajlaşması hizmetidir.

SNMP: "Simple Network Management Protocol"'ün kısaltması. "Basit Ağ Yönetimi Protokolü" adı verilen bu teknoloji, bilgisayar ağları büyüdükçe bu ağlar üzerindeki birimleri denetlemek amacıyla tasarlanmıştır.

SSH: (Secure Shell) güvenli veri iletimi için kriptografik ağ protokolüdür. Ssh ile ağa bağlı olan iki bilgisayar arasında veri aktarımı güvenlik kanalı üzerinden güvensiz bir ağda yapılır. Bu durumda ağda Ssh ile haberleşen makinelerden biri ssh sunucusu diğeri ssh istemcisi olur. Ssh kabuk hesabına erişim için Unix ve benzeri işletim sistemlerinde protokolün en iyi uygulaması olarak bilinir, ama aynı zamanda Windows üzerindeki hesaplara erişim için de kullanılabilir. SSH uzaktaki makineye bağlanıp kimlik kanıtlaması yapmak için açık anahtarlı şifrelemeyi kullanır ve bu sayede kullanıcıya sistemi kullanmasına izin vermiş olur.

SSL: Secure Socket Layer (Türkçe'ye Güvenli Yuva Katmanı olarak çevrilebilir) protokolü, internet üzerinden şifrelenmiş güvenli veri iletişimi sağlar.

Sunucu: (İngilizce: Server), bilgisayar ağlarında, diğer ağ bileşenlerinin (kullanıcıların) erişebileceği, kullanımına ve/veya paylaşımına açık kaynakları barındıran bilgisayar birimi. Bir ağda birden fazla sunucu birim bulunabilir. Karşıtı istemci (İngilizce: Client) dir.

USB Bellek (USB Flash): Kapasiteleri 256 GB'a kadar ulaşabilen, küçük, hafif, çalışma esnasında sökülüp takılabilir ve taşınabilir veri depolama aygıtlarıdır.

Virüs Tespit Ajanı (Antivirus Agent): Bilgisayarınızı zararlı programlardan korumak için virüsten korunma yazılımının virüsleri tespit eden yazılım parçasıdır.

WEP: WEP (Wired Equivalent Privacy), kablosuz ağ bağlantılarında veri bağ tabakasında çalışan şifreleme yöntemidir. Kabloya Eşdeğer Mahremiyet (KEM) olarak Türkçe'ye çevrilebilir.

Wi-fi: Wi-fi: "Wireles Fidelity" kelimelerinin kısaltması olup kablosuz bağlılık veya kablosuz bağlantı anlamına gelir.

WPA: WPA (Wi-Fi Protected Access)Wi-Fi korumalı Erişim olarak adlandırılır. WEP şifreleme sisteminden daha güvenli olduğu söylenen ve WEP şifrelemeden daha yeni bir teknolojidir.

Yazılım Yaması (Software Patch): Yazılımlarda oluşan bir hatayı ya da programın içeriğindeki hatalı bir fonksiyonu düzelten bir programcıktır.

Zip: (dosya formatı), bir popüler veri sıkıştırma ve arşivleme formatıdır. ZIP uzantılı dosyalar ".zip" şeklinde gözükür.

Zombi Bilgisayar (Zombie): Zombi bilgisayar, (genelde yalnızca zombi olarak kısaltılır) genel ağa (internet) bağlı, bir kırıcı (hacker) tarafından bilgisayar virüsü veya truva atı ile tehlikeye atılmış bilgisayardır.

## F. KAYNAK


1. Sağlık Bilgi Sistemleri Genel Müdürlüğü
2. TUBİTAK-BİLGEM
3. http://www.bilgiguvenligi.gov.tr/kilavuz-dokumanlar/index.php
4. www.bilgimikoruyorum.org.tr
5.http://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/veri-merkezlerinin-sahipolmasi-gereken-ozellikler.html
6. Ömer Faruk Acar, TÜBİTAK BİLGEM
7. Neşe SAYARI, Türkiye Bilişim Derneği, Bilgi Güvenliği ve Yönetimi
8. TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, BGYS Risk Yönetim Süreci,2007

**Kurum yönetimi olarak "Kurum Bilgi Güvenliği Politikası"nın uygulanmasının sağlanmasının ve kontrolünün yapılmasının güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.**

**Muhittin SELVİTOPU**
**Harita ve Kadastro Mühendisi**
**Belediye Başkanı**