BİLGİ GÜVENLİĞİ

GÖLBAŞI ŞEHİT AHMET ÖZSOY DEVLET HASTANESİ

2022

TANIM

- **Bilgi,** kurumun en değerli varlığıdır.
- Korunması ve verimli kullanılması sağlanmalıdır.
- **Bilgi Güvenliği,** kurumun en değerli varlığı olan bilginin kaybolmasını, zarara uğramasını, yok olmasını, yetkisiz ve kötü niyetli kişilerin eline geçmesini engellemektir.
- Bilgi güvenliğini sağlamak tüm personelin sorumluluğundadır.

BİLGİNİN BULUNDUĞU ORTAMLAR

FİZİKSEL ORTAMLAR	ELEKTRONİK ORTAMLAR
• Kağıt, Tahta • Pano, Yazı tahtası • Fax kağıdı • Çöp/Atık Kağıtlar • Dosyalar • Dolaplar	• Bilgisayarlar, • Mobil iletişim cihazları, • E-posta, • USB,CD,Disk • Disket, • Manyetik ortamlar…

BİLGİNİN BULUNDUĞU ORTAMLAR

SOSYAL ORTAMLAR	TANITIM ALANLARI
• Telefon görüşmeleri • Muhabbetler • Yemek araları • Toplu taşıma araçları	• İnternet siteleri, • Broşürler, • Reklamlar, Sunumlar, • Eğitimler, Görsel sunumlar.

TANIMLAR

- **Gizlilik;** Bilgiye erişime izni olan yetkili kişiler yada sistemlerin erişmesini sağlamaktır.
- **Bütünlük;** Bilginin yetkisiz kişi yada işlemler tarafından değiştirilmemesini sağlamaktır. Böylece bilginin tutarlılığı sağlanmış olur.
- **Erişilebilirlik;** Bilgiye doğru zamanda erişimin ve erişim sürekliliğinin sağlanmasıdır.

TANIMLAR

İdeal Güvenlik

- Doğru kişinin (doğru yetkiler ile yetkilendirilmiş kişinin)
- Doğru bilgiye (içeriği bozulmamış bilgiye)
- Doğru zamanda ve doğru erişim yoluyla (ihtiyaç olunan zamanda)ulaşılarak kullanılmasıdır.

BİLGİ GÜVENLİĞİ

- Personele, yaptıkları iş kadar, iş yapış yöntemlerinin ve işledikleri bilginin değerini farkettirir.
- Kurumu, bilgi kaybı nedeni ile uğrayacağı zarardan korur. Rekabetçi bir avantaj sağlar.
- Riskleri yönetilebilir kılar.
- Toplam kalitenin artmasına neden olur.

İHMALLER OLURSA

- Para : Oluşabilecek tüm maddi kayıplar.
- İş Kaybı : Bilginin oluşturulmasında harcanan iş ve emek gücü kaybı.
- İmaj : Sektörde oluşan firma isminin, etiketin zarar görmesi.
- Güven : Müşteriler ile, tedarikçi firmalar ile, bayiiler ile ve birlikte çalışılan veya çalışılabilecek kurumlar ile güven kaybı oluşması.
- Zaman : Bilginin oluşturulmasında harcanan zamanın kaybolması.
- Hukuksal Problemler : Para Cezaları, Hapis Cezaları,

RİSKLER

Donanım ve Yazılım kurulması

- İlgili ekipman güvenlik açığına sebep olabilir
- İlgili ekipman mevcut sistemin çalışmamasına sebep olabilir
- Kopya ve lisanssız ise hukuki problem oluşturabilir
- İnternetten indirilmiş ise virüs taşıyor olabilir
- Mevcut sistemle uyuşmuyor olabilir

RİSKLER

Parola belirleme

- En az 8 karakterden oluşmalı
- Büyük harf, küçük harf, rakam ve özel karakterler içermeli
- Harflerle oluşmuş kısmı anlamlı sözcükler içermemeli
- Düzenli olarak değişmeli
- Başkaları ile paylaşılmamalı
- Rahat erişebilir yerde saklanmamalı
- Kolay tahmin edilir olmamalı

RİSKLER

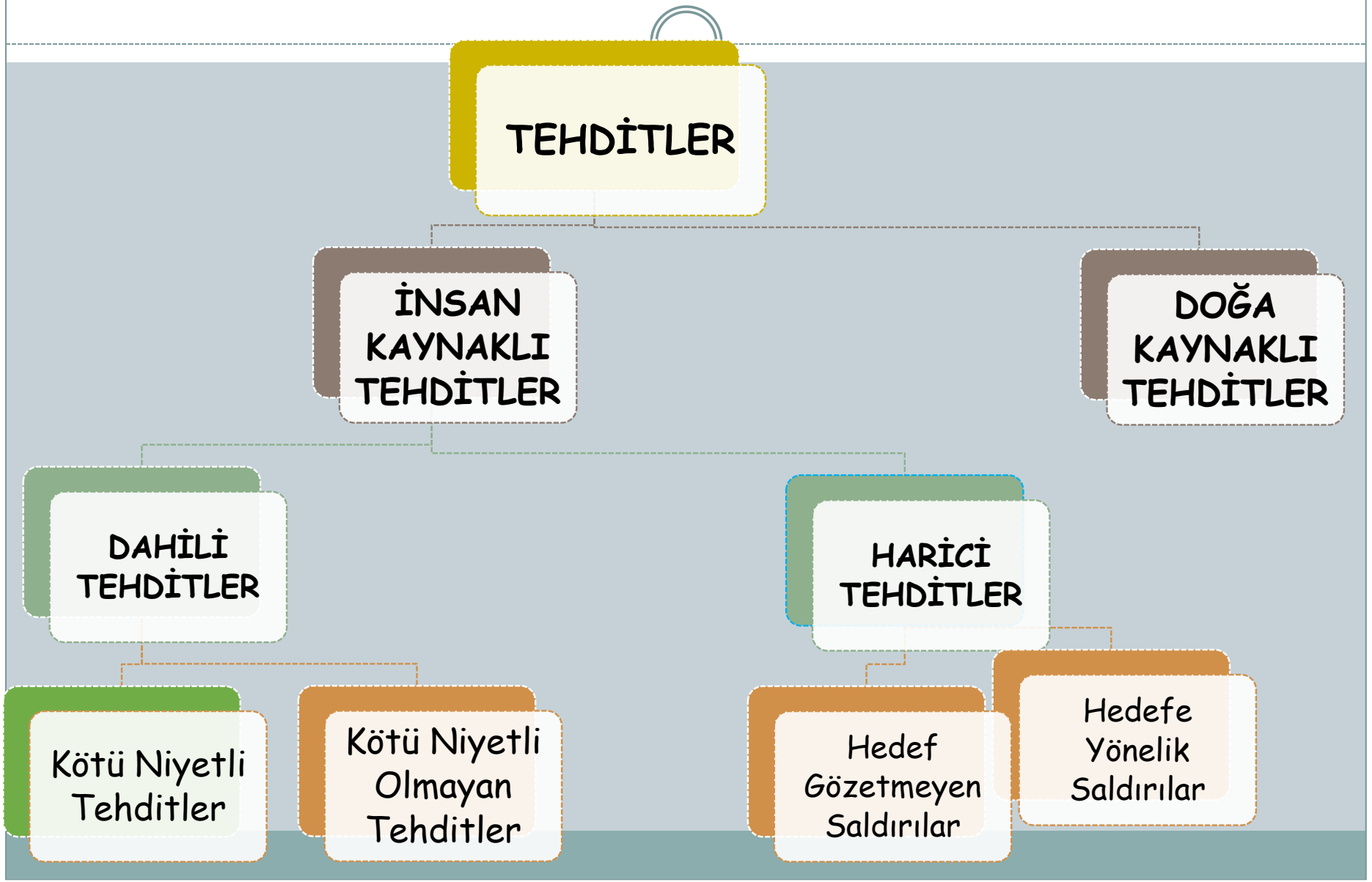
Virüsler

- Bilgi Güvenliği için gerçek ve kesin bir tehdit oluştururlar
- Bilgi ye zarar verebilir, yok edebilir, yetkisiz kişilerin eline geçmesini sağlayabilir

Virüsler nasıl bulaşır ?

- İnternet yada ağ üzerinden
- USB bellek yada harici disklerden
- Korsan \ Lisanssız yazılım CD lerinden
- E-Posta yoluyla

TEHDİTLER


TEHDİTLER
İNSAN KAYNAKLI TEHDİTLER
DOĞA KAYNAKLI TEHDİTLER
DAHİLİ TEHDİTLER
HARİCİ TEHDİTLER
Kötü Niyetli Tehditler
Kötü Niyetli Olmayan Tehditler
Hedef Gözetmeyen Saldırılar
Hedefe Yönelik Saldırılar

TEDBİRLER

- Çalışma masası ve bilgisayar ekranı üzerinde bilgiye yetkisiz ulaşım engellenmelidir
- Çalışma odaları ayrılırken kilitlenerek, anahtarları kontrol altında tutulmalıdır.
- Bilgisayar ekran kilidi aktif hale getirilmeli ve süresi çok uzun olmamalıdır.
- Bilgisayar başından ayrılırken Windows Logo + L tuşlarıyla bilgisayar kilitlenmelidir.
- Kullanıcı adı ve şifre iyi korunmalıdır.

TEDBİRLER

- E-posta adresini haber grupları, sohbet odaları, internet sayfaları, sosyal paylaşım siteleri gibi herkese açık yerlerde yayınlanmamalı
- Birden çok kişiye veya bir gruba e-posta gönderirken kişilerin e-posta adreslerini gizli karbon kopya (BCC) bölümüne yazmalı
- Bir web sitesinde yapılan işlem gereği e-posta adresi istendiğinde, sitenin gizlilik politikasını kontrol etmeli
- İstenmeyen e-postalara hiç bir şekilde cevap yazmamalı
- Kullanım amacına göre farklı e-posta adresleri kullanmalı.
- Kişisel, kurumsal ve mali bilgiler tanıdığınız kişiler dahil hiç kimseye e-posta yoluyla gönderilmemeli
- E-posta mesajlarındaki internet bağlantılarına tıklanmamalı

YASAL DAYANAKLAR

- Anayasa,
- 5237 sayılı Türk Ceza Kanunu,
- 4721 sayılı Türk Medeni Kanun,
- 3359 sayılı Sağlık Hizmetleri Temel Kanunu,
- 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun,
- 5258 sayılı Aile Hekimliği Pilot Uygulaması Hakkında Kanun,
- 663 sayılı Kanun Hükmünde Kararname,
- 5070 sayılı Elektronik İmza Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun",

YASAL DAYANAKLAR

- 26716 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik”,
- 26680 sayılı “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”,
- Sağlık Bakanlığı ve Bağlı Kuruluşlarının Elektronik Belge Yönetimi Sistemi Uygulama Yönergesi,
- **Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi.**

- **Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi**
- Amaç: Sağlık Bakanlığına ait tüm bilgilerin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek korunmasını sağlamak.

KURUMA AİT GİZLİ KALMASI GEREKEN BİLGİLER

- 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe konulan “Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar” ile tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belge
- Kurum tarafından işlenen (24/3/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan) kişisel veriler ile (20/10/2016 tarih ve 29863 sayılı Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik ile tanımlanan) kişisel sağlık verileri

KURUMA AİT GİZLİ KALMASI GEREKEN BİLGİLER

- Açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya kuruma haksız yarar sağlama ihtimali bulunan her türlü bilgi ve belge
- Bakanlığa veya hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgisayar sistemleri içerisinde saklanan veriler, donanım/yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduğu işler

PERSONEL YÜKÜMLÜLÜKLERİ

- Kuruma ait gizli kalması gereken bilgiler, yasal zorunluluklar ve kurum tarafından resmi olarak izin verilmesi halleri dışında süresiz olarak korunur,
- Kurum tarafından aksi belirtilmedikçe, hiç bir şekilde söz konusu bilgileri doğrudan veya dolaylı olarak kullanılmaz; başka bir yere aktarılmaz, yayımlanmazı, açıklanmaz, kopyaları alınmaz.

PERSONEL YÜKÜMLÜLÜKLERİ

- Kuruma ait gizli kalması gereken her türlü bilgiyi sır olarak saklamak, bunları üçüncü kişilere inceletmemek, söylememek, iletmemek ve açıklamamak,
- Öğrenilen bilgiler ve bunlara ilişkin belgeler yetkileri olmayan kişilere ve makamlara açıklanmaz ve bu yükümlülük kurum ile ilişkinin sona ermesi halinde de devam eder.

PERSONEL YÜKÜMLÜLÜKLERİ

- Sosyal medya hesaplarını kullanırken görevin gerektirdiği dikkat ve özeni gösterilir, kuruma ait gizli kalması gereken bilgileri, hastalara ilişkin kişisel bilgiler (hasta görüntüleri vb.) sosyal medya platformlarında paylaşılmaz.

PERSONEL YÜKÜMLÜLÜKLERİ

- Kurum tarafından uygun görülen sistem, uygulama, kullanıcı işlemleri ve bilgi sistem ağındaki veriler ve veri akışının iz kayıtları hukuki ve idari süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla toplanabilir.

PERSONEL YÜKÜMLÜLÜKLERİ

- Çalışanlara kurum tarafından verilen bilgisayar, tablet, telefon, taşınabilir medya gibi cihazlar sadece göreve yönelik, kurumsal faaliyetler için kullanılır, özel işlemlerde kullanılmaz.

PERSONEL YÜKÜMLÜLÜKLERİ

- Kullanıcıya verilen "kullanıcı adı" ve "parola” bir başkası ile paylaşılmaz ve bir başkasına kullandırılmaz.
- Kurumdan ayrılmak halinde şahsa tahsis edilen kullanıcı adı ve parolayı iptal ettirilir, kullanılan bilgisayar ve/veya diğer elektronik veri depolama cihazlarında oluşturulan veri, bilgi ve belgeler dâhil tüm dosyalar, cihazlar ve ofis malzemeleri eksiksiz olarak kurum yetkilisine teslim edilir ve kopyası alınmaz.

PERSONEL YÜKÜMLÜLÜKLERİ

- Kişiye tahsis edilen "kullanıcı adı" ve "parola" ile her kullanıcı kendi oturumunu açar, çalışma bitince, oturum veya bilgisayar kapatılarak bilgisayara başkalarının fiziksel erişimine fırsat verilmez, bilgisayarımın başından kısa süreli ayrılmalarımda bilgisayar oturumu kilitlenir.

PERSONEL YÜKÜMLÜLÜKLERİ

- Kurum tarafından sağlanan internet üzerinden girilen ve girilemeyen tüm siteler ve adresler sistem tarafından gerekli olduğunda kullanılmak üzere kayıt altına alınır; bu kapsamda 5651 sayılı “İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun” gereği kişiye tahsis edilen kullanıcı adı ve parola kullanılmak suretiyle usulüne uygun olarak kayıt altına alınan işlemlerden yasal olarak ilgili kullanıcı sorumlu tutulur.

PERSONEL YÜKÜMLÜLÜKLERİ

- Kurum sunucuları üzerinde kişiye tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP/MAC adresini kullanarak gerçekleştirilen her türlü etkinlikten, kurum bilişim kaynaklarını kullanarak oluşturulan ve/veya kişiye tahsis edilen kurum bilişim kaynağı üzerinde bulundurulan her türlü kaynağın (belge, doküman, yazılım vb.) içeriğinden kullanıcı sorumludur.

PERSONEL YÜKÜMLÜLÜKLERİ

- Çalışan kendisne teslim edilen kullanıcı adı ve parolanın gizli kalmasını sağlamakla yükümlüdür, şahsi kusur nedeniyle kullanıcı adı ve parolanın başkaları tarafından öğrenilmesi halinde, bu bilgiler kullanılarak yapılan iş ve işlemlerden şahıs kendisi sorumludur.

PERSONEL YÜKÜMLÜLÜKLERİ

- İşin gerektirdiği haller dışında kurumsal e-posta hesabı kullanılmaz, kurum içindeki diğer kullanıcılara iş ile ilgili olmayan toplu ve/veya kişisel e-posta gönderilmez; kurum içine veya kurum dışına gönderilen tüm e-postalardan çalışan kişisel olarak sorumludur.

PERSONEL YÜKÜMLÜLÜKLERİ

- Çalışana teslim edilmiş elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılım, donanım, araç ve gereç üzerinde kurum bilgisi dışında hiçbir mekanik ya da yazılımsal yapılandırma değişiklik yapılamaz.

PERSONEL YÜKÜMLÜLÜKLERİ

- Bilgisayarlara kurum tarafından yüklenmiş işletim sistemi ve uygulama yazılımları dışında herhangi bir işletim sistemi veya lisanssız yazılım yüklenmez, kurum tarafından yüklenmemiş yazılımlardan doğacak sorumluluk personele aittir.