KAYSERİ İLİ KAMU HASTANELERİ BİRLİĞİ
GENEL SEKRETERLİĞİ

PERSONEL İÇİN BİLGİ GÜVENLİĞİ POLİTİKASI

1. TANIM

Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.
Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

- **Gizlilik**
- **Bütünlük**
- **Kullanılabilirlik**

Bu kavramları biraz daha açacak olursak:
Gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.
Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz.
Kullanılabilirlik, bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

2. KAPSAM

Bu politika, kurum Bilgi İşlem altyapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

3. DAYANAK

- T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı 17 Eylül 2007 tarih ve 2023 sayılı "Bilgi Güvenliği Politikaları" konulu yazıları,
- T.C. Sağlık Bakanlığı İdari ve Mali İşler Daire Başkanlığının 2010/61 sayılı Genelgeleri.
- T.C. Sağlık Bakanlığı Bilgi Sistemleri Genel Müdürlüğü Bilgi Güvenliği Kılavuzu 2014

4. AMAÇ

Kurum yönetimi açısından;

- Kurumun güvenilirliğini ve temsil ettiği makamın imajını korumak,
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak,
- Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak

Amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

5. İLKELER

- Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes
- Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
- Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
- Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,
- Bilgi güvenliği ihlal olaylarını raporlamalı ve Bilgi İşlem Birimi'ne bildirmeli, bu ihlalleri engelleyecek önlemleri almalıdır.

- Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.
- Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.
- Kurumun tüm çalışanları; bu politikaya ve talimatlarına uymakla yükümlüdür.

6. ROLLER VE SORUMLULUKLAR

a) İş süreçlerinin gereksinimi olarak her tür bilgi, en az kesintiyle kapsam dahilindeki birimler, hizmet verenler ve gereken üçüncü taraflarca erişilebilir olacaktır.
b) Bilgilerin bütünlüğü her durumda korunacaktır.
c) Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.
d) Bilgi Güvenliği Yönetim Sisteminin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeye indirilecektir.
e) Bilgi; bilginin elektronik iletişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak korunacaktır.
f) Çalışma alanlarında "Temiz Ekran/Temiz Masa" prensiplerine uygun olarak, tasnif dışı özellikteki bilgiler dışında bilgilerin, başkalarınca görülmesine imkan verilmeyecek şekilde önlemler alınacaktır.
g) Tüm çalışanlarımız bütün faaliyetlerde "bilmesi gereken" prensibine göre bilgilendirilecek olup; elektronik ortamda da "bilmesi gereken" prensibi çerçevesinde erişilebilir olacaktır.
h) Tüm birim yöneticileri bu esasları uygulanmasından birinci dereceden sorumlu olacaklar ve personelin bu esaslara uygun olarak çalışmasını sağlayacaklardır.

7. POLİTİKA İHLALİ VE YAPTIRIMLAR

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, ilgililer hakkında Bilgi Güvenliği Disiplin Prosedürüne göre yasal işlem başlatılabilir.
İşbu "Bilgi Güvenliği Politikası" Kayseri İli Kamu Hastaneleri Birliği Genel Sekreterliği tarafından onaylanmasının ardından yürürlüğe girer ve tüm bağlı sağlık tesisleri personelince uyulması zorunludur.
"Bilgi Güvenliği Politikası" çerçevesinde, Kurumsal Bilişim sistemlerinin güvenliğinde herhangi bir aksamaya mahal verilmemesi için genel sistem seviyesinde alınmış olan güvenlik tedbirleri yanında tüm personelimizin aşağıda belirtilen hususlara uyması zorunludur.

8. İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ

8.1. Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
8.2. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.
8.3. ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında (izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.
8.4. Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
8.5. İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kağıt kesme makinasında imha edilmelidir.
8.6. Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
8.7. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
8.8. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

8.9. Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

9. EKİPMAN GÜVENLİĞİ

9.1. Masalarda ya da çalışma ortamlarında korumasız bırakılmış bilgiler yetkisiz kişilerin erişimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle bütünlüğünün bozulmalarına ya da yok olmalarına sebep olabilir. Tüm bu veya daha fazla tehditleri yok edebilmek için aşağıda yer alan belli başlı temiz masa kurallarına ilişkin politikalar geliştirilmeli ve bu politikaların çalışanlar tarafından haberdar olunması sağlanmalıdır.

9.2. Belli başlı temiz masa kuralları;

9.2.1 Hassas bilgiler içeren evraklar, bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir. Bu bilgi ve belgelerin kilitli yerlerde muhafaza edilmesi gerekmektedir.

9.2.2 Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir.

9.2.3 Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır.

9.2.4 Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yakma vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir.

9.2.5 Faks makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmamalıdır.

9.2.6 Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), PCler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

10. PAROLA GÜVENLİĞİ

10.1. Güvenliğin oluşturulacağı birim için kullanılan programlarda uygulanan parola standardı belirlenmeli, bu parola sistemi aşağıdaki unsurları içerecek standarda getirilmelidir.

10.2. Bilgi Güvenliği Yetkilisinin devreye girmesi ile parola standardı belirlenerek uygulanmaya başlanmalı, geliştirilerek aşağıdaki yapıya çekilmesi konusunda plan yapılmalıdır.

10.3. Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.

10.3.1 Kişisel bilgiler gihi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır.
(Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız gibi)

10.3.2 Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.

10.3.3 Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

10.4. Basit bir kelimenin içerisindeki harf veya rakamları benzerleri değiştirilerek güçlü bir parola elde edilebilir.

'B' yerine 8	'Z' yerine 2	**Örneğin**
'I', 'i', 'L', 'l' yerine 1	'O' harfi yerine 0	Balıkçıl-Kazak 8a1Ikçl1-Ka2ak
'S' yerine 5 'G' yerine 6	'g' yerine 9	Solaryum! 501aryum!

Tablo 6. Güçlü parola yöntemleri

10.5. Basit bir cümle ya da ifade içerisindeki belirli kelimeler özel karakter veya rakamlarla değiştirilerek güçlü bir parola elde edilir.

'T', 't' yerine '+'	'$', 'ş' yerine '$'	**Örneğin** "Dün Kar Yağmış" : Dün*Yağm1$ "Şeker gibi bir soru sordu" : $eker~1?Sordu "Tek eksiğim bir güldü" : 1-ğim1:)dü "Yüzeysel bir soru eşittir eksi puan": %eysel1?=-Puan
"kar", "yıldız" yerine '*'	"dolar", "para" yerine '$'	
"Soru" yerine '?'	"gibi" yerine '~'	
"gül" yerine ':)'	"eksi" yerine '-'	
"bir", "tek" yerine 1	"yüz", "yüzde" yerine '%'	

Tablo 7. Güçlü parola yöntemleri

10.6 . Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her üç ayda birdir.
10.7. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
10.8. Şifreler başkası ile paylaşılmamalı, kâğıtlara ya da elektronik ortamlara yazılmamalıdır.
10.9. Şifrelemede, küçük ve büyük karakterlere (örnek, a-z, A-Z), hem rakam hem de noktalama karakterlerine (örnek, 0-9, !'^+%&/()=?_;*) sahip olmalıdır.
10.10. En az sekiz adet alfa nümerik karaktere sahiptir.
10.11. Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
10.12. Aile isimleri kullanılmamalıdır.
10.13. Herhangi bir kişiye telefonda şifre verilmemelidir.
10.14. E-posta mesajlarında şifre yazılmamalıdır.
10.15. Şifreler aile bireyleriyle paylaşılmamalıdır.
10.16. Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.
10.17. Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.
10.18. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

11. E-POSTA KULLANIM KURALLARI

11.1. Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.
11.2. İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.
11.3. Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.
11.4. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.
11.5. İnternet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-posta adresi bu mesajlarda kullanılamaz. Ancak iş gereği üye olunması yararlı internet haber grupları için yöneticisinin onayı alınarak Kurumun sağladığı resmi eposta adresi kullanılabilir.
11.6. Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.
11.7. E-posta gönderiminde konu alanı boş bir e-posta mesajı göndermemelidir.
11.8. Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.
11.9. E-postaya eklenecek dosya uzantıları ".exe", ".vbs" veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip veya rar formatında) mesaja eklenmelidir.
11.10. Bakanlık ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine ilişti-rilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

11.11. Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.
11.12. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.
11.13. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Sistem Yönetimine haber verilmelidir.
11.14. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verilmemelidir.
11.15. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
11.16. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur.
11.17. Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.
11.18. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.
11.19. Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.
11.20. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Sistem Yönetimine haber verilmelidir.
11.21. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Sistem Yönetimine haber vermelidir.
11.22. Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır
11.23. Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
11.24. Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki bir kişisel klasöre (personel folder) çekilmelidir.
11.25. Kullanıcılar gönderdikleri, aldıkları veya sakladıkları e-maillerde kişisellik aramamalıdır. Yasadışı ve hakaret edici e-posta haberleşmesi yapılması durumunda yetkili kişiler önceden haber vermeksizin e-mail mesajlarını denetleyebilir ve kullanıcı hakkında yasal ve idari işlemler başlatabilir.
11.26. Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludurlar. Şifrelerin kırıldığını fark ettikleri andan itibaren yetkililerle temasa geçip durumu haber vermekle yükümlüdürler.
11.27. Altı ay süre ile kullanılmayan e-posta kutuları Bilgi İşlem birimi tarafından kaldırılabilir. Kurumdan ayrılan personel kurumsal e-posta sistemini kullanamaz. E-posta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma, işten ayrılma sebepleriyle kurumdaki değişikliğinin yetkililer tarafından Bilgi İşlem birimine en kısa zamanda bildirilmesi gerekmektedir.

12. ANTİVİRÜS POLİTİKASI

- Bütün bilgisayarda kurumun lisanslı antivirüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.
- Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem birimine haber verilmelidir.
- Zararlı programları (örneğin, virüsler, solucanlar, truva atı, e-mail bombaları vb) kurum bünyesinde oluşturmak ve dağıtmak yasaktır.

• Hiçbir kullanıcı herhangi bir sebepten dolayı anti virüs programını sistemden kaldıramaz ve başka bir anti virüs yazılımını sisteme kuramaz.

13. İNTERNER KULLANIM POLİTİKASI

• Hiçbir kullanıcı peer-to peer bağlantı yoluyla internetteki servisleri kullanamayacaktır. (Örneğin; KaZaA, iMesh, eDonkey, Gnutella, Napster, Aimster, Madster, FastTrak, Audiogalaxy, MFTP, eMule, Overnet, Neo-Modus, Direct Connect, Asquisition, BearShare, Gnucleus, GTK-Gnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, XoLoX, OpenNap, WinMX. vb)

• Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ, MIRC, Messenger, Facebook, Twitter, WhatsApp vb. mesajlaşma ve sohbet programları gibi chat programlarının kullanılmaması. Bu chat programları üzerinden dosya alışverişinde bulunulmamalıdır.

• Hiçbir kullanıcı internet üzerinden Multimedia Streaming (Video, mp3 yayını ve iletişimi) yapmayacaktır.

• Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.

• İş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek yasaktır.

• İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz.

• Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.

• Bilgisayar İşletim Sistemlerine zarar verdiği için internet üzerinden ekran koruyucu, yamalar, masaüstü resimleri, yardımcı, tamir edici program olduğu belirtilen araçlar gibi her türlü dosya ve programların indirilmesi ve/veya kurulması yasaktır.

• Üçüncü şahısların kurum içerisinden interneti kullanmaları Bilgi İşlem sorumlusunun izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.

• Bilgi İşlem Birimi, iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir.

14. MOBİL CİHAZ GÜVENLİĞİ

Bilgiyi taşımanın kolay bir yolu laptop ve akıllı telefonlar gibi mobil cihazlardır. Bu cihazlarda bulunan hassas bilgiler ve erişim yetkileri de düşünüldüğünde mobil cihazlarda güvenliğin dikkat edilmesi gereken bir konu olduğu anlaşılmaktadır.

14.1. Mobil cihazlara erişimde mutlaka parola kullanılmalıdır.

14.2. Mobil cihazınızda ne tür bilgiler sakladığınızın farkında olun, hassas ve gizli bilgileri mümkün olduğunca mobil cihazınızda bulundurmayınız.

14.3. Verilerinizin yedeklerini alın ve güncel bir kopyasını farklı bir yerde saklayınız.

14.4. Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

15. KAYDEDİLEBİLİR TAŞINIR MATERYALLER GÜVENLİĞİ

USB flash diskler ve harici hddler; yüksek veri kapasiteleri, boyutları, taşınabilirlikleri ve farklı sistemlerde sorunsuzca çalışabilmeleri ile yanımızdan hiçbir zaman ayırmadığımız temel ihtiyaçlarımızdandır. Hemen hemen her sistemde çalıştırılabiliyor olmaları nedeniyle de bilgisayarlar arası veri alışverişimizi USB diskler ve harici hddler yardımıyla yapıyoruz.

USB disklerimizi onlarca farklı bilgisayarda kullanıyor, yine bilgisayarımıza onlarca farklı diskin takılmasına izin veriyoruz. Aslında USB diskleri tehlikeli kılan da bu çok da denetimli olmayan taşınabilirlikleri. Taşınabilir medya

üzerinden bilgisayara giren zararlı yazılımlar başta bilgi sızdırma, uzaktan komut koşturma ve servis dışı bırakma olmak üzere birçok güvenlik zafiyetine neden olabilmektedir.

15.1. Taşınacak veri eğer USB disk ile taşınacaksa bu USB diskin tehdit unsuru olan bir yazılım içermediğine emin olunmalıdır.
15.2. USB disk biçimlendirdikten sonra veriyi kopyalanmalıdır. Aksi takdirde içerisinde tehdit unsuru olan casus yazılımlar USB disk içindeki verinin silinmesine veya başkalarını eline geçmesine neden olabilir.
15.3. Taşınacak verinin de tehdit unsuru içeren herhangi bir yazılım içermediğine emin olunmalıdır.
15.4. Veriyi ister USB disk isterse de CD, dvd ortamında taşınsın kesinlikle şifrelemelidir.
15.5. Veriyi USB disk ile taşıyorsak; bunları bilgisayara takarken USBlerin sağlıklı çalıştığından emin olmalıyız. Aksi taktirde aygıtımızın bozulmasına neden olabilir.
156. USB diskleri bilgisayardan çıkartırken aygıtı düzenli şekilde çıkart dedikten sonra bilgisayardan çıkartmalıyız aksi taktirde aygıtımız bozulabilir.
15.7. Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir. Özellikle hard diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır.
15.8. CD ve dvdlerde veri saklamak için ise kaliteli medyalar kullanmalı, düşük hızla yazdırmalı, alt yüzeye mümkün olduğunca temas etmemeli, nemli, ışık almayan ortamlarda CDleri çok fazla sıkıştırmadan saklanmalıdır.
15.9. Kötü amaçlı kimselerin bilgilerimize ulaşmasını engellemek için taşınabilir materyallerimizi güvenilir şekilde muhafaza etmeliyiz. Gerekirse kilitli dolaplarda veya çelik kasalarda muhafaza edilmelidir.
15.10. Taşınır materyaller çalışma masasında veya bilgisayarda güvensiz şekilde bırakılmamalıdır. Yanımızda, kaybedebileceğimizden dolayı mümkün olduğunca taşınmamalıdır. Eğer taşınıyorsa veri kesinlikle şifrelenmelidir.

16. BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ

16.1. Bakanlık ve Bağlı Kuruluşlar kendi bünyelerinde oluşturacakları arşivden sorumludur. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.
16.2. Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.
16.3. Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.
16.4. İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
16.5. Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.
16.6. Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
16.7. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
16.8. Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.
16.9. Hacimsel küçültme işlemi için parçalanmalıdır.
16.10. Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.
16.11. Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme

tesislerine iletilmesi gerekmelidir.

17. SOSYAL MÜHENDİSLİK ZAFİYETLERİ

Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Başka bir tanım ise; İnsanoğlunun zaaflarını kullanarak istediğiniz bilgiyi, veriyi elde etme sanatına sosyal mühendislik denir. Sosyal mühendisler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanların zaaflarından faydalanıp, en çok etkileme ve ikna yöntemlerini kullanırlar.

17.1. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.
17.2. Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
17.3. Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.
17.4. Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgileriniz paylaşılmamalıdır.
17.5. Şifre kişiye özel bilgidir. Sistem yöneticiniz dahil telefonda veya e-posta ile şifrenizi paylaşmamalısınız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
17.6. Oluşturulan dosyaya erişecek kişiler ve hakları "bilmesi gereken" prensibine göre belirlenmelidir.
17.7. Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.
17.8. Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.
17.9. Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.
17.10. Kazaa, emule gibi dosya paylaşım yazılımları kullanılmamalıdır.

18. SOSYAL MEDYA GÜVENLİĞİ

18.1. Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
18.2. Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
18.3. Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.

19. GENEL KULLANIM POLİTİKASI

19.1. Bütün PC ve Laptoplar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmelidir.
19.2. Laptoplar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
19.3. Kurumda domain (çalışma alanı) yapısı varsa mutlaka login olunmalıdır. Bu durumda, domain' e bağlı olmayan bilgisayarların yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.
19.4. Laptopların çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Birimi' ne haber verilmelidir.
19.5. Bütün Cep Telefonu ve PDA (Personal Digital Assistant) cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, vs) özellikleri aktif halde olmamalıdır ve mümkünse antivirüs programları ile yeni nesil virüslere karşı korunmalıdır.
19.6. Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) sistemin sahibi sorumludur.
19.7. Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.
19.8. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service,hotspot, ultrasurf vb.) eylemlere girişmemelidir.
19.9. Port veya ağ taraması yapılmamalıdır.
19.10.Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DOS saldırısı, port-network taraması vb. yapılmamalıdır.

19.11. Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.
19.12. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
19.13. Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.
19.14. Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD'leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.
19.15. Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır. Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, müdürlüğümüzün bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilemez.
19.16. Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin düzenli olarak farklı ortamlara (CD,DVD, USB, External Harddisk vb) yedeklenmesinden ve bu yedeklerin korunmasından sorumludur.
19.17. Bilgi İşlem birimi tarafından atanan yetkili kişiler kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel kişisel bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.
19.18. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
19.19. Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
19.20. Kurumda Bilgi İşlem biriminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.
19.21. Birimlerde sorumlu Bilgi İşlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.
19.22. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
19.23. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir.