T.C.

SAĞLIK BAKANLIĞI

BAMMAN İL SAĞLIK MÜDÜRLÜĞÜ

BATMAN AĞIZ VE DİŞ SAĞLIĞI MERKEZİ

BİLGİ GÜVENLİĞİ POLİTİKALARI KILAVUZU

V.II

EYLÜL 2018


T.C. Sağlık Bakanlığı
Bilgi Güvenliği Politikaları Kılavuzu
Bakanlık Makamının 02/05/2018 tarihli ve
98813779.719.54 sayılı onayı ile Bilgi Güvenliği
Politikaları Yönergesinin eki

T.C.
SAĞLIK BAKANLIĞI
BATMAN İL SAĞLIK MÜDÜRLÜĞÜ
BATMAN AĞIZ VE DİŞ SAĞLIĞI MERKEZİ
BİLGİ GÜVENLİĞİ POLİTİKASI

EK: A

1.Tanım,

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 (Confidentiality)**
- **Bütünlük (Integrity)**
- **Kullanılabilirlik (Availability)**

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;

a) T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı 17 Eylül 2007 tarih 2023 sayılı VE "Bilgi Güvenliği Politikaları" konulu yazıları,

b) T.C. Sağlık Bakanlığı İdari ve Mali İşler Daire Başkanlığının 2010/61 sayılı Genelgeleri.

c) T.C. Sağlık Bakanlığı Bilgi güvenliği Politikaları Kılavuzu Bakanlık Makamının 28/02/2014 tarihi ve 5181.1272 sayılı yönergesi

e) T.C. Sağlık Bakanlığı Bilgi güvenliği Politikaları Kılavuzu Bakanlık Makamının Bakanlık Makamının 02/05/2018 tarihli ve 98813779.719.54 sayılı yönergesi

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:

a) Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,

b) Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,

c) Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,

d) Bilgi güvenliği ihlal olaylarını raporlamalı ve Bilgi İşlem Birimi'ne bildirmeli, bu ihlalleri engelleyecek önlemleri almalıdır.

e) Kurum içi bilgi kaynakları (Duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.

f) Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.

Kurumun tüm çalışanları; bu politikaya, Prosedür 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. Politika İhlali ve Yaptırımlar;

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, ilgililer hakkında adli ve idari yasal takibat başlatılarak; aşağıdaki yaptırımlardan bir ya da birden fazla maddesi uygulanabilir.

- Uyarma,
- Kınama,
- Aylıktan Kesme,
- Kademe İlerlemesinin durdurulması,
- Para cezası,
- Sözleşmenin feshi,

8. İşbu "Bilgi Güveliği Politikası" Batman ADSM Başhekimliğince onaylanmasının ardından yürürlüğe girer ve tüm ADSM personelince uyulmalıdır.

İl Müdürlüğümüz "Bilgi Güvenliği Politikası" çerçevesinde, Kurumsal Bilişim sistemlerinin güvenliğinde herhangi bir aksamaya mahal verilmemesi için genel sistem seviyesinde alınmış olan güvenlik tedbirleri yanında aşağıda belirtilen hususlara bütün ADSM çalışanları uymak zorundadır.

1. 1. E-Posta Kullanma Kuralları

a. Kurumun e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.

b. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

c. Kişisel kullanım için İnternet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

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

e. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

f. Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

g. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

h. Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.

i. Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.

j. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodlar içerebilirler.

k. Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.

l. Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki bir kişisel klasöre (personel folder) çekilmelidir.

m. ADSM çalışanları 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.

n. 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.

o. 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.

2. 2. Şifre Kullanma Kuralları

a. 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.

b. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

c. Şifreler başkası ile paylaşılmamalı, kağıtlara yada elektronik ortamlara yazılmamalıdır.

d. Şifrelemede, küçük ve büyük karakterlere (örnek, a-z, A-Z), hem rakam hemde noktalama karakterlerine (örnek, 0-9, !'^+%&/()=?_;*) sahip olmalıdır.

e. En az sekiz adet alfa nümerik karaktere sahiptir.

f. Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.

g. Aile isimleri kullanılmamalıdır.

h. Herhangi bir kişiye telefonda şifre verilmemelidir.

i. E-posta mesajlarında şifre yazılmamalıdır.

j. Şifreler aile bireyleriyle paylaşılmamalıdır.

k. Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.

l. Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.

m. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

3. 3. Antivirüs Politikası

a. Bütün bilgisayarda kurumun lisanslı antivirüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.

b. Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem birimine haber verilmelidir.

c. Zararlı programları (örneğin, virüsler, solucanlar, truva atı, e-mail bombaları vb) kurum bünyesinde oluşturmak ve dağıtmak yasaktır.

d. Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını sisteme kuramaz.

4. 4. İnternet Kullanım Politikası

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

b. Bigisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ, MIRC, Messenger vb. mesajlaşma ve sohbet programları gibi chat programlarının kullanılmaması. Bu chat programları üzerinden dosya alışverişinde bulunulmamalıdır.

c. Hiçbir kullanıcı internet üzerinden Multimedia Streaming (**Video, mp3 yayını ve iletişimi**) **yapamayacaktır**.

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

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

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

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

h. 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.

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

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

5. 5. Genel Kullanım Politikası

a. Bütün PC ve Laptoplar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmelidir.

b. Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.

c. 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.

d. Laptop bilgisayarın çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Birimi' ne haber verilmelidir.

e. 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.

f. 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.

g. Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.

h. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service vb.) eylemlere girişmemelidir.

i. Port veya ağ taraması yapılmamalıdır.

j. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.

k. Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.

l. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.

m. Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.

n. Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (**Dergi CD' leri veya internetten indirilen programlar vs.**) kurmak ve kullanmak **yasaktır**.

o. Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.

p. 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.

q. 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.

r. 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.

s. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.

t. Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

u. Kurumda Bilgi İşlem biriminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.

v. 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.

w. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.

x. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

y. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir.

Yukarıda belirtilen talimatları okudum, uygulamada aksaklığa mahal vermeyeceğimi taahhüt eder, aksi halde yapılacak olan adli ve idari işlemden doğacak hukuki sonuçlarına katlanacağımı taahhüt ederim.