1. YÖNETİM SÜREÇLERİ

Sağlık tesisimiz teşhis tedavi hizmetlerinde; yasal mevzuat şartların karşılanmasından, hizmet sunumunda hasta ihtiyaç ve beklentilerine cevap verecek şekilde gerçekleşmesinden sorumludur. Hasta kayıtları, tanı ve tedavi bilgileri radyoloji görüntüleri, laboratuvar sonuçları, ameliyat bilgileri, ücretlendirmeler gibi tüm bilgiler HBYS ortamında kaydedilmekte ve veri tabanında saklanmaktadır.

AMAÇ:

a. Faaliyetlerimizin ticari, mali ve diğer iç ve dış baskılardan ve etkilerden uzak tutulmasını,
b. Hasta ve hak sahiplerine ait gizli bilgilerin ve tescilli hakların korunmasını,
c. Teşhis ve tedavi sonuçlarının uygun şartlarda muhafaza edilmesini ve iletilmesini,
d. Yeterlilik, tarafsızlık, karar verme ve çalışmalarda güveni azaltacak herhangi bir faaliyette bulunmamayı,
e. Sağlık hizmeti sunarken beklenen kalite seviyesinin sağlanmasını,
f. Vereceğimiz hizmetin belirlenen standartlar çerçevesinde gerçekleştirilmesini,
g. Söz konusu bilgileri hasta onayı dışında ya da yasal bir yükümlülük altında bulunmadığı sürece herhangi bir üçüncü şahıs, kurum ve kuruluş ile paylaşmamayı taahhüt eder. Kurum olarak gizliliğin önemli olduğuna inanırız. Bu politika hastanemizde sunulan tüm sağlık hizmetleri için geçerlidir.
h. Hastanemiz Hasta Hakları, güvenlik, veri bütünlüğü, erişim ve uygulama ile ilgili gizlilik ilkelerine bağlıdır.

KAPSAM:

a. Sağladığınız bilgiler; hastanemize teşhis ve tedavi için başvurduğunda hastalarımızdan kişisel bilgiler (ad, soyad, hastalık bilgileriniz, T.C Kimlik numarası, adres, telefon bilgileri, vb..) istenmektedir.
b. Hastanemiz yalnızca, Hasta Bilgi Güvenliği Politikası ve/veya belirli hizmetlere ilişkin gizlilik uyarısında açıklanan amaçlarla kişisel bilgileri kullanır.
c. Bilgi güvenliğini sağlamak amacıyla Bilgi Güvenliği gizlilik sözleşmesi tüm personele imzalatılmaktadır.
d. Bu doküman kurumumuz bilgi yönetimi işlemleri, genel HBYS kullanımı, erişim kuralları ile bilgi güvenliği konularını kapsar.

SORUMLULAR:

Başkan		**Başhekim**
Başkan Yrd.		**Kaliteden Sorumlu Diş Hekimi**
Koordinatör		**İdari ve Mali İşler Müdürü**
Raportör		**Bilgi Güvenliği Yetkilisi**
Üye		**Kalite Direktörü**

2. BİLGİ GÜVENLİĞİ

a. Verileri yetkisiz erişime, yetkisiz şekilde değiştirilmelerine, açıklanmalarına veya imha edilmelerine karşı korumak için uygun önlemleri alınır.

b. Tüm personele Merkezimiz tarafından hazırlanmış **Personel Gizlilik Sözleşmesi (DBY.YD.002**) imzalatılır.

c. Hastalarla ilgili her türlü kaydın kim tarafından, hangi tarihte girildiği, ulaşma, değiştirme bilgisi hastane bilgi işlem programı log kayıtları altında tutulmaktadır.

d. Hastaların klinik kayıtları, yalnızca konu ile ilgili yetkilendirilmiş kişinin giriş yaptığı hastane bilgi işlem programında izlenebilmektedir.

e. Veri tabanı üzerinde Hasta kayıt logları, Hasta Hizmet logları, Hasta Fatura Logları, Hasta Poliklinik logları, Tanımlama Logları, Hasta Dosya logları, Veri tabanı oturum logları, Sağlık kurulu kayıt logları kayıt altına alınmaktadır.

f. Veri tabanı yada tablolarda sisteme giriş yapan kullanıcıların gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hata logları kayıt altına alınmaktadır.

g. Kullanıcıların ara yüze bağlanmak için kullandıkları şifreler, şifreli biçimde veri tabanında saklanmaktadır. Veri tabanı, tablolara ve sistem loglarına sadece bilgi sisteminde yönetici olarak yetkilendirilmiş kişiler ulaşabilmektedir.

h. Kullanıcılar veri tabanına yapılacak müdahale (yama, güncelleme vb.) öncesinde otomasyon sistemi üzerinden bilgilendirilmektedir.

i. Hastaneye destek hizmeti veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında hastane tarafından onaylanmış gizlilik sözleşmesi mevcut olup dış ortamdan iç ortama erişimler kayıt altına alınmaktadır.

j. Her kullanıcının veri tabanında hangi bilgilere erişebileceği bilgi işlem biriminde sorumlular tarafından belirlenmektedir. Ayrıca bu kişilerin hangi yetkilere sahip olduğu HBYS üzerinden takip edilebilmekte ve rapor edilebilmektedir.

2.1. Bilgi Güvenliği Üst Yönetim Görev, Yetki ve Sorumluluklar:

1. Bilgi Güvenliği altyapısını oluşturmak için sunulacak projelere ait yönetim temsilcilerini atamak ve yetkilendirmek.

2. Sağlık Bilgi Sistemleri (SBS) tarafından hazırlanmış bilgi güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için hazırlanan projelere gerekli kaynağı sağlamak.

3. SBS tarafından hazırlanmış, Bilgi Güvenliği Politikasını onaylamak.

4. SBS tarafından hazırlanmış, Bilgi Güvenliği Faaliyet Komisyonu tarafından kabul edilmiş kontrollerin seçimlerine onay vermek.

5. Kurum bünyesinde bilgi işleme olanaklarını kullanarak bilginin üretilmesini, taşınmasını, geliştirilmesini, yönetilmesini ve saklanmasını sağlayan tüm çalışanlar (Danışmanlar ve yüklenici firma personeli dahil) Bilgi Güvenliği farkındalığının artırılmasına yönelik planlanan çalışmaların etkinliğinin artırılması için teşvik edici faaliyetleri onaylamak.

6. Bilgi Güvenliği konularında yapılacak olan çalışmalarına işlerlik kazandırmak, sürdürmek iyileştirmek ve gözden geçirmek için gerekli iç denetimlerin yapılmasına onay vermek.

7. SBS tarafından hazırlanmış Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak.

2.2. Bilgi Güvenliği Ekibi Görev, Yetki ve Sorumlulukları:

1. BG Komisyonu Yönetim tarafından oluşturulur, kurum yöneticisi tarafından onaylanır.

2. Bu komisyona ekip sorumlusu başkanlık eder.

3. Bilgi Güvenliği konularının altyapısını oluşturacak projelerin yürütülebilmesi için gerekli onayları vermek.

4. Kurumumuza bağlı birimlerde uygulanması gereken Bilgi Güvenliği politikaların geliştirilmesi için hazırlanan projelere katkı sunmak.

5. Kapsam kararları, risk değerlendirme metodolojisi, kontrollerin uygulanması konularında onay vermek ve bağlı oldukları birimlerde uygulanmasını sağlamak.

6. SBS birimi tarafından hazırlanan projelerin gerekliliği olan, birim çalışanlarının, danışmanların ve yüklenici firma personellerinin farkındalık düzeylerinin artırılmasına yönelik organize edilen çalışmaların tüm tabana yayılması için gerekli desteği vermek.

2.3. Bilgi Güvenliği Birimi Genel İşleyiş

a. Topraklık Ağız ve Diş Sağlığı Merkezi; web sayfası, Forum Sayfası ve Sosyal Medya Hesapları HBYS Birimi tarafından günlük olarak takip edilir ve güncelliği sağlanır.

b. Tüm düzeylere erişim yetkisi HBYS Birimi'ndedir.

c. HBYS tarafından sunucu hafızasındaki bilgilerin korunması, yanlış bilgi girişinin talimatlar doğrultusunda düzeltilmesi, sistemde oluşabilecek arızaların giderilmesi, süreç içinde programın alt birimlerine işlerlik kazandırılması ve talepler doğrultusunda değişiklik ve yenilik yapılması sağlanır.

d. Kurumumuzda' Bilgi Güvenliği Birimi bilgi yönetim sistemi ile ilgili durumların değerlendirilmesi, olası riskler için risk analizi yapılması ve risklerin bertaraf edilmesi ve sonuçların gözlemlenmesinden sorumludur. Risklerin bertarafı için belirtilen dönem içinde gerekli önlemler alınır. Risklerin analizi ve bertarafı için **Düzeltici Faaliyet Prosedürü** ve **Önleyici Faaliyet Prosedürü** ile belirtilen adımlar izlenerek düzeltici önleyici faaliyet başlatılır.

e. Kurumumuzda HBYS sisteminde tanımlı kullanıcıların yetki düzeyleri kayıt altına alınır.

2.4-Destek Birimi

1. Kurumumuzda bilgi yönetiminden sorumlu ekibi mevcuttur. Yazılım-Donanım Teknik Destek Ekibi, Bilgi Güvenliğinden Sorumlu İdari ve Mali İşler Müdür Yardımcısı'na bağlı olarak çalışır. HBYS yazılımının desteğini sağlayan firma personelide ekipte görev almaktadır. Yazılım-Donanım Teknik Destek Ekibindeki personeller 7/24 teknik desteğin sağlanmasıyla görevlidirler. Gerek duyulması durumunda firma yetkilileri aranarak yaşanan soruna müdahale etmeleri sağlanmaktadır. Yazılım-Donanım Teknik Destek personellerinin listesi ve gerekli iletişim bilgileri

(DBY.FR.002) **HBYS İLETİŞİM BİLGİ FORMU** dokümanında belirtilir ve bu listenin güncel hali santralde ve nöbetçi personelde bulunur.

2. Bilgi Güvenliği Birimi ve Yazılım-Donanım Teknik Destek Ekibi yetkilerin güncel durumunu izler ve gerektiğinde HBYS' deki yetkilendirmeleri yapar.

3. Bilgilerinin güncelliğini sağlar. Yetkilendirme düzeylerinde herhangi bir değişiklik olduğunda ilgili kullanıcılara yapılan değişikliklerle ilgili gerekli bilgiyi vermekle de yükümlüdür.

2.4. Dış ortamdan iç ortama erişimlerde güvenlik tedbirleri alınmaktadır:

Bu tedbirler güvenlik duvarı, anti virüs programı ve şifreleme ile sağlanır. ADSM'ye destek hizmeti veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında Merkezimiz tarafından onaylanmış (DBY.YD.003) gizlilik sözleşmesi bulunmaktadır. Kuruma destek hizmeti veren firmanın dış ortamdan iç ortama HBYS de oluşacak sistem hatalarında, kurum iş ve işleyişe özgü özel bir değişiklik yapılmasını istemesi halinde yazılım firmasının personeli bilgimiz dâhilinde bağlanmaktadır. Merkezimize HBYS yazılım firması tarafından belirlenmiş olan, Veri Tabanı ve diğer ağ bileşenlerine uzaktan erişim ile yetkili personel listesi yer almaktadır. Ayrıca Dış Ortamdan İç Ortama Erişim Formu **(DBY.FR.008)** ve yazılım firması tarafından kullanılan ve merkezimiz bilgisayarlarına kurmuş olduğu uzak bağlantı programı "NETSUPPORT" programı ile kayıt altına alınmaktadır.

Bilgi Yönetim Sisteminde kullanılabilirlik açısından gerekli düzenlemeler

Bilgi Yönetim Sisteminde kullanılabilirlik açısından gerekli düzenlemeler HBYS'de kullanılabilirlik açısından incelenebilecek unsurlardan bazıları aşağıda verilmiştir:

- Kullanım Kolaylığı
- Öğrenilebilirlik
- Verimlilik
- Hataların Azlığı
- Memnuniyet
- Esneklik
- Sekmelere Kolay Erişilebilirlik

gibi konularda talepler arıza talep- modülü kullanılarak yapılmaktadır. Ayrıca whatsapp gurubu üzerinden fikir alışverişi yapılabilmekte ve aynı yazılım firmasını kullanan ADSM ler ile de istişare edilerek sistem üzerinde kullanılabilirlik sağlanabilmektedir.

3. BİLGİ YÖNETİM SİSTEMİNE İLİŞKİN YAZILIMSAL SÜREÇLER

Bu hizmetin daha hızlı ve standartlara uygun kayıt ortamında verilebilmesi için Hastane Bilgi Yönetim Sistemi (HBYS) kullanılmaktadır. HBYS hizmeti 4734 sayılı kanun doğrultusunda satın alınmakta olup, 24 saat kesintisiz hizmet sunulmaktadır.

HBYS de oluşan sorunların çözümünde uyulması gereken kurallar:

a. Yazılım-Donanım Teknik Destek Ekibi ile telefon veya HBYS modülü üzerinden irtibat kurulmaktadır.

b. HBYS ile ilgili sorunlar ve çözümler sorunun oluştuğu tarih ve saat bildirimin yapıldığı tarih ve saat kayıt altına alınmaktadır. Bu kayıtlar HBYS modülü üzerinden izlenebilmektedir.

c. Sorunlar ile ilgili gerekli düzeltici önleyici faaliyet başlatılmaktadır.

4. SİSTEM ALT YAPISINA İLİŞKİN SÜREÇLER

4.4.1. Sahip Olma ve Sorumluluklar

a. Firma tarafından hazırlanan HBYS yazılımı sunucular vasıtasıyla sağlık tesisimizde hasta kayıt işlemi, laboratuvar tektik işlemleri, PACS işlemleri için kullanılan uç kullanıcılara(bilgisayarlara) ulaştırılmaktadır.

b. Fiziki güvenlikleri için sunucular; girişi çıkışı kontrol altında tutulan sistem odalarında muhafaza edilmektedir

c. Kurum bünyesindeki bütün dahili sunucuların yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılır.

d. Bütün sunucular (kurumun sahip olduğu) ilgili kurumun yönetim sistemine kayıtlıdır. Bu işlemde **HBYS Sunucu bilgi formu (DBY.FR.010)**kullanılarak sunucu bilgileri kayıt altına alınır. Sunuculardan ve veri tabanından sorumlu kişilerin iletişim bilgileri **HBYS İLETİŞİM BİLGİ FORMU** dokümanında bulunur.

e. Sunucu odasına Teknik Destek Ekibi dışındaki personelin girmesi yasaktır, şifreli kapıyla kontrolü sağlanır.

f. Bütün bilgiler tek bir merkezde güncel olarak tutulur.

4.4.2. Genel Konfigürasyon Kuralları

a. İşletim sistemi konfigürasyonları Kurumumuzun Bilgi Güvenliği ve Teknik Destek Ekibi'nin talimatlarına göre yapılır.

b. Kullanılmayan servisler ve uygulamalar kapatılır.

c. Servislere erişimler logların ve erişim kontrol metotlarıyla koruma sağlanır.

d. Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanır. Mümkünse, yama ve anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılır, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanır.

e. Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "roof" gibi genel kullanıcı hesapları kullanmaz, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanırlar. Genel yönetici hesapları yeniden adlandırılmıştır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yaparlar.

f. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılır.

g. Sunucular fiziksel olarak korunmuş sistem odalarında bulunur.

h. Sunucu odasının sıcaklık değeri 18-22 °C; nem değeri % 30 - % 50 arasında olmalıdır. Sunucu odasının sıcaklık nem kaydı **Isı Nem Takip Formu (SİY.FR.009)** kullanılarak, sabah ve akşam olmak üzere günde 2 defa kaydedilir.

4.4.3. Yedekleme

1. Bütün hasta kayıtları ve yedeklenmiş hasta bilgileri fiziksel olarak korunmuş mekânlarda saklanmaktadır.
2. Hasta kayıtlarının yedeklenmesi Bilgi İşlem tarafından günlük olarak yapılmaktadır.
3. Yapılan yedeklemeler Harici Hardisk kurum dışı ortamda güvenli alanlarda saklanmaktadır.
4. Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenir ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulur. (DBY.FR.025)
5. Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilerek ve güncellenir.
6. Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenir. Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilir.
7. Yedekleme ortamlarının düzenli periyotlarda test edilir ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanır.

4.4.4. Temiz Masa

Çalışma saatleri dışında bilgisayarlar Merkezimizin belirlediği saatler de otomatik olarak kapanmaktadır.

4.4.5. Kişisel Sağlık Kayıtlarının Güvenliği

a. Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mâli vb.) güvenliğinin sağlanmasına dikkat edilir.

b. Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; veri gizliliği, bütünlüğü(değiştirilmemiş olması) ve erişilebilirliğidir.

c. Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmış olup yetkisiz kişiler hastanın sağlık kayıtlarına erişmez.

d. Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar (hastanın tedavisinden sorumlu sağlık personeli) ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilir. Ancak hastanın yazılı onayı, ve yasalarca belirlenmiş görevleri yerine getiren diğer sağlık çalışanları bu veriye erişebilirler.

e. Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.

f. Hasta dosyasının bir kopyası hastaya teslim edilir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmez."

g. Hastanın rızası olmadan hiçbir çalışan yazılı veya sözlü olarak hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.

h. Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara ve kurumlara iletilemez. Hastanın kullandığı ilaçlar, diyet programlan vs. buna dahildir.

i. Hastanın dosyasının izlenmemesi için gerekli tedbirler alınır. Hasta dosyaları gelişigüzel ortada bırakılmaz, bilgisayar ekranının başkalarınca okunmaması için gerekli tedbirler alınır.

j. Telefonda konuşurken hastanın mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen gösterilir.

k. Bütün hasta sağlık kayıtları (online bilgi veya yedek medya) fiziksel olarak korunmuş mekanlarda saklanır.

l. Elektronik sağlık kayıtlarına internet ortamından erişim, ancak yetkilendirilmiş kullanıcılara güvenli erişim sağlandığında mümkün olabilir.

m. Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya kurumumuzun Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir,

n. Kurum, kritik bilgiye erişim hakkı olan çalışanlar ve firmalar ile gizlilik anlaşması imzalar.

4.4.6. İnternet Erişim ve Kullanımı

Bütün kullanıcılar ve Bilgi İşlem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkar.

a. Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkacaktır. Ağ güvenlik duvarı (firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır. Ağın dışından ağın içine erişimin denetimi burada yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlar.

b. Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılır. İstenilmeyen siteler(pornografik, oyun, kumar, şiddet içeren vs) yasaklanır.

c. Anti-virusgateaway sistemleri kullanılır. İnternete giden veya gelen bütün trafik (smtp, pop3, ayrıca mümkünse http ve ftp vs) virüslere karşı taranır.

d. İnternet erişimlerinde firewall, anti-virus, içerik kontrol vs. güvenlik kriterleri hayata geçirilmiştir.

e. Ancak Yetkilendirilmiş Sistem Yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahiptir. Bunlar; www,ftp,telnet, ping, traceroute vs.

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

g. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemesi ve dosya indirimi yapılmaz.

h. İş ile ilgili olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek yasaktır, internet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve Kurum sistemleri üzerine bu yazılımlar kurulamaz. Kurumsal işlevlere yönelik yazılım ihtiyaçları için ilgili prosedürler dahilinde ilgili Bilgi işlem sorumlularına müracaat edilmesi gerekmektedir.

i. Üçüncü şahısların kurum internetini kullanmaları Bilgi İşlem sorumlularının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.

4.4.7. E-Posta Kullanımı

a. Yasaklanmış Kullanım

b. Kurumun e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.

c. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.

d. Kurum ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğeler de dahildir.

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

f. Kişisel kullanım için internetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

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

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

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

j. Kurumda kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır. Ayrıca iş dışındaki e-postalar farklı bir klasör içerisinde saklanmalıdır.

1. **Kişisel Kullanım**

a. Kurum personeli tarafından internet ortamı aracılığı ile iletilen her türlü kişisel e-posta mesajının altında, Kurum tarafından belirlenen "gizlilik notu" ve "sorumluluk notu" bilgileri yer almalıdır. Bu bilgiler, e-posta iletisinin içeriğinden ve niteliğinden Kurum'un sorumlu tutulamayacağı gibi açıklamalar içermelidir.

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

c. Gizli ve hassas bilgi içeren elektronik postalar kriptolanarak iletilmelidir.

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

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

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

g. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

h. Elektronik postaların sık sık gözden geçirilmesi, gelen mesajların uzun süreli olarak genel elektronik posta sunucusunda bırakılmaması ve bilgisayardaki kişisel klasöre (personel folder) çekilmelidir

i. 6 ay süreyle hiç kullanılmamış e-posta adresleri kullanıcıya haber vermeden kapatılabilir.

3-Şifre Kullanımı

a. Bütün sistem seviyeli şifreler (örnek, root, administrator, enable, vs) en az üç ayda bir değiştirilmelidir.

b. Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir.

c. Tavsiye edilen değiştirme süresi her dört ayda birdir.

d. Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

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

f. SNMP kullanıldığı durumlarda varsayılan olarak gelen "public", "system" ve "private" gibi communitystring'lere farklı değerler atanmalıdır.

g. Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlar yazmaması konusunda bilgilendirilmelidir.

h. Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

i. Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır.

j. Bir kullanıcı adı ve şifresinin birim zamanda birden çok bilgisayarda kullanılmamalıdır. Bütün kullanıcı ve sistem seviyeli şifrelemeler aşağıdaki ana noktalara uymalıdır.

4-Genel Şifre Oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs.). Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

Zayıf şifreler aşağıda belirtilen karakteristiklere sahiptir.

a) Şifreler sekizden daha az karaktere sahiptirler.
b) Şifreler sözlükte bulunan bir kelimeye sahiptir.
c) Aaabbb, qwerty, zyxwuts, 123321 vs. Gibi sıralı harf veya rakamlar.
d) Yukarıdaki herhangi bir kelimenin geri yazılış şekli.
e) Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek ,gizli1, gizli2)

Güçlü şifreler aşağıdaki karakteristiklere sahiptir.

f) Küçük ve büyük karakterlere sahiptir (örnek, a-z, A-Z)
g) Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir.(0-9, !@#$%A&*()_+|~-=VÖ[]:";'<>?,/)
h) En az sekiz adet alfa nümerik karaktere sahiptir.
i) Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
j) Aile isimleri gibi kişisel bilgilere ait olmamalıdır. Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır. Kolayca hatırlanabilen şifreler oluşturulmalıdır. Örnek olarak; "olmaya devlet cihanda bir nefes sıhhat gibi" cümlesi "OdCInSg!" veya türevleri şeklinde olabilir.

i. Şifre Koruma Standartları

Kurum bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanmayınız. (örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde). Değişik sistemler için farklı şifreleme kullanın, örnek, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanınız.
Kurum bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler kuruma ait gizli bilgiler olarak düşünülmelidir.

a) Aşağıdakiler yapılmayacakların listesidir:

- Herhangi bir kişiye telefonda şifre vermek.
- E-posta mesajlarında şifre belirtmek.
- Üst yöneticinize şifreleri söylemek.
- Başkaları önünde şifreler hakkında konuşmak.
- Aile isimlerini şifre olarak kullanmak.
- Herhangi form üzerinde şifre belirtmek.
- Şifreleri aile bireyleri ile paylaşmak.
- Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirmek.

b) Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstererek Bilgi işlem birimi yetkilisini aramasını söyleyiniz.

c) Uygulamalardaki "şifre hatırlama" özelliklerini seçmeyiniz, (örnek, Outlook, Internet Explorer vs.)

d) Tekrar etmek gerekirse, şifreleri herhangi bir yere yazmayınız ve herhangi bir ortamda elektronik olarak saklamayınız.

e) Şifreler an az altı ayda bir değiştirilmelidir (sistemlerin şifreleri ise en az üç ayda bir değiştirilmelidir). Tavsiye edilen aralık ise 3 ayda birdir.

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

j.Uygulama Geliştirme Standartları

Uygulama geliştiricileri programlarında aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

a) Bireyleri(grupların değil) kimlik doğrulaması (authentication) işlemini destekleyebilmelidir.

b) Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.

c) Kural yönetim sistemini desteklemelidir, (örnek; bir kullanıcı diğer bir kimsesin şifresini bilmeden fonksiyonlarına devam edebilmesi.)

d) Mümkün olduğu kadar TACACS+,RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

k. Uzaktan Erişen Kullanıcılar için Şifre Kullanımı

Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılacaktır.

4.5. Uzaktan Erişim

Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir. 6698 sayılı Kanun'un açıklanması amacıyla KVKK tarafından yayımlanan 2018/10 sayılı karar uyarınca, özel nitelikli verilerin işlendiği, muhafaza edildiği elektronik ortamlara uzaktan erişim yapılırken, en az iki kademeli kimlik doğrulama sistemi kullanılması yasal bir zorunluluktur. Diğer sistemler için de çok faktörlü kimlik doğrulama yapılması tercih edilir.

a. Gereklilikler

1. Internet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. Veri bütünlüğünün korunması,erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.

2. Kurum çalışanları hiç bir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.

3. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.

4. Çalışanlar Kurum ile ilgili yazışmalarında Kurumun dışındaki e-posta hesaplarını (örnek, hotmail, yahoo, mynetvs) kullanamazlar.

5. Dış ortamdan iç ortama yapılan erişimlerde **Bilgi Sistemine Dışarıdan Erişim Formu**'n **(DBY.FR.008)**da kayıt altına alınmalıdır.

4.6. Kablosuz Erişim

Erişim Cihazları (Access Point) ve Kartların Kayıt Olunması Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları (örnek, PC Card) Bilgi İşlem birimi tarafından kayıt altına alınması gerekmektedir. Erişim cihazları periyodik olarak güvenlik testlerinden geçirilmelidir. Ancak Mac adresleri kayıtlı olan cihazlar Kurumun bilgisayar ağına erişebilmelidir.

a. Onaylanmış Teknoloji

Bütün kablosuz erişim cihazları Bilgi işlem güvenlik birimi tarafından onaylanmış olmalıdır ve Bilgi işlemim belirlediği güvenlik ayarlarını kullanmalıdır.

b. Güvenlik Ayarları

a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için VVi-Fi ProtectedAccess(WPA) şifreleme kullanılmalıdır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılabilmelidir.

b) Erişim cihazlarında ki firmware'leri düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.

c) Erişim cihazlarını kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü, cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.

d) Cihaza erişim için güçlü bir şifre kullanılmalıdır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır

e) SSID numaraları yayınlanmamalıdır. Böylece sniffer tarzı cihazların otomatik olarak bu numaralan çözmesi engellenecektir.

4.7. Bilgi Güvenliği İhlal Olayları

a. Bilgi güvenliği ile ilgili olaylar derhal rapor edilmelidir. Raporun verileceği ve bilgi sunulacak bölümler tabloda belirtilmiştir.

b. Kurum politikalarına uymayan her tür davranış, kurum bilgi güvenliği prensipleri ve talimatlarına aykırı her tür bilgi paylaşımı, uygunsuz PC/Laptop kullanımı, yetkisiz girişler, uygun olmayan yerde yetkisiz personelin görülmesi, bilgisayar varlıkları ile ilgili arıza, hırsızlık, kaybolma vb. olumsuzluklar bilgi güvenliği olayı kapsamına girmektedir.

c. Olay halinde müdahaleyi ilgili/yetkili birimler yaparlar. Olayı raporlayan kişinin müdahale etmemesi ve uzmanların müdahalesi için hiçbir şeye dokunmaması gerekmektedir.

4.8. Bilgi Güvenliği Zaafiyetleri

Zayıflıklar şunlardan biri olabilir: politikaya direnen kullanıcılar, işletim sistemindeki eksik yamalar, e-postalardaki spamin artması, sistemin yavaşlaması, cihazların fazla ısınması, giriş ve çıkışlarda tespit edilen yetkisiz girişe uygun alanlar ve durumlar, kapatılmayan kapılar, kilitlenmeyen dolaplar, kapatılmayan oturumlar (bilgisayarı açık bırakıp gitme), dağınık ve halka açık ortamlarda duran bilgiler ve bunun gibi konularda gözlemlenen ve Bilgi Güvenliği Komisyonunun dikkatinden kaçan konular.

4.9. İnsan Kaynakları Ve Zafiyetleri Yönetimi

a. Çalışan personele ait hsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.

b. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilir.

c. ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.

d. Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir

e. İmha edilmesi gereken (müsvedde halini almış yada iptal edilmiş yazılar vb.) kağıt kesme makinesinde imha edilmelidir.

f. Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

g. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.

h. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

i. Personel görevden ayrıldığında yetkisinde bulunan EBYS, ÇKYS, Mail adresi, Bilgisayar şifreleri HBYS Birimi tarafından teslim alınarak, ilişik kesme belgesinde yetkilerinin iptal edildiğine dair imza altına alınır.

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

5. Bilgi Kaynakları Atık Ve İmha Yönetimi

a. Evraklar idari ve hukuki hükümlere göre belirlenmiş evraklar , Arşiv Birimi tarafından muhafaza edilir.

b. Evrakların yasal bekleme süreleri sonunda tasfiyeleri sağlanır. Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınır ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.

c. 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 gerçekleştirilir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilir.

d. İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenir.

e. Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi SBS tarafından temin edilir.

f. Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenir.

g. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılır ve hacimsel küçültme işlemi için parçalanır.

h. Son ürünler gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilir.

i. Çıkan metaller sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilir.

j. Yukarıda maddelinmiş tüm bu iş ve işlemler Arşiv İşleyiş Prosedürü doğrultusunda gerçekleştirilir.

6. Mal Ve Hizmet Alımları Güvenliği

a. Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilir.

b. Üçüncü taraflarla yapılan anlaşmalarda üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.

c. Mal ve hizmet alımının özelliğine göre gizlilik ve ya ifşa etmeme sözleşmeleri imzalanması gerekebilir.

d. Gizlilik ve ifşa etmeme anlaşmaları Merkezimizin ihtiyaçları doğrultusunda farklı şekillerde kullanılabilir.

e. Gizlilik veya ifşa etmeme anlaşmalarında aşağıda yer alan bilgilerin yer alması sağlanır. Bunlar;

f. Korunacak bilginin bir tanımı (örneğin; gizli bilgileri)

g. Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dahil olmak üzere anlaşma süresi,

h. Anlaşma sona erdiğinde yapılması gereken eylemler,

i. Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi (‘bilmesi gereken’ gibi),

j. Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiği,

k. Gizli bilgilerin kullanım izni ve bilgileri kullanmak için imza hakları,

l. Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,

m. Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesinin bildirimi ve raporlama prosesi,

n. İade veya imha anlaşmasına bırakılacak bilgi için terimler.

o. Bu anlaşmanın ihlali durumunda yapılması beklenen eylemler.

p. Yukarıda maddelinmiş tüm bu iş ve işlemler Satın alma Prosedürü kapsamında gerçekleştirilir.

7. Sosyal Mühendislik Zafiyetleri

a. Merkezimizde sosyal mühendislik zafiyetlerinin önlenebilmesi için sosyal medya içerikli web sayfalarına giriş yapılmasına izin verilmemektedir. Sosyal Medya içerikli web sayfaları firewall ile engellenmiş olup, loglaması yapılmaktadır.

b. Çalışanlar tarafından; özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgiler paylaşılmaz.

c. Şifre kişiye özel bilgidir. Sistem yöneticisi dahil telefonda veya e-posta ile şifre paylaşılmaz.

d. Kazaa, emule gibi dosya paylaşım yazılımlarının kullanımı yasaklanmış olup, firewall ile engellenmiştir.

8. Sosyal Medya Güvenliği

a. Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olacak şekilde bilgi işlem birimi tarafından oluşturulur. Sosyal medya hesapları bilgi işlem personeli tarafından takip ve kontrol edilir.

b. Kurum içi bilgiler sosyal medyada paylaşılması yasaklanmıştır.

c. Kuruma ait gizli bilgi veya yazının sosyal medyada paylaşılması yasaklanmıştır.

9. Gizlilik Sözleşmesi Ve Bg Disiplin

a. BGYS gerekliliklerine uyulmaması tespit edildiği durumlarda tutanak tutularak üst yönetime havale edilir.

b. Disiplin Prosedürünü Merkezimiz ve üst yönetim yürütecektir.

c. Merkezimizde bulunan donanımlar Kurumumuzun malı olup bunlara verilecek zararlar kanun nezdinde suç teşkil eder. Donanımın dış görünüşünü değiştirmek, bağlı parçaların bağlantı şeklini değiştirmek, parçaları çalmak veya çalmaya teşebbüs etmek. Bu tür durumlar gerçekleştiğinde yetkili birim ve kişiler tarafından tutanak tutulur, disiplin soruşturması açılır. Ek olarak kullanıcı hesabı süresiz kapatılır. Kurum söz konusu davranışlarda bulunan kişiler hakkında yetkili makamlara şikayette bulunur.

d. Disk alanında zararlı dosyalar bulundurulması durumunda kullanıcı hesabı süresiz kapatılır ve dosyalar silinir.

e. Başkalarının alanlarına erişilmesi durumunda kullanıcı hesabı süresiz kapatılır, kanuni süreç başlatılır, disiplin soruşturması açılır.

f. Her türlü kişisel şifreyi paylaşmak disiplin soruşturması gerektirir. Şifresini paylaşan her türlü sorumluluğu kabul etmiş sayılır.

g. Başkasının e-posta hesabını kullanılması durumunda kullanıcı hesabı süresiz kapatılır.

h. Hakaret içerikli e-posta gönderilmesi durumunda kullanıcı hesabı süresiz kapatılır, kanuni süreç başlatılır, disiplin soruşturması açılır.

i. Kurum tarafından sağlanan e-posta hizmeti kullanılarak devlet sırrı niteliğindeki her türlü bilgi ve evrak, Knowhow üçüncü şahıslarla paylaşılması durumunda kanuni girişimlerde bulunulur ve disiplin prosesi başlatılır.

j. Bunun dışındaki kural ihlallerinde en fazla iki uyarı yapılır. Tekrarlanması durumunda disiplin soruşturması açılır.

k. Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Bilgi Güvenliği Birimi bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa yasa uygulayıcı ile işbirliği yapar.

l. Kullanım Politikasını kabul eden taraf, yukarıdaki maddelerde belirlenen kurallara uygun kullanımının, kullanıcının kişilik hakları saklı kalmak üzere, kontrol edebileceğinden haberdardır ve bunu açıkça kabul eder. Kullanıcı, sorun yaratan herhangi bir olayın farkına varması üzerine, güvenliği sağlamak için acil önlemler alabileceğini kabul eder. Ancak bu önlemler, belirtilen durum genel ağ işleyişini ve güvenliğini etkilemediği sürece, ilgili kişi veya birim ile iletişim kurulduktan ve belli bir süre tanındıktan sonra alınacaktır.

m. Kullanıcıların, kurum bünyesinde çalışmaya başladığı zaman Personel Gizlilik Sözleşmesini imzalar, sözleşmede yazan tüm hususlara uymayı taahhüt ve kabul eder. Edilmediği takdirde iş bu disiplin prosedürü usullerine göre hareket edilir.

n. Kurum hizmet aldığı yüklenicilerle de Kurumsal Gizlilik Sözleşmesi imzalar.

10.Yaptırım

10.1 Yukarıda sayılan kurallardan biri ya da birkaçının ihlâlinin tespit edilmesi halinde, güvenlik ihlâline yol açan personel hakkında işlem başlatılır.

10.2 Yapılan ihlalin ilgili kanunlar gereği suç ve ceza öngören bir fiil olması halinde, ilgili personel hakkında suç duyurusunda bulunulur.

10.3 Ayrıca idari bir tedbir olarak, yapılan ihlalin 10.2 maddesinde belirtildiği şekilde suç olup olmadığına bakılmaksızın, Kurum tarafından ihtiyaç duyulması halinde; 657 Sayılı Devlet Memurları Kanunu'na tabi olanlar için aynı Kanun'un 125'inci maddesinde sayılan hükümlere göre, 657 Sayılı Devlet Memurları Kanunu'nun dışında kalan çalışanlar ile ilgili olarak (danışmanlar, firma personeli vb.) sözleşmelerinde belirtilen özel hükümlere göre, yoksa genel hükümlere göre idari işlem tesis edilir.

11.İlgili Doküman

- **Personel Gizlilik Sözleşmesi (DBY.YD.002)**
- **HBYS iletişim bilgi formu (DBY.FR.002)**
- **Kurumsal gizlilik sözleşmesi (DBY.YD.003)**
- **Dış Ortamdan İç Ortama Erişim Formu (DBY.FR.008)**
- **HBYS Sunucu bilgi formu (DBY.FR.010)**
- **Isı Nem Takip Formu (SİY.FR.009)**
- **Yedekleme kontrol formu (DBY.FR.025)**