2015

Bilgi Güvenliği Politikası

ÇANKIRI İL SAĞLIK MÜDÜRLÜĞÜ

İÇİNDEKİLER

BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU

T.C. Sağlık Bakanlığı Çankırı İl Sağlık Müdürlüğü bünyesinde Bilgi Güvenliği Politikalar Yönergesi gerekliliklerini yürütmek üzere Bilgi Güvenliği Faaliyet Komisyonu kurulmuştur. Komisyon aşağıda yazılı isimlerden oluşmaktadır;

1. BG Üst Yönetim Görev, Yetki ve Sorumluluklar:

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

1.2. SBS tarafından hazırlanmış bilgi güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için hazırlanan projelere gerekli kaynağı sağlamak.

1.3. SBS tarafından hazırlanmış, Bilgi Güvenliği Faaliyet Komisyonu tarafından kabul edilmiş Bilgi Güvenliği Politikasını onaylamak.

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

1.5. 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.

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

1.7. SBS tarafından hazırlanmış, Bilgi Güvenliği Faaliyet Komisyonu tarafından kabul edilen Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak.

2. BG Faaliyet Komisyonu Görev, Yetki ve Sorumlulukları:

2.1. BG Komisyonu BG Yönetim Temsilcisi tarafından oluşturulur, kurum yöneticisi tarafından onaylanır.

2.2. BG Yönetim Temsilcisi bu komisyona başkanlık eder.

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

2.4. Sağlık Müdürlüğüne bağlı birimlerde uygulanması gereken Bilgi Güvenliği politikaların geliştirilmesi için hazırlanan projelere katkı sunmak.

2.5. BG yönetim temsilcisi ve SBS birimi tarafından gerekli görüldüğünde toplantılara

katılmak.

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

2.7. 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.

3. BİLGİ GÜVENLİĞİ GENEL İŞLEYİŞ

3.1. Çankırı İl Sağlık Müdürlüğünün web sayfası, Forum Sayfası ve Sosyal Medya Hesapları SBS kontrolünde Bilgi İşlem Teknik Personeli tarafından günlük olarak takip edilir ve güncelliği sağlanır.

3.2. Tüm düzeylere erişim yetkisi SBS 'dedir.

3.3. SBS 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.

4. PAROLA GÜVENLİĞİ

4.1. Çankırı İl Sağlık Müdürlüğü bağlı birim ve kurumlarda parola sistemi aşağıdaki unsurları içeren standartlarda olmalıdır.

4.2. Parola en az 8 karakterden oluşmalıdır.

4.3. Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içermelidir.

4.4. Büyük ve küçük harfler bir arada kullanılmalıdır.

4.5. Bu kurallara uygun parola oluştururken, aynı zamanda saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.

4.6. Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, qwerty, doğum tarihi, soyadı gibi)

4.7. Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.

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

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

Örn;

’B’ yerine 8	’Z’ yerine 2	Örneğin Balıkçıl-Kazak 8a11kç11-Ka2ak Solaryum! 501aryum!
’1’, ’i’, ’L’, ’l’ yerine 1	’O’ harfi yerine 0	
’S’ yerine 5 ’G’ yerine 6	’g’ yerine 9	

4.10. İşe yeni başlayan personele, kullanacağı bilgisayar, program vb. şifreler kapalı zarf içerisinde Sağlık Bilgi Sistemleri Birimi tarafından zimmet ile teslim edilir.

4.11. Personel işten ayrılacağı zaman Müdürlük bünyesinde kullandığı şifreleri Sağlık Bilgi Sistemleri Birimi tarafından iptal edilir yada kullanım dışı bırakılır.

4.12. Kullanılan tüm şifreler ilgili personel tarafından 6 aylık periyotlar halinde değiştirilir.

4.13. İl Sağlık Müdürlüğümüze ait bilgisayar ve programların şifreleri ……. Şifre Envanter Formu ile şifreli bir şekilde Sağlık Bilgi Sistemleri Biriminde muhafaza edilir.

5. TEMİZ MASA

5.1. Çalışma saatleri dışında bilgisayarlar kapalı ya da kilitli şekilde bırakılmalıdır. Çalışma saatleri içerisinde başından ayrıldığında mutlaka bilgisayar kilitli bırakılmalıdır.(Ekran koruyucu 5-10 dk arasında devreye girmelidir ve şifre koruması olmalıdır.)

5.2. Kuruma ait dokümante edilmiş gizli bilgiler kilitli ortamda tutulmalıdır.

5.3. Gizlilik dereceli evraklar, işlevini tamamladıktan sonra imha edilirler.

5.4. Gelen ve giden mesaj noktaları ve faks veya teleks makineleri başıboş olarak bırakılmaz.

5.5. Kuruma ait antetli kağıtlar kilitli dolaplarda tutulmalıdır.

5.6. Hassas ve sınıflandırılmış bilgi basıldığında yazıcıdan hemen temizlenir.

5.7. Bilgisayarların masaüstlerinde kuruma ait özel bilgiler içeren dokümanlar bulundurulmamalıdır.

5.8. Bilgisayarlara ait olan şifreler kesinlikle kâğıt ortamlara yazılı bir şekilde bırakılmamalı.

6. E-POSTA GÜVENLİĞİ

6.1. Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.

6.2. İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.

6.3. Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.

6.4. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.

6.5. Internet 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 e-posta adresi kullanılabilir.

6.6. Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e- posta adresini yazamaz.

6.7. Personel KONU alanı boş bir e-posta mesajı göndermemelidir.

6.8. KONU alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.

6.9. E-postaya eklenecek dosya uzantıları ".exe", ".vbs" veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip ve/ya rar formatında) mesaja eklenecektir.

6.10. Bakanlık ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

6.11. Kullanıcı, Kurumun e-posta sistemi üzerinden taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.

6.12. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.

6.13. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Sistem Yönetimine haber verilmelidir.

6.14. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt verilmemelidir.

6.15. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

6.16. 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.

6.17. Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.

6.18. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.

6.19. Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

6.20. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Sistem Yönetimine haber verilmelidir.

6.21. 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.

7. BİLGİ GÜVENLİĞİ İHLAL OLAYLARI

Çankırı İl Sağlık Müdürlüğü 'nde Bilgi Güvenliği İhlal Olayları aşağıdaki gibi yönetilmektedir;

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

7.2. 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.

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

OLAY TANIMI	YETKİLİ KİŞİ/BİRİM	İLETİŞİM BİLGİLERİ
Her türlü bilgi güvenliği ihlal olayları durumunda	Emin Alper KAYA /Sağlık Bilgi Sistemleri Birimi	0553 612 52 42 0376 213 10 61 / 1017-1054
Virüs, izinsiz giriş, trojan, spyware vb. bulgular için, sistem sunucu	Emin Alper KAYA /Sağlık Bilgi Sistemleri Birimi	553 612 52 42 0376 213 10 61 / 1017-1054
Donanım arızaları, network problemleri için	Emin Alper KAYA /Sağlık Bilgi Sistemleri Birimi	553 612 52 42 0376 213 10 61 / 1017-1054
Veri kaybı, bilgilere yetkisiz erişim durumlarında	Emin Alper KAYA /Sağlık Bilgi Sistemleri Birimi	553 612 52 42 0376 213 10 61 / 1017-1054
Hırsızlık, kaybolma, yanma, kırılma vb. durumlar için	Emin Alper KAYA /Sağlık Bilgi Sistemleri Birimi	553 612 52 42 0376 213 10 61 / 1017-1054
Uygunsuz davranışlar ve politikaya uymayan kişiler için	Emin Alper KAYA /Sağlık Bilgi Sistemleri Birimi	553 612 52 42 0376 213 10 61 / 1017-1054
Ağ üzerinden Saldırı	Emin Alper KAYA /Sağlık Bilgi Sistemleri Birimi	553 612 52 42 0376 213 10 61 / 1017-1054

7.4. Zayıflıkların tespiti durumunda önlem alınması için İl Sağlık Müdürlüğü web sayfası iletişim linki altında yer alan Bilgi Güvenliği (İhlal Bildirimi) formu internet ortamında düzenlenerek, Sağlık Bilgi Sistemleri Biriminin bilgi sahibi olması sağlanır.

7.5. Zayıflıklar şunlardan biri olabilir: politikaya direnen kullanıcılar, işletim sistemindeki eksik yamalar, epostalardaki 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.

8. İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ

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

8.2. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilir.

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

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

9. BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ

9.1. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak Arşiv Birimi tarafından muhafaza edilir.

9.2. 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.

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

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

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

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

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

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

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

9.10. Yukarıda maddelenmiş tüm bu iş ve işlemler CSM.YÖN.PR.015 Arşiv İşleyiş Prosedürü doğrultusunda gerçekleştirilir.

10. MAL VE HİZMET ALIMLARI GÜVENLİĞİ

10.1. 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.

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

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

10.4. Gizlilik ve ifşa etmeme anlaşmaları Çankırı İl Sağlık Müdürlüğü 'nün ihtiyaçları doğrultusunda farklı şekillerde kullanılabilir.

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

10.6. Korunacak bilginin bir tanımı (örneğin; gizli bilgileri),

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

10.8. Anlaşma sona erdiğinde yapılması gereken eylemler,

10.9. Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi ('bilmesi gereken' gibi),

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

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

10.12. Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,

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

10.14. İade veya imha anlaşmasına bırakılacak bilgi için terimler,

10.15. Bu anlaşmanın ihlali durumunda yapılması beklenen eylemler.

10.16. Yukarıda maddelenmiş tüm bu iş ve işlemler CSM.YÖN.PR.003 Satınalma Prosedürü kapsamında gerçekleştirilir.

11. SOSYAL MÜHENDİSLİK ZAFİYETLERİ

11.1. Müdürlük ve bağlı sağlık kuruluşlarında 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.

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

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

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

12. SOSYAL MEDYA GÜVENLİĞİ

12.1. 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.

12.2. Kurum içi bilgiler sosyal medyada paylaşılması yasaklanmıştır.

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

13. GİZLİLİK SÖZLEŞMESİ VE BG DİSİPLİN

13.1. T.C. Sağlık Bakanlığı Çankırı İl Sağlık Müdürlüğü kapsamı dahilinde uygulanan Bilgi Güvenliği Yönetim Sistemi dokümantasyonu gerekliliklerine aykırı davranılması durumunda başta 657 Sayılı Devlet Memurları Kanunu Disiplin hükümlerine göre ve yaşanan olayın durumuna göre ilgili kanun ve yönetmeliklere göre hareket edilecektir.

13.2. 657 Sayılı Devlet Memurları Kanununa tabi olanlar aynı kanunun 125 maddesinde sayılan hükümlere göre değerlendirilecek olup 657 Sayılı Devlet Memurları Kanununun dışında kalan çalışanlar (Danışmanlar, Firma Personelleri) sözleşmelerinde belirtilen özel hükümlere göre, yoksa genel hukuk kuralları çerçevesinde hareket edilecektir.

13.3. BGYS gerekliliklerine uyulmaması tespit edildiği durumlarda tutanak tutularak T.C.Sağlık Bakanlığı Çankırı İl Sağlık Müdürlüğü Bilgi Güvenliği Komisyonuna havale edilir.

13.4. Disiplin Prosedürünü T.C. Sağlık Bakanlığı Çankırı İl Sağlık Müdürlüğü Bilgi Güvenliği Komisyonu ve üst yönetim yürütecektir.

13.5. T.C. Sağlık Bakanlığı Çankırı İl Sağlık Müdürlüğünde bulunan donanımlar Çankırı İl Sağlık Müdürlüğünün 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.

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

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

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

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

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

13.11. 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.

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

13.13. 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.

13.14. Kullanım Politikasını kabul eden taraf, T.C. Sağlık Bakanlığı Çankırı İl Sağlık Müdürlüğü 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.

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

13.16. Kurum hizmet aldığı yüklenicilerle de **BG.SZ.. Kurumsal Gizlilik Sözleşmesi** imzalar.

13.17. Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, 657 Devlet Memurları Kanunun 125 Maddesinde yer alan hükümler uygulanacaktır.

13.18. 657 Devlet Memurları Kanun hükümlerine tabi olmayan personelin (Danışmanlar, Firma Personelleri) kurumla aralarındaki sözleşmelerde yer alan hükümler uygulanacaktır aksi durumda genel hukuk kurallarına tabi olacaktır.

14. YAPTIRIM

14.1. Kurumsal Bilgi Güvenlik Talimatları ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla **BG Disiplin Prosedürü** Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.