BGYS politikası, T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır.

1. AMAÇ

Bakanlığımız, T.C. Anayasası ve kanunlar çerçevesinde yürütmekte olduğu iş ve işlemlerin işleyen süreçlerinde ülke nüfusunun tamamı ile ilgili olan sağlık ve tüm alt unsurları ile ilgili olarak doğum öncesinden ölüme kadar olan tüm süreçlerde çalışmakla yükümlendirilmiş bir kurum olma hüviyeti ile ülkedeki her bir vatandaşa karşı sorumlulukları olan kuruluşlardan birisidir. Her bir vatandaşın sağlık kuruluşuna müracaat ettiğinde en gizli ve mahrem sayılabilecek bilgilerine dair erişebilen kaydedebilen yegâne kuruluştur.

T.C. Sağlık Bakanlığı hasta sıfatı ile bir bireyle muhatap olduğunda ve bireyin herhangi bir verisini ve bilgisini kayıt altına aldığında, kayıt altına alınan bireye ait her türlü veri ve bilginin kendisine emanet edilmiş bir değer olduğu düşüncesiyle kendisini bu sorumluluğun yerine getirilmesinde mükellef olarak görmektedir.

T.C. Sağlık Bakanlığı kişi verilerinin ve bilgilerinin korunması ve güvenliği ile alakalı her türlü “teknik idari ve hukuki yöntemi” kullanmak sureti ile emanetinde bulunan tüm bilgi sistemleri kaynaklarını “bilgi güvenliği ana politikası çerçevesinde” korumakla ve bu hususta tüm tedbirleri almakla yükümlü olduğunun bilincindedir.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuyu da kapsar.

Bilgi güvenliği bilinçlendirme süreci kurum içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir. Kurum çalışanları, yüklenici firma personeli, yarı zamanlı personel, stajyerler, diğer kurum çalışanları, ziyaretçiler, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girmektedir. Kullanıcılar, bilgi güvenliği bilinçlendirme sürecindeki en büyük ve önemli hedef kitledir. Kurum içindeki işler yürütülürken istemeden yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek onların elindedir. Yöneticiler, bilgi güvenliği bilinçlendirme ve eğitimi sürecinin gereklerine personelinin uymasını sağlamakla sorumludurlar.

Sağlık sektöründe güncel teknolojinin hissedilir şekilde kullanılmasıyla birlikte teknolojinin taşıdığı bazı risklerle de yüz yüze gelinmiştir. Elektronik ortamdaki tüm veriler gibi, kişisel sağlık bilgilerini tehdit eden riskler için güvenlik önlemlerinin alınması zorunlu hale gelmiştir. Kişisel sağlık bilgileri, kişinin doğum öncesinden ölüm sonrasına kadar geçen süreyi kapsayan sağlık bilgilerinin tümüdür. Sağlık kayıtlarının sayısallaştırılması etkin sağlık hizmeti için yadsınamayan ciddi bir hamledir. Güncel teknolojilerin kişisel sağlık bilgilerinin gizlilik, bütünlük ve erişilebilirlik risklerini artırmasından dolayı sağlık bilgilerinin güvenliği zedelenmektedir. Kişisel sağlık bilgilerinin mahremiyeti esastır. Bu nedenle önlemlerin alınması, risklerin saptanıp indirgenmesi zorunlu hale gelmiştir.

2. KAPSAM

Rize İl Sağlık Müdürlüğü, bilgi güvenliği kapsamında yer alan basılı ve elektronik ortamdaki tüm bilgilerin, yasal mevzuat ışığında ve risk değerlendirme metotları kullanılarak “gizlilik, bütünlük ve erişilebilirlik” ilkelerine göre yönetilmesi amacıyla;

Bilgi güvenliği standartlarının gerekliliklerini yerine getirmek,

Bilgi güvenliği ile ilgili tüm yasal mevzuata uyum sağlamak,

Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,

Bilgi güvenliği yönetim sistemini sürekli gözden geçirmek ve iyileştirmek,

Bilgi güvenliği farkındalığını artırmak için teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmek vizyon ve misyonuyla hareket etmektedir.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iş olduğu gibi, sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine; iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine kadar birçok konuyu da kapsar.

Bilgi güvenliği bilinçlendirme süreci, kurum içinde en üst seviyeden en alt seviyeye kadar tüm çalışanların katılımını gerektirir. Kurum çalışanları, yüklenici firma personeli, yarı zamanlı personel, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girer.

3. TANIMLAR VE KISALTMALAR

BGYS: Bilgi Güvenliği Yönetim Sistemi

BTHYS: Bilgi Teknolojileri Hizmet Yönetim Standardı

Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar.

Bilgi güvenliği ihlal olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

Bilgi güvenliği yönetim sistemi (BGYS) : Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir.

Bilgi Güvenliği Riski: Açıklıklardan fayda sağlamak suretiyle kuruluşa zarar verebilecek varlık ya da varlık gruplarının potansiyel tehdidi dir. Bir olayın ve sonucunun olasılığının kombinasyon koşulları olarak ölçülür.

Risk Yönetimi: Bilgi güvenliği risklerinin analizi, değerlendirilmesi, işlenmesi ve sürekli iyileştirilmesi amacıyla yürütülen yönetimsel faaliyetler.

Risk Analizi: Tehdit ve iş etkisinin çarpımı olan risk puanının bulunması amacıyla her bir bilgi varlığı için zayıflıkların, tehditlerin, iş etkilerinin bulunması ve hesaplanması çalışması.

Risk Değerlendirme: Risk analizi sonucu bulunan değerlerin yorumlanması ve derecelendirilmesi.

Riskin Kabulü/Kabul edilebilir Risk: Bir riski kabul etme kararı. Bir riskin zararını (negatif sonuçlarını) kabullenme.

Bilgi Güvenliği Riski: Açıklıklardan fayda sağlamak suretiyle kuruluşa zarar verebilecek varlık ya da varlık gruplarının potansiyel tehdidi dir. Bir olayın ve sonucun olasılığının kombinasyon koşulları olarak ölçülür.

Riskten Kaçınma: Riski oluşturan durumdan kaçınma.

Risk İletimi: Karar verici veya diğer ortaklar arasında risk hakkındaki bilgiyi paylaşım ya da değişimdir.

Riski Belirleme: Riski oluşturan öğelerin ortaya çıkartılması, tasnif edilmesi ve özelliklerin belirlenmesini içeren süreçtir.

YGG: Yönetimin Gözden Geçirilmesi

PUKÖ: Planla, Uygula, Kontrol Et, Önlem Al

4. BİLGİ GÜVENLİĞİ HEDEFLERİ VE PRENSİPLERİ

Rize İl Sağlık Müdürlüğü Bilgi Güvenliği Politikasının hedefleri; bilgi varlıklarını korumak, bilginin ve verinin gizliliğini sağlamak, bütünlüğünü bozmaya çalışacak yetkisiz kişilerin erişimini engellemek, ihtiyaç duyulan her alanda bilgiyi erişilebilir halde tutmak ve böylece Sağlık Bakanlığının güvenini ve itibarını sarsacak durumları bertaraf etmektir.

5. BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU

BGYS TAKIMI VE YETKİLERİ

Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü bünyesinde bu politika metninde tarif edilen kapsam dahilinde TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerini yürütmek üzere BGYS Komisyonu, BGYS Çalışma Grubu ve Bilişim Teknik Destek Alt Çalışma Grubu kurulmuştur

BG Üst Yönetim Görev, Yetki ve Sorumluluklar:

- Bilgi Güvenliği altyapısını oluşturmak için sunulacak projelere ait yönetim temsilcilerini atamak ve yetkilendirmek.
- Bilgi güvenliği yetkilisi ve/veya çalışma grubu tarafından hazırlanmış komisyon tarafından onay verilmiş bilgi güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için hazırlanan projelere gerekli kaynağı sağlamak.
-

- BGYS yetkilisi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş Bilgi Güvenliği Politikasını onaylamak.
- BGYS yetkilisi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş kontrollerin seçimlerine onay vermek.
- Belirli aralıklarla yapılacak olan BGYS YGG (Bilgi Güvenliği Yönetim Sistemi Yönetim Gözden Geçirme) toplantılarına başkanlık etmek.
- Kurum bünyesinde bilgi işleme olanaklarını kullanarak bilginin üretilmesini, taşınmasını, geliştirilmesini, yönetilmesini ve saklanmasını sağlayan tüm çalışanlar (firma personeli dahil) Bilgi Güvenliği farkındalığının artırılmasına yönelik planlanan çalışmaların etkinliğinin artırılması için teşvik edici faaliyetleri onaylamak.
- Bilgi Güvenliği konularında yapılacak olan çalışmalarına işlerlik kazandırmak, sürdürmek iyileştirmek ve gözden geçirmek için gerekli iç denetimlerin yapılmasına onay vermek.
- BGYS yetkilisi tarafından hazırlanmış, BGYS Komisyonu tarafından kabul edilen Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak.

BGYS Komisyon Başkanı Görev, Yetki ve Sorumlulukları:

- Bilgi Güvenliği konularının altyapısını oluşturacak projeler hazırlanmasını sağlamak.
- Çalışmaların yürütülebilmesi için gerekli komisyonları, çalışma gruplarını oluşturmak ve görev tanımlarını yapmak.
- BGYS Komisyonuna başkanlık etmek.
- BGYS Biriminden, BGYS Komisyonundan ve Çalışma Grubundan gelen istek ve talepleri değerlendirmek Projelerin dayandırıldığı standartlar çerçevesinde onay vermek.
- BGYS Biriminden, BGYS Komisyonundan ve Çalışma Grubundan gelen istek ve talepleri değerlendirmek Projelerin dayandırıldığı standartlar çerçevesinde onay vermek.
- Yönetim Sistemi dokümantasyonlarının hazırlanmasına rehberlik etmek ve hazırlanan dokümanları onaylamak.
- Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak.
- Yönetim Sistemi dokümantasyonlarının hazırlanmasına rehberlik etmek ve hazırlanan dokümanları onaylamak.
- Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak.
- Projelerin yürütülebilmesi için gerekli olan yönetim hizmetleri çerçevesinde ihtiyaçların temin edilmesinin sağlanması.
- Yapılan çalışmalarla ilgili üst yönetime ve BGYS Komisyonuna rapor sunmak ve bilgilendirme toplantıları düzenlemek.
- Yönetim sistemi gerekliliklerinden olan Yönetim Gözden Geçirme, İç Denetim, Farkındalık Eğitimleri gibi faaliyetlerin gerçekleşmesini sağlamak.

BGYS Yetkilisi Görev ve Sorumlulukları:

- Bilgi Güvenliği altyapısını oluşturacak projeler hazırlanmasına katkı sunmak.
- Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde uygulanması gereken Bilgi Güvenliği politikaların geliştirilmesi için gerekli araştırmaları yapmak ve çalışma grubuna katkı sunmak.
- Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde yapılacak olan çalışmalarda gerekli iletişim organizasyonu için gerekli düzenlemeleri yapmak.
- Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standartlar seviyesinde bir hizmet kalitesini yakalamak amacıyla TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, TS ISO/IEC 20000 Bilgi Teknolojileri Hizmet Standardı gibi standartlar Kurumsal Bilgi Güvenliği Mimarisi gibi konuların gerekliklerinin yerine getirilmesi için yapılan çalışmalara katkı sunmak.
- BGYS Üst Yönetim, Komisyon ve Çalışma Grubu ile planlanan ve yürütülen çalışmalara katkı sunmak ve rehberlik etmek.
- Projelerin yürütülebilmesi için gerekli olan tüm dokümantasyon (Politika, Prosedür, Plan, Süreç Analizi, Risk Yönetimi, Etki Analizi gibi) gerekliliklerine katılmak, dokümantasyon geliştirme faaliyetlerinde yer almak.
- Hazırlanan dokümantasyonun yönetim temsilcisi ve (gerekli olanların) üst yönetim tarafından onaylanmasını sağlamak.
- Projelerin yürütülebilmesi için gerektiğinde, komisyon toplantısı, çalışma grupları toplantısı, sağlık tesisleri ziyaretleri gibi çalışmaların organize edilmesi, yasal izinlerin, araç izinlerinin alınması gibi hususlarda gerekli organizasyonları yapar.
- Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde yapılacak olan çalışmaların proje planlarının hazırlanması, gerekli bilgilendirme raporları, sunumları ve eğitimlerin organize edilmesi ve gerçekleştirilmesi konularında rehberlik etmek ve katkı sunmak.
-

- Projelerin yürütülebilmesi için gerekli olan tüm dokümantasyon (Politika, Prosedür, Plan, Süreç Analizi, Risk Yönetimi, Etki Analizi gibi) gerekliliklerini yerine getirme hususunda çalışmalara katılmak hazırlanan dokümantasyonun ilgili taraflar tarafından okunmasını ve anlaşılmasını sağlamak.

- Projeler kapsamında yapılacak olan farkındalık eğitimi, temel eğitim, eğitim değerlendirmeleri yapmak, katılımcı imzalarının alınmasını sağlamak.

- Yönetim sistemi gerekliliklerinden olan Yönetim Gözden Geçirme, İç Denetim, Farkındalık Eğitimleri gibi faaliyetlerin zamanında ve efektif bir şekilde gerçekleştirilmesi için gerekli planlamaların gerçekleşmesini sağlamak.

BGYS Komisyonu Görev, Yetki ve Sorumluluklar:

- BGYS Komisyonu BGYS Yönetim Temsilcisi tarafından oluşturulur, kurum yöneticisi tarafından onaylanır.
- Bilgi Güvenliği konularının altyapısını oluşturacak projelerin yürütülebilmesi için gerekli onay vermek.

- Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde Bilgi Güvenliği politikaların geliştirilmesi için hazırlanan projelere katkı sunmak.

- BGYS yönetim temsilcisi ve BGYS yetkilisi tarafından gerekli görüldüğünde toplantılara katılmak.

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

BGYS Çalışma Grubu, Yetki ve Sorumluluklar:

- BGYS çalışma grupları BGYS Yönetim Temsilcisi tarafından oluşturulur, BGYS Komisyonu kabul eder ve üst yönetim onaylar.

- BGYS Yetkilisi ve Yönetim Temsilcisi tarafından planlanan çalışmalara katılmak.

- BGYS Yetkilisine ve Yönetim temsilcisine karşı sorumludurlar.

- Planlanan çalışmalara BGYS Yetkilisi, BGYS Yönetim Temsilcisi istekleri paralelinde katkı sunmak.

- Yürütülen çalışmaların tabana yayılması hususunda planlanan çalışmalara katılmak bağlı oldukları birimlerde bu çalışmaların yayılmasına öncülük etmek.

6. BGYS YGG (BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNETİM GÖZDEN GEÇİRME) TOPLANTILARI

BGYS biriminin ve üst yönetimin bilgi güvenliğinin uygunluğunu, verimliliğini, risk yönetiminin işlevselliğini, tetkik sonuçlarını, düzeltici ve önleyici faaliyetleri ele aldığı en az üç ayda bir düzenlenen bir toplantıdır. Bu toplantıda yönetim risk kabul kriterlerini ve kaynak ihtiyaçlarını değerlendirir. Çalışmaların, risk değerlendirme ve işleme faaliyetlerinin verimliliğini inceler.

Bu toplantılarda standarda göre girdi ve çıktılar Toplantı Tutanağı Formu kullanılarak kayıt altına alınmaktadır.

6.1. Bilgi Varlıklarımız

T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü kapsam dahilinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları işlerde üretilen bilgiler bilgi varlıklarımızı oluşturmaktadır.

Masaüstü bilgisayarlar, laptoplar, CD ve DVD ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (internet, email, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

6.2. Varlık Sınıflandırılması

Bilgi Sınıflandırma Kılavuzu		Saklanma Yeri
Gizli	En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır.	Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar ve kişisel bilgisayarlar
İç Kullanım	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır.	Departmanın kilitli dolapları, kişisel bilgisayarlar
Kişisel	Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kurum işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, Laptop veya Dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişilebilirlik ön plandadır.	Çalışma masalarının kilitli çekmeceleri
Kuruma Açık	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın kilitli ortak dolapları
Halka Açık	Bu bilgiler T.C. Sağlık Bakanlığına bağlı tüm teşkilatına, tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Dolaplar ve dolap dışlarında

Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmalıdır. Bu sınıflandırmaya göre halka açık dokümanlar web sitesinde yayınlanan ve işlem için üçüncü taraflara verilen kağıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

7. BİLGİ GÜVENLİĞİ POLİTİKA, PROSEDÜR VE KILAVUZU

BGYS Politikası kurumumuzca yayınlanan bir çok farklı politika, prosedür, talimat ve rehberi kontrol ve risk yönetimi amaçları çerçevesinde adresler.

7.1. Bilgi Güvenliği Politikası ve Kılavuzu

T.C. Sağlık Bakanlığı tarafından yayımlanan Bilgi Güvenliği Politikaları Yönergesi ve kılavuzu çerçevesinde, Rize İl Sağlık Müdürlüğü tarafından yayınlanan bu dokümanda genel bilgi güvenliği kuralları tanımlanmıştır. Her çalışan bu dokümanda belirtilen kurallara uymakla sorumludur.

7.2. Bilgi Güvenliği Prosedürleri ve Planları

Erişim kontrolü / Mobil cihazlar ve uzaktan çalışma,

Bilgi sınıflandırma (ve işleme)

Fiziksel ve çevresel güvenlik

Varlıkların kabul edilebilir kullanımı / Temiz masa ve temiz ekran

Bilgi transferi, Haberleşme güvenliği

Yazılım kurulumu ve kullanımı ile ilgili kısıtlamalar

Yedekleme

Kötücül yazılımlardan koruma

Kriptografik kontrollerin kullanımı

Teknik açıklıkların yönetimi

Kişi tespit bilgisinin mahremiyeti ve korunması

Tedarikçi ilişkileri gibi prosedür ve planlarda sistemin işleyişi anlatılmaktadır. İlgili çalışanlar yönetimce tanımlanan ve yayınlanan bu prosedür ve planlara uygun hareket etmelidirler.

7.3 Bilgi Güvenliği Sözleşmeleri

Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış farkındalık bildirgesi ve gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Bilgi Güvenliği Farkındalık Bildirgesi kurum personelleri (657-4c-4b vs) ile Personel Gizlilik Sözleşmesi ise personel çalıştırılmasına dayalı olan veya olmayan hizmet yapım ve mal alımları ile işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir. Ayrıca mal ve hizmet alımı kapsamında yapılan ihalelerde yükleniciler ile Kurumsal Gizlilik Sözleşmesi imzalanacaktır.

7.4 Bilgi Güvenliği Eğitimleri

Samsun İl Sağlık Müdürlüğü bünyesinde çalışan tüm personele Bilgi Güvenliği Farkındalık Eğitimi yılda en az bir defa verilecek olup sağlık tesislerimizin hizmet içi eğitim planlarına dahil edilmiştir.

8. PLANIN İHLALİ VE YAPTIRIMLAR

Bilgi Güvenliği Planı kapsamında oluşturulmuş kural ve süreçleri ihlal eden personel, paydaş ve üçüncü taraflar hakkında adli ve idari yasal takibat başlatılarak; 657 sayılı Devlet Memurları Kanununun 125. Maddesi gereğince işlem yapılabilir ve /ve ya ilgili sözleşmelerde yer alan yaptırımlarının bir ya da birden fazla hükmü uygulanabilir. Bahsi geçen cezai işlemlerden bazıları aşağıdaki gibidir:

- Uyarma
- Kınama
- Aylıktan kesme
- Kademe ilerlemesinin durdurulması
- Para cezası
- Sözleşmenin feshi

9. POLİTİKANIN YÜRÜRLÜĞE GİRİŞİ

"**Bilgi Güveliği Politikası"** ve hazırlanan tüm dökümanlar İl Sağlık Müdürünce onaylanmasının ardından yürürlüğe girer ve tüm personelce uyulması gereklidir.

10. POLİTİKANIN DUYURULMASI

"**Bilgi Güveliği Politikası"** yürürlüğe girmesinin ardından Tüm bağlı sağlık tesislerine yazılı olarak iletilir. Kurum Web sitesine eklenir. Planının tüm personelce okunup okunmadığı ayrı ayrı her sağlık tesisinin yöneticisinin sorumluluğundadır.

12. GÖZDEN GEÇİRME KURALLARI

Bilgi Güvenliği Çalışmaları, Bilgi Güvenliği Sorumluları tarafından periyodik olarak en az üç ayda bir kez, üst yönetim tarafından ise en az altı ayda bir kez gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler planının gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen plan Kurum Yönetimi tarafından onaylanır. Onaylanan plan Kurum internet sitesinde yayımlanır.**BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ POLİTİKASI**

A. AMAÇ

T.C Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesisleri bünyesinde normal çalışma saatleri süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar ve kaldırılabilir depolama ortamları ve kişisel bilgisayarlar için gerekli şartları tanımlamak.

B .KAPSAM

T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü personeli için yazılmış olup, güvenlik sorumlulukları olan tüm departman ve çalışanlar için geçerlidir.

C.POLİTİKA METNİ

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

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.

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.

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

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

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

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

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

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

D.YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, BGYS Komisyonu ve ilgili yöneticinin onaylarıyla BGYS Disiplin Prosedürü Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

E-POSTA GÜVENLİĞİ VE KULLANIM POLİTİKASI

Bu doküman, e-posta mesajlarında alma, gönderme, yönlendirme ve otomatik gönderme kullanımına ait T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinin E-Posta kullanım politikasını tanımlamaktadır.

KAPSAM

Bu politika, T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü bünyesinde kurumun sağladığı resmi E-Posta kutusu, tüm kullanıcılar içindir.

1. POLİTİKA METNİ

1.1 E-POSTA KULLANIMI

1.1.1. Bakanlığımızda görev yapan personel tarafından görevleri gereği yürütülen kurumsal iş ve işlemlerde, @saglik.gov.tr uzantılı kurumsal veya tüzel e-posta hesabı kullanılır. Kurumsal iş ve işlemler, kişilerin özel işleri için (Gmail, Hotmail gibi) internet hizmet sağlayıcılarından alınan hesaplar üzerinden yürütülmez.

1.1.2. KVKK tarafından 6698 sayılı Kanunda yer alan bazı hususların açıklanması amacıyla alınan 2018/10 sayılı karar gereği, e-posta ile aktarılacak verilerin özel nitelikli kişisel veri statüsünde olması durumunda aktarma işlemlerinin kurumsal e-posta veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak yapılması kanuni zorunluluktur.

1.1.3. Bakanlığımızda görev yapan 657 sayılı Kanuna bağlı tüm kamu personeline, talep etmeleri halinde kurumsal e-posta hesabı açılır.

1.1.4. Çeşitli sözleşmeler kapsamında Bakanlığımızda görev yapan ve yaptıkları iş gereği e-posta hesabı olması gereken personele, sıralı yöneticileri tarafından onay verilmesi halinde kurumsal e-posta hesabı açılır.

1.1.5. Kullanıcılara e-posta hesabı ilk kez açıldığında bir (1) GB disk alanı tanımlanır. Kota artırımı E-Posta Birimi tarafından dinamik olarak veya E-Posta Birimine e-posta ile yapılan talepler doğrultusunda yapılır.

1.1.6. Yüksek sayıda üye içeren dağıtım gruplarına gönderilen iletilerin denetim ve onay işlemleri için "moderatör" tanımlanır. İhtiyaç olması durumunda sadece belirli kullanıcıların veya grupların, söz konusu dağıtım gruplarına ileti göndermesi için detay yetkilendirmeler yapılır.

1.1.7. Yüksek sayıda üye içeren dağıtım grupları, tüm kullanıcılar tarafından görülen genel adres defterinden gizlenir.

1.1.8. Bir e-postaya eklenebilecek en fazla alıcı sayısı 100 (yüz) e-posta adresi ile sınırlı tutulur.

1.1.9. Gönderilen e-posta boyutu 25 MB geçemez.

1.1.10. Dağıtım gruplarının kullanım durumları (e-posta akış trafiği) takip edilir ve bir yıl boyunca kullanılmayan gruplar tespit edilerek silinir.

1.1.11. E-posta erişim trafiği SSL ile şifrelenir.

1.1.12. E-posta iletimlerinde "exe" gibi çalıştırılabilir dosyaların gönderilmesi engellenir.

1.1.13. Kullanıcılar, kendilerine tahsis edilen e-posta hesabını bir başka kişiye kullandıramaz veya devredemez. Kullanıcılar, kendilerine ait parolanın güvenliğinden ve söz konusu parola kullanılarak gönderilen e-postalardan doğacak hukuki işlemlerden sorumludur.

1.1.14. Kurumsal e-posta hesabı, yalnızca kurumsal süreçlere ilişkin iş ve işlemlerde kullanılabilir. Kurumsal e-posta hesaplarının, idari ve hukuki düzenlemelere aykırı ya da şahsi iş ve işlemlere ilişkin kullanımından kaynaklanan her türlü adli, idari, mali ve cezai sorumluluk ilgili hesap kullanıcısına aittir.

1.1.15. Sosyal medya, alışveriş siteleri, forumlar gibi üyelik isteyen uygulamalarda, Bakanlık tarafından verilen kurumsal e-posta hesapları kullanılamaz. Aksine durumlarda, yapılan tüm işlemlerden ve dile getirilen ifadelerden, ilgili kullanıcı sorumludur.

1.1.16. Konusu suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden ve sahip olduğu görev kapsamı içindeki iş ve işlemler dışındaki e-posta hesabının kullanımından kullanıcı sorumludur.

1.1.17. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-posta gönderilemez.

1.1.18. İnternet haber gruplarına üyelik için kurumun sağladığı resmi e-posta hesabı kullanılmaz. Ancak iş gereği üye olunması yararlı internet haber grupları için yöneticisinin onayı alınarak kurumun sağladığı resmi e-posta adresi kullanılabilir.

1.1.19. Kullanıcılar, eposta hesaplarında hukuki açıdan suç teşkil edecek materyal ve belgeleri bulunduramaz. Kullanıcılar, kendi kullanıcı hesaplarında barındırdıkları içeriklerden ve gerçekleştirilen tüm elektronik posta işlemlerinden sorumludur.

1.1.20. Kurumsal e-posta vasıtasıyla gizlilik dereceli veri aktarımı için Kılavuzun A.10.4.17 (E-Posta ile Veri Aktarımı) maddesinde belirtilen hususlara riayet edilir. E-postaların, gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilir.

1.1.21. E-posta gönderimlerinde, mesajın en alt kısmına gönderen kişinin kimlik ve iletişim bilgileri yazılır.

1.1.22. Kullanıcılar, gelen veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemek için her türlü tedbiri alır.

1.1.23. Tanınmayan elektronik postaların açılması, eklentilerinde bulunan dosya veya programların indirilip çalıştırılması kaynaklı oluşabilecek güvenlik sorunlarının sorumluluğu kullanıcıya aittir.

1.1.24. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verilmez.

1.1.25. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmaz.

1.1.26. Kullanıcılar, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

1.2 PAROLA GÜVENLİĞİ

1.2.1. Parola politikaları belirlenirken, sistem ve uygulamaların, kullanıcıları asgari olarak aşağıdaki kurallara uygun parola kullanmaya zorlamaları sağlanır.

1.2.2. Parolalar en az 8 (sekiz) karakterden oluşur. Root, administrator gibi sistem yönetim işlemlerinde kullanılan parolaların en az 12 karakterden oluşması tavsiye edilir.

1.2.3. İçerisinde en az 1 (bir) tane büyük ve en az 1(bir) tane küçük harf bulunur.

1.2.4. İçerisinde en az 1 (bir) tane rakam bulunur.

1.2.5. İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !,?,A,+,$,#,&,/,{,*,,],=,...)

1.2.6. Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, ababab...)

1.2.7. Sıralı karakterlerin kullanılması engellenir. (abcd, qwert, asdf,1234,zxcvb...)

1.2.8. Kişisel bilgiler veya klavye kombinasyonları ile basitçe üretilebilecek karakter dizilerinin kullanılması engellenir. (Örneğin 12345678, qwerty, doğum tarihi, çocuğun adı, soyadı gibi)

1.2.9. Sözlükte bulunabilen kelimelerin kullanılması engellenir.

1.2.10. Kullanıcının son 3 parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenir.

1.2.11. Sistem ve uygulamalarda oturum (session) kontrolü yapılarak bir kullanıcı adı ve parolasının aynı anda birden çok bilgisayarda kullanılması engellenir.

1.2.12. Veri tabanı yönetim sistemi, aktif dizin sunucusu, uygulama sunucusu, ağ cihazları gibi sistem hesaplarına ait parolalar (root, administrator, vs.) en geç 3 (üç) ayda bir değiştirilir.

1.2.13. Kullanıcı hesaplarına ait parolalar (örnek: HBYS, e-posta, web, masaüstü bilgisayar vs.) en geç 6 (altı) ayda bir değiştirilmesi sağlanır.

1.2.14. Parolalar, e-posta iletilerine veya herhangi bir elektronik forma eklenmez.

1.2.15. Parolalar gizli bilgi olarak muhafaza edilir. Kişiye özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.

1.2.16. Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da bu bölümde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.

1.2.17. İnternet tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup, kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.

1.2.18. Yazılım uygulamalarında erişim yetkisi tanımlanan kullanıcılara, gönderilen parola sıfırlama linkinin, aktivasyon işlemi başlatıldıktan (linke tıklandıktan) sonra en geç 15 dk. İçerisinde tamamlanacak şekilde konfigüre edilmesi gerekir.

2. YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla Bilgi Güvenliği Yönetim Sistemi Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

ERİŞİM KONTROLÜ VE ERİŞİM KAYDI TUTULMASI POLİTİKASI 1. AMAÇ

Bu doküman, bilgi ve bilgi işleme tesislerine yapılacak olan erişimlerin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesine imkân verecek bir sistemin tesis edilmesini amaçlamaktadır.

2. KAPSAM

Bu politika, T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde veri tabanlarına, sistem alt yapısına erişim yöntemlerini kapsamaktadır.

3. POLİTİKA METNİ

3.1. Erişim Yönetimi

3.1.1. Kurumun erişim sağlanacak sunucularına admin/root yetkili yönetici kullanıcılar, sudo ve runas yetkili kısıtlı yönetici kullanıcılar ve dış dünyadan erişen, uygulamayı kullanan kullanıcılardan oluşmaktadır.

3.1.2. Bakanlık sunucularına erişim için IP/SEC ya da SSL VPN kullanılmalıdır. Mümkünse kullanıcıların erişimi için SSL ve VPN tercih edilmelidir. Güvenlik Birimi tarafından gerekli kontroller sağlanmalıdır.

3.1.3. Sunuculara kullanıcı erişimi için SSH, RDP gibi protokollerle sunucu yönetimi için belirli portlar erişim verilmelidir.

3.1.4. Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.

3.1.5. Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir. Parola yönetimi bakanlık bilgi güvenliği kılavuzundaki parola yönetim politikaları ile yürütülmelidir.

3.1.6. Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, ssh key) ile yapılmalıdır.

3.1.7. Kullanıcıların sunucu yönetim için sağlanan erişimde sudo, runas gibi erişim kısıtlı erişim yetkileri tanımlanmalıdır.

3.1.8. Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir.

3.1.9. Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri idarede yetkili personellere teslim edilmelidir.

3.1.10. Sunucu servislerinin yönetim işlemleri merkezi kullanıcı yönetimi ve kısıtlı erişim yetkileriyle kullanıcılara sağlanmalıdır.

3.1.11. Kurumun yedekleme sistemlerine sadece memur ya da birim sorumlusu yetkili kişi erişim yapmalıdır Firmaların yapacakları tüm işlemler birim sorumlusu nezaretinde yürütülmelidir.

3.2. Kayıt Tutulması (Log Tutulması)

3.2.1. Kurumun güvenlik cihazlarına ait loglar kurum tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde işbirliği içinde raporlar paylaşılmalıdır.

3.2.2. Kurumun veri tabanlarına ait loglar kurum tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde işbirliği içinde raporlar paylaşılmalıdır

3.2.3. Kurumun network cihazlarına ait loglar kurum tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde işbirliği içinde raporlar paylaşılmalıdır

3.2.4. Tüm sunuculara ve servislere sağlanan tüm yönetici erişimleri uzak ve merkezi bir kayıt sunucusuna gönderilmelidir.

3.2.5. Merkezi kayıt sunucusu üzerinde yapılan analizler sonucunda başarısız erişimler raporlanmalıdır.

3.2.6. Merkezi kayıt sunucusu üzerinde alınan başarısız erişim istekleri uyarı olarak yetkili Birimlere gönderilmelidir.

3.2.7. Merkezi kayıt sunucusu üzerindeki başarılı girişler de istatiksel veriler halinde raporlanabilmelidir.

3.2.8. Merkezi kayıt sunucusu üzerindeki kayıt verileri belirli tarih aralığında tutulmalı ve istenildiğinde raporlanabilir olmalıdır.

3.2.9. Merkezi kayıt sunucusu kayıtlar üzerinde yaptığı analizler doğrultusunda saldırı ve normal olmayan durumları tespit edip, uyarı gönderebilmelidir.

3.3. Uzaktan Erişim Yöntemi

3.3.1. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.

3.3.2. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamalıdır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermelidir.

3.3.3. Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one time password authentication, örnek; Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmelidir. Daha fazlası için parola politikasına bakınız.

3.3.4. Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

3.3.5. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

3.3.6. Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.

3.3.7. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.

3.3.8. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

3.3.9. Uzak erişimde yapılan tüm network hareketleri loglanmalıdır

3.3.10. Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.

3.3.11. Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir. Sınırsız izin verilmekten kaçınılmalıdır.

3.3.12. VPN ile erişecek olan kullanıcı VPN Erişim formunu doldurmak zorundadır.

3.3.13. Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.

4. YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla Bilgi Güvenliği Yönetim Sistemi Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

BİLGİ GÜVENLİĞİ İNTERNET, AĞ KULLANIM-ERİŞİM PLANI VE ANTİ VİRÜS PLANI

A. AMAÇ

T.C Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü ve bağlık sağlık tesisleri İnternet ve Ağ Kullanımı-Erişimi planı ile Anti virüs planı politikasını tanımlamaktadır.

B. KAPSAM

T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü personeli için yazılmış olup, güvenlik sorumlulukları olan tüm departman ve çalışanlar için geçerlidir.

C. POLİTİKA METNİ

1. İnternet ve Ağ Kullanım-Erişim Planı

2.1. Hiçbir kullanıcı peertopeer bağlantı yoluyla internetteki servisleri kullanmayacaktır, (örneğin: KaZaA, iMesh, eDonkey, Gnutella, Napster, Aimster, Madstcr, FastTrak, Audiogalaxy, MFTP, eMule, Ovemet, NeoModus, Direct Connect, Asquisition, BearShare, Gnucleus, GTK-Gnutella, LimeVVire, Mactella, Morpheus, Phex, Otella, Shareaza, XoLoX, OpenNap, WinMX. vb)

2.2. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumum bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

2.3. Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ, MIRC, Messenger vb. mesajlaşma ve sohbet (chat) programları kullanılmamalıdır. Bu sohbet programları üzerinden dosya alışverişinde bulunulmamalıdır.

2.4. Hiçbir kullanıcı internet üzerinden Multimedia Streaming (video, mp3 yayını ve iletişimi)yapmayacaktır.

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

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

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

2.8. Üçüncü şahısların kurum içerisinden internet kullanımları İl Sağlık Müdürlüğü Bilgi İşlem Birim Sorumlusunun izni ve bu konudaki kurallar dâhilinde gerçekleştirilebilecektir.

2.9. Bilgisayar işletim 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.

2.10. Erişim Cihazları (Access Point) ve bilgisayarlara bağlanan bütün erişim cihazlarının ve alt arabirim kartlarının (örnek, PC Card) Bilgi İşlem birimi tarafından kayıt altına alınması gerekmektedir.

2. Anti virüs Planı

2.1. Bütün bilgisayarlarda kurumun lisanslı anti virüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.

2.2. Anti virüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Kurum Bilgi İşlem Birimine haber verilmelidir.

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

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

D.YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, BGYS Komisyonu ve ilgili yöneticinin onaylarıyla BGYS Disiplin Prosedürü Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

VERİ YEDEKLEME YÖNETİMİ POLİTİKASI

1. AMAÇ

Bu doküman, Müdürlüğümüz ve bağlı sağlık tesislerinde veri tabanlarında yer alan yedeklenmesi gereken her türlü verinin yedeklenmesine dair doküman olarak tanımlanmaktadır.

2 . KAPSAM

Bu politika, T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde veri yedekleme politikası ve kontrollerini kapsamaktadır.

3. POLİTİKA METNİ

3.1. Kurumun bütün verisinin, kurum çapında kullanılan işletim sistemlerinin ve uygulamaların tamamının yedeği uygun ve düzenli olarak alınmalıdır

3.2. Yedekleme sistemi iş sürekliliği planında yer alan veri yedekleme ihtiyacını karşılamalıdır

3.3. Yedeği alınacak veri ve uygulamalar için sınıflandırma yapılmalı ve her bir sınıf için kabul edilmeli veri kaybı süresi belirlenmelidir

3.4. Kabul edilir veri kaybı süresi yönetim tarafından onaylanmalıdır

3.5. Yedekleme işlemlerinin sağlanması için yedekleme politikasına uygun olarak bir yedekleme planı oluşturulmalıdır.

3.6. Yedekleme işlerine ait kayıtlar tutulmalıdır

3.7. Başarısız olan yedekleme işleri takip edilmeli ve yedeği alınamamış verinin yedeği alınmalıdır

3.8. Yedekleme medyaları etiketlenmeli ve hangi medyada hangi yedeğin bulunduğuna dair kayıtlar tutulmalıdır
3.9. Yedekleme medyalarının kopyaları alınarak ana sistem odasına zarar verebilecek felaketlerden etkilenmeyecek kadar uzakta ve güvenli olarak depolanmalıdır
3.10. Yedeklenmiş verinin düzenli aralıklarla geri döndürme testi yapılmalıdır
3.11. Yedekleme altyapısı, yedekleme ve geri döndürme işlemleri için talimatlar hazırlanmalıdır
3.12. Yedeklemesi alınacak bilginin seviyesi belirlenmelidir
3.13. Yedekleme kopyalarının doğru ve tam kayıtları ve dokümante edilmiş geri yükleme süreçleri sağlanmalıdır

3.14. Yedeklemenin türü (tam yedekleme/değişen kayıtların yedeklenmesi), yedeklemenin sıklığı iş gereklerine, güvenlik gereksinimlerine ve bilginin kritiklik derecesine göre belirlenmelidir
3.15. Yedeklerin bir kopyası doğal afetlerden ve olası tehlikelerden korumak maksadıyla ana merkezden uzak bir merkezde saklanmalıdır
3.16. Yedekleme bilgisine uygun seviyede fiziksel ve çevresel koruma sağlanmalıdır
3.17. Herhangi bir tehlike durumunda kullanımını sağlamak maksadıyla yedekleme bilgisi düzenli olarak test edilmelidir
3.18. Geri yükleme süreci düzenli olarak kontrol ve test edilmelidir. Gizliliğin önemli olduğu durumlarda yedeklemelerin kriptolu olarak alınması göz önünde bulundurulmalıdır
3.19. Bu kapsamda özellikle kişisel sağlık bilgilerinin kriptolu olarak yedeklenmesine dikkat edilmelidir

4. YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla Bilgi Güvenliği Yönetim Sistemi Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

BİLGİ GÜVENLİĞİ DİSİPLİN PROSEDÜRÜ

A. AMAÇ

Bu doküman, T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü kapsamında uygulanması planlanan Bilgi Güvenliği Yönetim Sistemleri (TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı) çerçevesinde yayımlanmış olan dokümantasyonda belirtilen hükümlere, prosedürlerde yer alan iş yapma biçimlerine uymayanlara karşı uygulanacak disiplin sürecini tanımlar.

B . KAPSAM

T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü Bilgi Güvenliği Yönetim Sistemi Politikası Kapsam maddesinde yer alan fiziki tanımlı alanlarda faaliyet gösteren tüm birimler ve tüm insan kaynaklarıdır.

C. SORUMLULAR

T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü faaliyet gösteren tüm personel. Bu sürecin işletilmesinden Bilgi Güvenliği Yönetim Sistemi Komisyonu Sorumludur.

D. UYGULAMA

1. T.C. Sağlık Bakanlığı Rize 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.

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.

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

4. Disiplin Prosedürünü T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü Bilgi Güvenliği Komisyonu ve Üst Yönetim yürütecektir.

5. T.C. Sağlık Bakanlığı Rize İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde bulunan donanımlar Rize İl Sağlık Müdürlüğü 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.

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

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

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

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

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

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.

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

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.

14. Kullanım Politikasını kabul eden taraf, T.C. Sağlık Bakanlığı T.C. Sağlık Bakanlığı Rize 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.

15. 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.

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

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

18. 657 Sayılı Devlet Memurları Kanun hükümlerine tabi olmayan personelin, (Danışmanlar, Firma Personelleri vb.) yüklenici ile kurum arasında imzalanan kurumsal gizlilik sözleşmesi ve yine yüklenici ile personel arasında yer alan personel gizlilik sözleşmesinde yer alan hükümler uygulanacaktır aksi durumda genel hukuk kurallarına tabi olacaktır.

19. 657 Sayılı Devlet Memurları Kanunda yer alan ve diğer kabul edilecek cezai yaptırımlar aşağıdaki gibi olacaktır.

a) Uyarma,
b) Kınama,
c) Aylıktan kesme,
d) Kademe ilerlemesinin durdurulması,
e) Devlet Memurluğunda çıkarma,
f) Para cezası (657 dışında kalanlarla yapılan sözleşmeler),
g) Sözleşme feshi.