|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 1/14 |

**1.AMAÇ:** Hastanemiz bilişim sistemlerinde bulunan bilgilerin güvenliği, gizliliği ve kişisel mahremiyetinin korunmasını sağlamak.

**2.KAPSAM:** Hastanemizin tüm birimlerini kapsar

**3.SORUMLULAR:** Tüm hastane çalışanları politikalara uymak zorundadır.

**Genel Kullanım Politikası**

1. Bütün PC ve laptoplar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmelidir.
2. Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
3. Hastanemizde domain (çalışma alanı) yapısı vardır mutlaka login olarak çalışılmalıdır. Bu durumda, domain'e bağlı olmayan bilgisayarların yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır,
4. Laptop bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi İşlem Merkezine de haber verilmelidir.
5. Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek hastanemize veya kişiye yönelik saldırılardan (örnek, elektronik bankacılık vs.) sistemin sahibi sorumludur.
6. Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.
7. Ağ güvenliğini (örnek, bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (paket sniffing, paket spoofing, denial of service vs. ). Ortadan kaldıracak eylemlere girişmemelidir. Port veya ağ taraması yapılmamalıdır.
8. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır,
9. Kurum bilgilerini kurum dışından üçüncü şahıslara iletilmemelidir.
10. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Merkezinin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
11. Cihaz, yazılım ve verinin izinsiz olarak kurum dışına çıkarılmamalıdır,
12. Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD'leri veya internetten indirilen programlar vs) kurmak ve kullanmak yasaktır, Yetkisi olmayan personelin, hastanemizdeki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
13. Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, Bakanlığımızın bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilemez.
14. Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin düzenli olarak farklı ortamlara ( cd, dvd, usb, external harddisk vs..) yedeklenmesinden sorumludur.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 2/14 |

1. Bilgi İşlem birimi tarafından atanan yetkili kişiler kullanıcıya haber vermeden yerinde veya uzaktan çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel kişisel bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.
2. Bilgisayarlarda oyun ve eğlence amaçlı programların çalıştırılmamalı/ kopyalanmamalıdır.
3. Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
4. Kurumda Bilgi İşlem biriminin bilgisi olmadan Hastanemiz Ağ sisteminde (web hosting servisi, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır,
5. Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri v.b. üzerinde mevcut yapılan düzenlemelerin hiçbir surette değiştirilmemelidir.
6. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.
7. Gerekmedikçe bilgisayar kaynaklarını paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
8. Hastanemizdeki tüm bilgisayar kullanıcıların mesai saatleri bittiği anda bilgisayarlarını ve bilgisayarlarına bağlı olan tüm dolanım birimlerinin elektriklerini kapalı konuma getirmeleri gerekir. Aksi taktirde bilgisayarın yada donanım biriminin aşırı ısınma yada elektrik arızasına sebep olarak yangına sebebiyet vermesi halinde bilgisayar başındaki kullanıcı sorumludur.
9. Hastanemiz sisteminde kullandığımız akıllı kart sistemi her bağlı olduğu kullanıcının sorumluluğundadır. Akıllı karttan doğabilecek arıza direk bilgi işlem personellerine bildirilmeli. Bildirim yapılmadan önce kendilerine bildirilen talimatlar uygulanmalıdır.
10. Bilgisayar başında görevli tüm personeller bilgisayarları ile ilgili olarak teknik donanım bakımından kendilerini eğitmelidirler (toner değişimi, yazıcıya kâğıt yüklenmesi v.s) Ayrıca sistem üzerinde kullanıcı hatalarından kaynaklanan problemler yetkili kişiler tarafından 3 raporla belgelendikten sonra aynı hatalar devam ettiği takdirde kullanıcı hakkında idari işlem uygulanacaktır.
11. Kullanıcılar bilgisayarları ile ilgili yazıcı, toner, klavye, Mouse gibi arızaları bilgi işlem merkezine bildirecekler arıza durumu giderilemiyorsa, gerekli malzeme talebini ayniyat sarf malzeme deposundan temin edeceklerdir.
12. Tüm hastane çalışanları yukarıda belirtilen hususlara ve konu ile ilgili bakanlıkça yayımlanmış ve yayımlanacak mevzuatı takip etmek ve uymak zorundadır.

|  |
| --- |
| 1. **SUNUCULAR İÇİN GÜVENLİK POLİTİKASI**
 |

* 1. **Kapsam**Bu politika Kurumun sahip olduğu bütün dahili sunucular için geçerlidir.
	2. **Politika**
		1. **Sahip Olma ve Sorumluluklar**Kurum bünyesindeki bütün dahili sunucuların yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigurasyonları sadece bu gruptaki kişiler tarafından yapılacaktır.
		2. Bütün sunucular (kurumun sahip olduğu) ilgili kurumun yönetim sistemine kayıt olmalıdır. En az aşağıdaki bilgileri içermelidir.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 3/14 |

* Sunucuların yeri ve sorumlu kişi.
* Donanım ve İşletim Sistemi.
* Ana görevi ve üzerinde çalışan uygulamalar.
* İşletim Sistemi versiyonları ve yamalar.
	+ 1. Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.
	1. **Genel Konfigurasyon Kuralları**
		1. İşletim sistemi konfigurasyonları Kurumun Bilgi İşlem Biriminin talimatlarına göre yapılacaktır.
		2. Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
		3. Servislere erişimler loglanacak ve erişim kontrol metotları ile koruma sağlanacaktır.
		4. Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır.
		5. Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.
		6. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
		7. Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdırlar.

**Gözlemleme**

* + 1. Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır.
* Bütün güvenlikle ilgili loglara online olarak minimum 90 gün süreyle erişilebilmelidir.
* Günlük loglar en az 1 ay saklanmalıdır.
* Haftalık loglar en az 3 ay tutulmalıdır.
* Aylık loglar en az 1 (bir) yıl tutulmalıdır.
	+ 1. Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlikle ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.
* Port tarama atakları.
* Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması.
* Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.
	1. **Uygunluk**
		1. Denetimler yetkili organizasyonlar tarafından Kurum bünyesinde belli aralıklarda yapılmalıdır.
		2. Denetimler Bilgi İşlem grubu tarafından yönetilecektir.
		3. Denetimler Kurumun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.
	2. **İşletim**
		1. Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
		2. Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.
		3. Sistem odalarına yetkisiz girişler engellenmelidir.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 4/14 |

|  |
| --- |
| 1. **YEDEKLEME POLİTİKASI**
 |

* 1. **Amaç**Bilgi sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigurasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak olarak yedeklenmesi gerekir. Bu politika yedekleme kurallarını tanımlamaktadır.
	2. **Kapsam**Tüm kritik bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.
	3. **Politika**
		1. Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigurasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekmektedir.
		2. Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak Manyetik kartuş, DVD veya CD ortamında yedekleri alınmalıdır.
		3. Taşınabilir ortamlar (Manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır. Veriler offline ortamlarda en az 30 (otuz) yıl süreyle saklanmalıdır.
		4. Kurumsal kritik verilerin saklandığı sistemler ile sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.
		5. Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.
		6. Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
		7. Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
		8. Yedek ünite üzerinde gereksiz yer tutmamak üzere, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dahil edilmemelidir.
		9. Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
		10. Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenmelidir.
		11. Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.
		12. Yedekleme ortamlarının düzenli periyodlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
		13. Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dahilinde tamamlanabileceğinden emin olunması gerekir.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 5/14 |

* + 1. Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
		2. Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyalarının bir felaket anında etkilenmeyecek bir ortamda bulundurulması gerekmektedir.
		3. Veri Yedekleme Standardı; yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği, yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

|  |
| --- |
| 1. **KİŞİSEL SAĞLIK KAYITLARININ GÜVENLİĞİ POLİTİKASI**
 |

* 1. **Amaç**Bu politikanın amacı hasta sağlık bilgisinin mahremiyeti hususunda uyulması gereken kuralları tanımlamaktır. Hasta kaydı bilgisi kapsamına, hasta ile ilgili sözlü bilgi, yazılı bilgi, tıbbı müdahaleler, ön tanı, teşhisler, görüntüleme filmleri ve faturalama gibi konular girmektedir.
	2. **Kapsam**Bu politika tüm çalışanları kapsamaktadır.
	3. **Politika**
		1. **Genel Kurallar**Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mâli vb.) güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.
			1. Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; veri gizliliğinin, değiştirilmediğinin (bütünlüğünün) ve erişilebilirliğinin sağlanmasıdır.
			2. Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.
			3. Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar (hastanın tedavisinden sorumlu sağlık personeli) ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidirler. Ancak hastanın yazılı onayı ile diğer sağlık çalışanları bu veriye erişebilirler.
			4. Hasta taburcu olmuş ise tanımlanmış yetkili kullanıcılar dışında hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.
			5. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemelidir.
			6. Hastanın rızası olmadan hiçbir çalışan yazılı veya sözlü olarak hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.
			7. Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara ve kurumlara iletilemez. Hastanın kullandığı ilaçlar, diyet programları vs. buna dahildir.
			8. Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. [Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi]
			9. Telefonda konuşurken hastanın mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen göstermelidir.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 6/14 |

* + - 1. Bütün hasta sağlık kayıtları (online bilgi veya yedek medya) fiziksel olarak korunmuş mekanlarda saklanmalıdır.
			2. Elektronik sağlık kayıtlarına internet ortamından erişim, ancak yetkilendirilmiş kullanıcılara güvenli erişim sağlandığında mümkün olabilir.
			3. Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya Bakanlığımızın Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir.
			4. Sağlık kayıt dosyalarının saklandığı kağıt veya elektronik medyalar (kartuş,CD,DVD, Flash disk, HDD, vb.) güvenli bir ortamda saklanmalıdır.
			5. Kurum, kritik bilgiye erişim hakkı olan çalışanlar ve firmalar ile gizlilik anlaşması imzalamalıdır.
			6. Yetkiler, "görevler ayrımı" ve "en az ayrıcalık' esaslı olmalıdır. "Görevler ayrımı", rollerin ve sorumlulukların paylaştırılması ile ilgilidir ve bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığını azaltılır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.
			7. Sağlık kayıt dosyalarına erişecek kurum çalışanları belirlenmiş olmalıdır. Bu çalışanlar dosyaların güvenliğinden ve her türlü hareketinden sorumlu olmalıdır.
			8. Sağlık kaydı arşivi en az 30 (otuz) yıl süre ile saklanmalıdır.
		1. **Sistem Güvenliği**
			1. Sağlık kurumları bünyesinde hasta tanımlayıcı olarak TC Kimlik numarası baz alınacaktır. Hastanın sağlık bilgisine erişimde özel olarak atanan protokol numarası kullanılabilinir.
			2. Bilgi sistemlerinde güvenlik veriye erişim bazında olacaktır. Bunun için bu sistemin özellikle yazılım ve veritabanı erişim katmanlarında özel uygulamalar oluşturulacaktır. Veriye erişecek kişiler aşağıdaki şekilde tanımlanmıştır.
			- Hasta kendi verisine online olarak kurum tarafından kendisine verilen sadece ilgili vakayla ilişkili pin numarası ve şifre ile internetten erişebilir. Diğer taraftan, Akıllı kart, elektronik imza, token vb. mekanizmaların kullanıldığı taktirde veriye tam erişim mümkün olabilir.
			- Bir Aile hekimi ancak kendisine kayıtlı olan hastaların elektronik sağlık kayıtlarına erişebilmelidir.
			- Hastanedeki yetkilendirilmiş sağlık çalışanları ise, ancak hastanın giriş tarihinden, taburcu olana kadar geçen zaman içerisinde hastanın elektronik sağlık kayıtlarına erişebilirler. Ve bu da "geçici bir süreliğine" olacaktır.
			- Sistem yöneticilerine de bir güvenlik katmanı konulacaktır. Bunun için veritabanı yazılımının gelişmiş güvenlik yönetimi özellikleri kullanılacaktır.
			- Gerektiğinde saat ve/veya gün bazında belirlenen bir sure için bazı kullanıcı ve istemci makinelerin sisteme oturum açmalarına kısıtlama getirilebilmelidir.
			- Aynı kullanıcı kodu ile aynı anda birden fazla oturum açılmasına izin verilmemelidir.
			- Eğer hasta, herhangi bir sağlık çalışanının elektronik sağlık kayıtlarına erişmesini istemiyorsa, sağlık çalışanı ilgili dosyayı okuma hakkına kavuşamamalıdır. Fakat sağlık çalışanı muayene sonuçlarını hastanın veri tabanına aktarabilmelidir. Bu diğer doktorlar tarafından yazılan kayıtlara erişilmemesi için kullanılan metottur.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 7/14 |

* + - * Sadece yetkisi olan kullanıcılar için veri girişi ve/veya verinin elde edilmesi için erişim izni verilmelidir. Birçok kullanıcının veri tabanında sadece belirli bir veri setine erişim yetkisinin denetlenebilmesini sağlamak için çok katmanlı denetim mekanizmaları olmalıdır.
			* Veri tabanında tutulacak verilerin tutarlılığı tam ve kesin bir şekilde sağlanmalıdır. Bunu sağlamak için en azından, veri onay (validation), çapraz sorgulama (cross-checking) ve mükerrer kayıt önleme gibi ölçütler uygulanmalıdır.
			* Yönetimsel analizler yapmak için veri tabanındaki veriler bir yerden başka bir yere aktarılırken, kayıtlarda bulunan kişisel kimlik tanımlayıcıları kayıtlardan çıkartılmalı ve analizler hasta ile hastalık bilgilerini eşleştirmeden yapılmalıdır.
			* Kullanıcı aktiviteleri (yapılan tüm işlemler ve erişimler) izlenebilmelidir. Veri tabanı üzerinde yapılan şüpheli işler denetlenebilmelidir. Sistemin hem etkin bir şekilde yönetilmesi, hem de yetkisiz erişimlerin engellenmesi ve izlenmesi anlamında gelişmiş bir kontrol mekanizması olmalıdır. Sistem, hangi kullanıcının sistemin hangi kısmına ne zaman ve nereden eriştiğine dair (zaman damgası-date stamp, işlem, kullanılan istemci bilgisayar tanımı gibi bilgileri de içeren) kayıt tutmalıdır.
			* Sistem yöneticilerinin kimlik tanımlama ve doğrulaması için mümkünse X.509v3 uyumlu sayısal sertifikalar kullanılmalıdır. Sayısal sertifikaların güvenli depolaması için akıllı kartlar veya usb token cihazları kullanılmalıdır.
			* Sertifika tabanlı kimlik doğrulama yapılamadığı durumlarda password ve hash tabanlı kimlik doğrulama yapılacaktır.
			* Kurum ile başka ağlar arasındaki tüm haberleşme şifreli yapılmalıdır. İletişim VPN teknolojisini kullanmalıdır

|  |
| --- |
| 1. **İNTERNET ERİŞİM VE KULLANIM POLİTİKASI**
 |

* 1. **Amaç**İnternet'in uygun olmayan kullanımı, Kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeden bu türden olumsuzluklara neden olunmaması ve İnternet'in kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır.
	2. **Kapsam**Bu politika Bakanlığın bütün kullanıcıları kapsamaktadır.
	3. **Politika**Bütün kullanıcılar ve Bilgi İşlem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkmamalıdır.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 8/14 |

* + 1. Kurum 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 sağlayabilmelidir.
			1. Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografik, oyun, kumar, şiddet içeren vs) yasaklanabilmelidir.
			2. Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır. (Intrusion Detection an Prevention Systems-IPS): Şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IPS, şüpheli durumlarda e-posta veya SMS gibi yöntemlerle sistem yöneticisini uyarabilmektedir.
			3. İnternet trafiğindeki yoğunluk dikkate alınarak gerekli protokollerde Anti-virus gateway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik (smtp, pop3, ayrıca mümkünse http ve ftp vs) virüslere karşı taranmalıdır.
			4. İnternet erişimleri *5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a* göre düzenlenmeli, loglar oluşturulmalı ve kayıt edilmelidir.. Tüm internet erişimleri zaman damgası ile loglanmalı ve bu loglar en az 1 (bir) yıl saklanmalıdır.
			5. Ancak Yetkilendirilmiş Sistem Yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahiptir. Bunlar; www,ftp,telnet, ping, traceroute vs.
			6. Hiçbir kullanıcı peer-to-peer bağlantı yoluyla internetteki servisleri kullanamayacaktır. (Örnek; KaZaA, iMesh, eDonkey2000, Gnutella, Napster, Aimster, Madster, FastTrack, Audiogalaxy, MFTP, eMule, Overnet, NeoModus, Direct Connect, Acquisition, BearShare, Gnucleus, GTK-Gnutella, LimevVire, Mactella, Morpheus, Phex, ötella, Shareaza, XoLoX, OpenNap, WinMX. v.b.)
			7. Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ,MIRC,Messenger v.b. mesajlaşma ve sohbet programları gibi chat programlarının kullanılmamalıdır. Bu chat programları üzerinden kurumsal işlemler dışında dosya alışverişinde bulunulmamalıdır.
			8. Yetkilendirilmiş kullanıcılar dışında hiçbir kullanıcı internet üzerinden Multimedia Streaming yapamayacaktır.
		2. Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.
		3. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemesi ve dosya indirimi yapılmamalıdır.
		4. İş ile ilgili olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload), indirmek (download etmek) yasaktır.
		5. İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve Kurum sistemleri üzerine bu yazılımlar kurulamaz. Kurumsal işlevlere yönelik yazılım ihtiyaçları için ilgili prosedürler dahilinde ilgili Bilgi İşlem sorumlularına müracaat edilmesi gerekmektedir.
		6. Üçüncü şahısların kurum internetini kullanmaları Bilgi İşlem sorumlularının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecekti

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 9/14 |

|  |
| --- |
| 1. **E-POSTA KULLANIMI POLİTİKASI**
 |

* 1. **Amaç**Bu politikanın amacı hastanemiz e-posta altyapısına yönelik kuralları ortaya koymaktır. Kurum'da oluşturulan e-postalar resmi bir kimlik taşımaktadırlar. E-posta, hastanemizin en önemli iletişim kanallarından biridir ve bu kanalın kullanılması kaçınılmazdır. Bunun yanı sıra e-posta, basitliği ve hızı nedeni ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır.
	2. **Kapsam**Bu politika Kurum'da oluşturulan e-postaların doğru kullanımını içermektedir ve bütün çalışanları kapsamaktadır.
	3. **Politika**
		1. **Yasaklanmış Kullanım**
			1. Kurumun e-posta sistemi, taciz, suistimal 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.
			2. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
			3. Hastanemiz ve Sağlık Bakanlığı ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğeler de dahildir.
			4. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
			5. Kişisel kullanım için Internet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
			6. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
			7. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
			8. Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb) gönderemezler.
		2. **Kişisel Kullanım**
			1. Hastanemizde kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır. Ayrıca iş dışındaki e-postalar farklı bir klasör içerisinde saklanmalıdır.
			2. Hastanemiz personeli tarafından internet ortamı aracılığı ile iletilen her türlü kişisel e-posta mesajının altında, Hastanemiz 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.
			3. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
			4. Gizli ve hassas bilgi içeren elektronik postalar kriptolanarak iletilmelidir.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 10/14 |

* + - 1. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-maillerin sahte e-mail olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
			2. Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
			3. Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.
			4. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.
			5. 6 ay süreyle hiç kullanılmamış e-posta adresleri kullanıcıya haber vermeden kapatılabilir.
			6. E-posta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma işten ayrılma sebepleriyle kurumdaki değişikliğinin yetkililer tarafından Bilgi İşlem birimine bu değişikliğin en geç 15 gün içinde bildirilmesi gerekmektedir.
		1. **Gözlemleme**Hastanemiz çalışanları gönderdikleri, aldıkları veya sakladıkları e-maillerde kişisellik aramamalıdır. Bu yüzden yetkili kişiler önceden haber vermeksizin e-mail mesajlarını denetleyebilirler.
		2. **E-Posta Yönetimi**Hastanemiz, e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur
		3. **E-Posta Virüs Koruma**Virüs, solucan, Truva Atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslerle bulaşmış e-postalar Anti-virus sistemleri tarafından analiz edilip temizlenmelidir. Ağ güvenlik yöneticileri bu sistemden sorumludur.

|  |
| --- |
| 1. **ŞİFRE KULLANMA POLİTİKASI**
 |

* 1. **Genel Bakış**Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. hastanemiz çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifreleme yapmakla sorumludurlar.
	2. **Amaç**Bu politikanın amacı güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkında standart oluşturmaktır.
	3. **Kapsam**Bu politika, kullanıcı hesabı olan (bilgisayar ağına erişen ve şifre gerektiren kişiler) bütün kullanıcıları kapsamaktadır.
	4. **Politika**
		1. **Genel**
			1. Bütün sistem seviyeli şifreler (örnek, root, administrator, enable, vs) en az üç ayda bir değiştirilmelidir.
			2. Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her dört ayda birdir.
			3. Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 11/14 |

* + - 1. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
			2. SNMP kullanıldığı durumlarda varsayılan olarak gelen "public", "system" ve "private" gibi community string'lere farklı değerler atanmalıdır.
			3. Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara yada elektronik ortamlara yazmaması konusunda eğitilmelidir.
			4. Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.
			5. Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır.
			6. Bir kullanıcı adı ve şifresi birim zamanda birden çok bilgisayarda kullanılmamalıdır.
			7. Bütün kullanıcı ve sistem seviyeli şifrelemeler aşağıdaki ana noktalara uymalıdır.
		1. **Ana Noktalar**
			1. **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.

* + - * Şifreler sekizden daha az karaktere sahiptirler.
			* Şifreler sözlükte bulunan bir kelimeye sahiptir.
			* Şifreler aşağıdaki gibi ortak değere sahiptir.
				+ Ailesinin, arkadaşının, sahip olduğu bir hayvanın veya bir sanatçının ismine sahiptir.
				+ Bilgisayar terminolojisi ve isimleri, komutlar, siteler, şirketler, donanım veya yazılım gibi.
				+ "Sağlık", "istanbul", "ankara" gibi isimler.
				+ Doğum tarihi veya adres ve telefon numaraları gibi kişisel bilgiler.
				+ aaabbb, qwerty,zyxwuts, 123321 vs. Gibi sıralı harf veya rakamlar.
				+ Yukardaki herhangi bir kelimenin geri yazılış şekli.
				+ Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek ,gizli1, gizli2).

Güçlü şifreler aşağıdaki karakteristiklere sahiptir.

* + - * Küçük ve büyük karakterlere sahiptir (örnek, a-z, A-Z)
			* Hem dijit hemde noktalama karakterleri ve ayrıca harflere sahiptir.
			( 0-9, !@#$%A&\*()\_+|~-=V{}[]:";'<>?,/ )
			* En az sekiz adet alfanümerik karaktere sahiptir.
			* Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
			* 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.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 12/14 |

***Not: Yukarıdaki herhangi bir örneği şifre olarak kullanmayınız.***

* + - 1. **Şifre Koruma Standartları**

Hastanemiz 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. Hastanemiz bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler hastanemize ait gizli bilgiler olarak düşünülmelidir.

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.
		- Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem birimi yetkilisini aramasını söyleyiniz.
		- Uygulamalardaki "şifre hatırlama" özelliklerini seçmeyiniz, (örnek, Outlook, Internet Explorer vs.)
		- Şifreleri herhangi bir yere yazmayınız ve herhangi bir ortamda elektronik olarak saklamayınız.
		- Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.
			1. **Uzaktan Erişen Kullanıcılar için Şifre Kullanımı**Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılacaktır.

|  |
| --- |
| 1. **UZAKTAN ERİŞİM POLİTİKASI**
 |

* 1. **Amaç**Bu politikanın amacı herhangi bir yerden Kurumun bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar kaynaklarının yetkisiz kullanımından dolayı kuruma gelebilecek potansiyel zararları minimize etmek için tasarlanmıştır. Bu zararlar şunlardır; kurumun gizli ve hassas bilgilerinin kaybı, beyin gücü kaybı, prestij kaybı ve içerideki kritik sistemlere meydana gelen zararlar vs.
	2. **Kapsam**Bu politika Kurumun bütün çalışanlarını, sözleşmelileri, İT hizmeti veren firmaları veya Kurum adına çalışanları ve kısaca Kurumun herhangi bir birimindeki bilgisayar ağına erişen bütün kişi ve kurumları kapsamaktadır. Bu politika, kuruma bağlı bütün uzak erişim bağlantılarını kapsamaktadır ve bunun içerisine e-posta okuma veya gönderme ve intranet web kaynaklarını gözlemleme dahildir. Bütün uzaktan erişim uygulamaları bu politika tarafından kapsanmaktadır.
	3. **Politika**
		1. **Genel**Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 13/14 |

* + 1. **Gereklilikler**
			1. Internet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. (Sağlık ocakları, hastaneler, grup başkanlıkları da bu kapsam içerisindedir). Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.
			2. Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one-time passvvord authentication ,örnek ; token device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmektedir. Daha fazla bilgi için Şifreleme Politikası'na bakınız.
			3. Kurum çalışanları hiç bir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.
			4. 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.
			5. Çalışanlar Kurum ile ilgili yazışmalarında Kurumun dışındaki e-posta hesaplarını (örnek, hotmail, yahoo, mynet vs) kullanamazlar.
			6. ISDN veya telefon hatları ile uzaktan erişen yönlendiriciler minimum olarak CHAP kimlik doğrulama protokolünü kullanmalıdırlar.
			7. Uzaktaki kullanıcı cihazını split-tunnel veya dual-homing (VPN bağlantısı esansında başka bir bağlantı daha yapmak) olarak konfigure edemez.
			8. Uzaktan erişim yöntemi ile kuruma erişen bütün bilgisayarlar en son güncellenmiş anti-virus yazılımına sahip olmalıdırlar.
			9. Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler Bilgi İşlem biriminin özel izni ile geçici olarak izin verilebilir.
			10. Periyodik olarak yapılan kontrollerle kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

|  |
| --- |
| 1. **KABLOSUZ AĞ ERİŞİM POLİTİKASI**
 |

* 1. **Amaç**Bu politika kablosuz cihazların gerekli güvenlik tedbirleri alınmaksızın kurumun bilgisayar ağına erişimini engellemeyi amaçlamaktadır. Sadece bu politikanın güvenlik kriterlerine uyan cihazlar kurumun bünyesinde kullanabilirler.
	2. **Kapsam**Bu politika kurum bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını ( PC, Cep telefonları, PDA vs) kapsamaktadır. Kablosuz veri transferi sağlayabilen herhangi bir cihaz bunun kapsamındadır. Kuruma bağlantısı olmayan herhangi bir cihaz veya bilgisayar ağı bu politikanın kapsamı içerisinde değildir.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ PROSEDÜRÜ** | DÖKÜMAN KODU | BY.PR.01 |
| YAYIN TARİHİ | 22.08.2016 |
| REVİZYON TARİHİ | 09.06.2017 |
| REVİZYON NO | 01 |
| SAYFA | 14/14 |

* 1. **Politika**
		1. **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.
		2. **Onaylanmış Teknoloji**Bütün kablosuz erişim cihazları Bilgi İşlem güvenlik birimi tarafından onaylanmış olmalıdır ve Bilgi işlemim belirlediği güvenlik ayarlarını kullanmalıdır.
		3. **Güvenlik Ayarlar**
			1. Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access(VVPA) şifreleme kullanılmalıdır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılabilmelidir.
			2. Erişim cihazlarında ki firmware'leri düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.
			3. Erişim cihazlarını kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü, cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.
			4. Cihaza erişim için güçlü bir şifre kullanılmalıdır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır
			5. SSID numaraları yayınlanmamalıdır. Böylece sniffer tarzı cihazların otomatik olarak bu numaraları çözmesi engellenecektir.
			6. Varsayılan SSID isimlerini kullanmayınız. SSID ayarı bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vs.
			7. Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir. Bunun için birectional antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.
			8. Erişim Cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dahil olmalıdırlar.
			9. İnternete çıkacak Erişim Cihazları üzerinden gelen kullanıcılar kurumun ağına dahil olmamalıdır. Kablosuz internet ağı için farklı bir internet altyapısı kullanılmalı, kurumun lokal ağının kullandığı internet altyapısını kullanmamalıdır.
			10. Kullanıcı bilgisayarlarında kişisel firewall yazılımları yüklü olmalıdır.
			11. Kritik yerlerde kullanıcılar VPN teknolojilerini kullanarak kurum ağına erişmelidirler.
			12. Lokal ağa bağlanacak kullanıcılar ve erişim cihazları statik ip adresleri kullanmalıdır. Aynı zamanda donanım adresleme (örnek, mac adresleme) kullanılmalıdır.
			13. İnternete çıkacak kullanıcılar firewall ve içerik yönetim sistemi üzerinden kullanıcı adı ve şifre ile yetki almalı ve kullanıcı adı, IP, mac adresi bilgileri loglanmalıdır. Bu loglar *5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun hükümlerine göre alınmalı ve kayıt edilmelidir.*
			14. Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir. Sistemde hackerlar tarafından konulmuş casus bir erişim cihazı olabilir veya mevcut erişim cihazı resetlenmiş olup kurumun güvenlik politikalarına aykırı bir şekilde ayar yapılmış olabilir.

|  |  |  |
| --- | --- | --- |
| HAZIRLAYAN | KONTROL EDEN | ONAYLAYAN |
| BİLGİ İŞLEM  | PERFORMANS VE KALİTE BİRİMİ | BAŞHEKİM |