**1.AMAÇ:** Eskişehir Osmangazi Üniversitesi Tıp Fakültesine başvuruda bulunan kişilere ait bilgilerin güvenliğinin sağlanması amaçlı öncelikle verilerin doğru olarak toplanması, depolanması ve kullanılmasına ilişkin uygulamalarımızı ve güvenlik önlemlerimizi dahili olarak gözden geçirmek ve kişisel verileri depoladığımız sistemleri yetkisiz erişime karşı korumak için fiziksel güvenlik önlemlerini almak ve bunun devamlılığını sağlamaktır.

**2. KAPSAM:** Bu prosedür, kurum Bilgi İşlem altyapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

**3. KISALTMALAR:**

- **HBYS:** Hastane Bilgi Yönetim Sistemi

**4. TANIMLAR:-**

**5. SORUMLULAR**

- Hastane Başhekimi
- Hastane Başmüdürü
- Hastane Müdürü (İdari)
- Bilgi İşlem Merkezi
- Tüm Bilgisayar Operatörleri

**6. FAALİYET AKIŞI:**

**6.1.SUNUCULARIN GÜVENLİĞİ**

**6.1.1.** Kurum bünyesindeki bütün sunucuların yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu yapılandırmaları sadece bu gruptaki kişiler tarafından yapılacaktır.

**6.1.2.** Kurumda bulunan bütün sunucuların kayıtları tutulmalıdır. Bu kayıtlar en az aşağıdaki bilgileri içermelidir;

- ✓ Sunucuların yeri,
- ✓ Sorumlu kişisi,
- ✓ Donanım,
- ✓ İşletim sistemi,
- ✓ İşletim sistemi üzerinde çalışan uygulama bilgileri.

**6.1.3.** Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

**6.1.4.** Sunucu yedekleri talimata uygun olarak düzenli şekilde alınmalıdır.

**6.1.5.** Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse yama ve anti-virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır.

**6.1.6.** Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

**6.1.7.** Sistem yöneticileri gerekli olmadığı durumlar dışında “Administrator”, “Root” gibi genel yönetici hesapları kullanılmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Gerekli olduğunda kendi hesapları ile log-on olup sonra genel yönetici hesabına geçiş yapılmalıdır.

**6.1.8.** Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

**6.1.9.** Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır, yetkisiz girişler engellenmelidir.

**6.1.10.** Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.

**6.1.11.** Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar yapılmalıdır.

**6.2.YEDEKLEME**

Bilgi sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, Bilgi İşlem Merkezinde aşağıda maddelenen şekilde çalışan sistemin yedeği alınmaktadır.

**6.2.1.** Cluster Yapısı ile yedekleme; Cluster yapısı, sunucu bilgisayarının bozulduğu anda, yükü diğer çalışan sunucu bilgisayar üzerine atar ve sistem kesintisiz çalışmaya devam eder. Yedekte tutulan sunucu sistem çalışıyor iken görev yapmaz ve hazırda bekler, sadece sunucu çöktüğü zaman devreye girer.

**6.2.2.** NAS Yapısı ile yedekleme; NAS (Network Attached Storage / Server = Ağa bağlı disk / sunucu) sistemleri veri depolama, yüksek ulaşılabilirlik ve verinin güvenliği amacı baz alınarak üretilmiş

depolama birimleridir. Temelde amaçları asıl veriyi tutmak değil verinin yedeğinin alınması olan bu sistemler kendi içlerinde RAID yapısı ile çalışabilmeleri sayesinde asıl verinin tutulduğu güvenilir cihazlardır.

**6.2.3.** Sisteme bağlı bulunan NAS, RAID 1 (Aynalama) yapısı ile çalışmaktadır. RAID 1 yapısı ile dizideki en az bir disk düzgün çalıştığı sürece, her türlü hata ve aksaklığa karşı koruma vardır ve dizi normal çalışmasını sürdürür.

**6.2.4.** Yedekleme planının sahibi Bilgi işlem birim sorumlusudur. Planı uygulamaktan sorumlu personel bilgi işlem otomasyon sorumlusudur. Bilgi işlem birim sorumlusu yedekleme işlemlerinin politikaya uygun olarak gerçekleştirilmesinden, bilgi işlem otomasyon sorumlusu planda yazılı işlemlerin yerine getirilmesinden sorumludur.

**6.2.5.** Her gün saat 00.00' de otomatik olarak SH dosyasının çalıştırılması ile alınan ve sıkıştırılmış yedek dosyası, bilgi işlem merkezinin dışındaki bir odada ağ yapımıza bağlı FTP destekli NAS cihazına her gün yedeklenir.

**6.2.6.** NAS cihazı, Bilgi İşlem Merkezinin Karşı tarafındaki odada muhafaza edilecektir.

**6.2.7.** Tüm Yedeklenmesi gereken bilgiler her gün NAS üzerine ağ üzerinden yedeklemesi yapılır. Yedek kontrolleri sağlanmalıdır.

### 6.3.KİŞİSEL SAĞLIK KAYITLARININ GÜVENLİĞİ

Hastanemizde kayıtlı olan hasta sağlık bilgisinin mahremiyeti hususunda uyulması gereken kuralları tanımlamaktadır. Hasta kaydı bilgisi kapsamına, hasta ile ilgili sözlü bilgi, yazılı bilgi, tıbbi müdahaleler, ön tanı, teşhisler, görüntüleme filmleri ve faturalama gibi bilgiler girmektedir.

#### 6.3.1.Genel Kurallar

Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mali vb.) güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.

- ✓ Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar veri gizliliğinin, değiştirilmediğinin (bütünlüğünün) ve erişilebilirliğinin sağlanmasıdır.
- ✓ Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.
- ✓ Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar (hastanın tedavisinden sorumlu sağlık personeli) ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidir. Ancak hastanın yazılı onayı ile diğer sağlık çalışanları bu veriye erişebilirler.
- ✓ Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez
- ✓ Hasta dosyasının bir kopyası hastaya teslim edilebilir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemelidir.
- ✓ Hastanın rızası olmadan hiçbir çalışan yazılı veya sözlü olarak hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.
- ✓ Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara ve kurumlara iletilemez Hastanın kullandığı ilaçlar, diyet programları vs. buna dahildir.
- ✓ Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi.
- ✓ Telefonda konuşurken hastanın mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen göstermelidir.
- ✓ Bütün hasta sağlık kayıtları (online bilgi veya yedek medya) fiziksel olarak korunmuş mekanlarda saklanmalıdır.
- ✓ Elektronik sağlık kayıtlarına internet ortamından erişim, ancak yetkilendirilmiş kullanıcılara güvenli erişim sağlandığında mümkün olabilir.
- ✓ Hasta sağlık bilgileri kurum tarafından veya Sağlık Bakanlığının Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir.
- ✓ Sağlık kayıt dosyalarının saklandığı kağıt veya elektronik medyalar (kartuş, CD, DVD, Flash disk, HDD, vb.) güvenli bir ortamda saklanmalıdır.
- ✓ Kurum, kritik bilgiye erişim hakkı olan çalışanlar ve firmalar ile gizlilik anlaşması imzalamalıdır.
- ✓ 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.

- ✓ Sağlık kayıt dosyalarına erişecek kurum çalışanları belirlenmiş olmalıdır. Bu çalışanlar dosyaların güvenliğinden ve her türlü hareketinden sorumlu olmalıdır.
- ✓ Sağlık kaydı arşivi en az 30 (Otuz) yıl süre ile saklanmalıdır.

**6.3.2.Sistem Güvenliği**

- ✓ Kurum bünyesinde hasta tanımlayıcı olarak TC Kimlik numarası baz alınacaktır. Hastanın sağlık kaydına erişimde özel olarak atanan protokol numarası kullanılabilir.
- ✓ Bilgi siteminde 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. mekanizmalar 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.
- ✓ 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.
- ✓ 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.
- ✓ Firma, CD, kartuş, kağıt vb. ortamında Kuruma ilettiği bilgileri tutanakla teslim edecektir.
- ✓ Sertifika tabanlı kimlik doğrulama yapılamadığı durumlarda password ve hash tabanlı kimlik doğrulama yapılacaktır.
- ✓ Kurum ile başka ağlar arasındaki tüm haberleşme şifreli yapılmalıdır.

**6.4.İNTERNET ERİŞİM VE KULLANIMI**

Kurum içinde güvenli internet erişimi için sahip olması gereken standartları belirlemektedir. 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 ne internet'in kurallarına, etiğe ve yasalara uygun kullanılmasının sağlanmasını amaçlamaktadır. Bütün kullanıcılar ve Bilgi İşlem yöneticileri aşağıdaki internet erişim ve kullanım kurallarına uymalıdır.

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

**6.4.2.** Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografik, oyun, kumar, şiddet içeren vs) yasaklanabilmelidir.

**6.4.3.** Anti-virus gateway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik (smtp, pop3, ayrıca mümkünse http ve ftp vs) virüslere karşı taranmalıdır.

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

**6.4.5.** 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, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, XoLoX, OpenNap, WinMX. v.b.)

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

**6.4.7.** Hiçbir kullanıcı internet üzerinden Multimedia Streaming yapamayacaktır.

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

**6.4.9.** Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemesi ve dosya indirimi yapılmamalıdır.

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

**6.4.11.** 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.

**6.4.12.** Üçüncü şahısların kurum internetini kullanmaları Bilgi İşlem sorumlularının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilir.

### 6.5. E-POSTA KULLANIMI

Kurumumuzda kullanılan ogu uzantılı e-posta kullanım hizmeti Rektörlük Bilgi İşlem Merkezi tarafından sağlanmaktadır.

### 6.6.ŞİFRE KULLANIMI

Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. Kurum çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifreleme yapmakla sorumludurlar.

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

**6.6.2.** 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.

**6.6.3.** Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

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

**6.6.5.** Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara yada elektronik ortamlara yazmaması konusunda eğitilmelidir.

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

**6.6.7.** Şifrelerin ilgili kişiye gönderilmesi “kişiye özel” olarak yapılmalıdır.

### 6.7.UZAKTAN ERİŞİM

Bu düzenleme herhangi bir yerden kurumun bilgisayar ağına erişilmesine ilişkin standartları belirlemektedir. Bu standartlar kaynakların yetkisiz kullanımından dolayı kuruma gelebilecek potansiyel zararları (hassas bilgilerin kaybı, prestij kaybı, içerideki sistemlerde meydana gelebilecek zararlar vs.) minimize etmek için tasarlanmıştır.

**6.7.1.** Uzaktan erişim için yetkilendirilmiş kullanıcılar kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

**6.7.2.** Internet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. (Aile Hekimleri, hastaneler, poliklinikler de 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.

**6.7.3.** Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Bağlantı güçlü bir şifre ile sağlanmalıdır. Daha fazla bilgi için Şifreleme Politikası’na bakınız.

**6.7.4.** Kurum çalışanları hiçbir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.

**6.7.5.** 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.

**6.7.6.** Çalışanlar Kurum ile ilgili yazışmalarında Kurumun dışındaki e-posta hesaplarını (örnek, irüs l, yahoo, mynet vs) kullanamazlar.

**6.7.7.** Uzaktan erişim yöntemi ile kuruma erişen bütün bilgisayarlar en son güncellenmiş anti irüs yazılımına sahip olmalıdırlar.

**6.7.8.** Kurum ağına standart dışı eğitim isteğinde bulunan organizasyon veya kişiler Bilgi İşlem biriminin özel izni ile geçici olarak izin verilebilir.

**6.7.9.** Periyodik olarak yapılan kontrollerde kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

**6.8.KABLOSUZ ERİŞİM**

Bu düzenleme kablosuz cihazların gerekli güvenlik tedbirleri alınmaksızın kurumun bilgisayar ağına erişimini engellemeyi amaçlamaktadır. Sadece bu düzenlemenin güvenlik kriterlerine uyan cihazlar kurumun bünyesinde kullanılabilir.

**6.8.1.** Bütün kablosuz erişim cihazları Bilgi İşlem birimi tarafından onaylanmış olmalıdır ve Bilgi İşlemin belirlediği güvenlik ayarlarını kullanmalıdır.

**6.8.2.** Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access (WPA,WPA2) şifreleme kullanılmalıdır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı doğrulama protokolleri kullanılabilmelidir.

**6.8.3.** Kablosuz erişim, Hastane Bilgi İşlem Bölümünün yetkisinde olacaktır. Kablosuz erişimler Yatan hasta ve Personellerin HBYS veri tabanındaki bilgileri ile giriş yapılmakta, bu girişler Kullanıcı Adı, Ip, Mac bazlı log sisteminde kayıt altına alınmaktadır.

**6.8.4.** Erişim cihazlarındaki firmware'ler düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.

**6.8.5.** Erişim cihazları kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.

**6.8.6.** Cihaza erişim için güçlü bir şifre kullanılmalıdır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır.

**6.8.7.** SSID numaraları yayınlanmamalıdır. Böylece sniffer tarzı cihazların otomatik olarak bu numaraları çözmesi engellenecektir.

**6.8.8.** Varsayılan SSID isimleri kullanılmamalıdır. SSID ayarı bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vs.

**6.8.9.** Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir.

**6.8.10.** Erişim Cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dahil olmalıdırlar.

**6.8.11.** Kullanıcı bilgisayarlarında kişisel firewall yazılımları yüklü olmalıdır.

**6.8.12.** Kritik yerlerde kullanıcılar VPN teknolojilerini kullanarak kurum ağına erişmelidirler.

**6.8.13.** Erişim cihazlarını bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir. Sistemde hackerler tarafından konulmuş casus bir erişim cihazı olabilir veya mevcut erişim cihazı resetlenmiş olup kurumun güvenlik politikalarına aykırı bir şekilde ayar yapılmış olabilir.

## 7. İLGİLİ DÖKÜMANLAR

- --