**1. AMAÇ:** Hastanemizde bilgi ve iletişim güvenliğini ve kişisel verilerin korunmasını sağlayıp ihlal olaylarına müdahale standartlarını belirlemek.

**2. KAPSAM:** Tüm hastanede bulunan bilgi yönetim ve iletişim araçlarını kapsamaktadır.

**3. KISALTMALAR:**

**SSL=** Açılımı **Secure Socket Layer**‘dır. Türkçe anlamıysa **Güvenli Giriş Katmanı**’dır.

**VPN=** Sanal özel ağ, uzaktan erişim yoluyla farklı ağlara bağlanmayı sağlayan İnternet teknolojisi. VPN sanal bir ağ uzantısı oluşturduğu için, VPN kullanarak ağa bağlanan bir cihaz, fiziksel olarak bağlıymış gibi o ağ üzerinden veri alışverişinde bulunabilir.

**TELNET=** Telnet, Internet ağı üzerindeki çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel isimdir.

**SSH ve RDP=**Şifreleme protokolleri

**MS AD, LDAP,** **sshkey** = Lightweight Directory Access Protocol veya kısaca LDAP TCP/IP üzerinde çalışan indeks servislerini sorgulama ve değiştirme amacıyla kullanılan uygulama katmanı protokolü.

BYS=Bilgi Yönetim Sistemi

**4. TANIMLAR:**

Netsupport, anydesk, radmin=Uzak masaüstü bağlantı programları

VLAN: Yerel ağ içerisinde çalışma grupları oluşturmak, yerel ağı anahtarlarla bölmektir.

**5. SORUMLULAR:** Tüm çalışan personel

**6. FAALİYET AKIŞI:**

**6.1.ERİŞİM VE YETKİ KONTROLÜ:**

**6.1.1.İnternet erişim ve kullanım:**

* Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar (lar) ı üzerinden internete çıkmalıdır. Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
* Kurum içinde free vpn, Proxy server, Tor, torrent, hotspot vb. uygulamaların kullanılması yasaktır.
* Kurumun politikaları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır.
* Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.
* Kurumun ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmalıdır.
* Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.
* İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.
* Mesai saatleri içerisinde iş ile ilgili olmayan video, müzik vb. aşırı veri çeken streming media kullanılmamalıdır.
* Mesai saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemelidir.
* Kurumsal alanlarda verilen internet hizmetinin şahsi iş ve işlemlerde kullanılamaz.
* Kurum network güvenliği açısından yönetilemeyen switch (Hub çoklayıcı) kullanılmamalıdır.
* Kurum network güvenliği açısından Hub, accespoint vb. cihazların bilgi işlem birimi izni dışında kurum networküne kesinlikle bağlanmamalıdır.
* İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz.
* Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumum bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir
* Kurum network güvenliği acısından mümkün olduğunca VLAN yapısı kullanılmalıdır.
* Merkezi olarak kullanılan BYS hizmetleri ve bakanlığımız uygulamalarına erişimin aksamaması, bant genişliği trafiğini sağlıklı yönetilmesi, siber saldırı tehditlerine karşın gerekli önlemleri almak için internet erişim düzenlemeleri gerekli hallerde İl Sağlık Müdürlüğü tarafından değiştirilir.
* Kamusal hizmetlerin yürütülmesinde erişim engeli yaşayan personeller için Ayrıcalıklı Erişim Talep Formuyla ıslak imzalı olarak İl Sağlık Müdürlüğüne resmi yazı ile bildirilerek gerekli değerlendirme yapılacaktır.
* Yasaklanması gereken siteler bilgi güvenliği yönetim komisyonu tarafından belirlenip onaylandıktan sonra uygulamaya konulacaktır. Ancak kurum bilgi güvenliğini tehlikeye düşürecek bir durumda (siber saldırı, veri kaybı vb.) onay alınması beklenmeden uygulamaya geçilebilecektir.

**6.1.2. Uzaktan Erişim:**

* Kurum sunucularına erişim için SSL VPN kullanılmalıdır.
* SSL VPN ile bağlantı verilen kullanıcılar sadece yetkisi olduğu sunuculara erişecek şekilde erişim kısıtlaması yapılmalıdır.
* SSL VPN gerçekleştirecek kullanıcılara (firma ve kurum personeli) mutlaka kurumsal gizlilik sözleşmesi imzalatılmalıdır. Eğer firmanın Kurumsal gizlilik sözleşmesi yok ise ilgili firma ile kurumsal gizlilik sözleşmesi de imzalanır.
* SSL VPN gerçekleştirecek kullanıcılar(firma personeli) mutlaka Kurumsal SSL VPN Erişim Talep Formunu imzalamalıdır.
* SSL VPN gerçekleştirecek kullanıcılar(kurum personeli) mutlaka Personel SSL VPN Erişim Talep Formunu imzalamalıdır.
* Kullanıcılara Sunucu yönetimi için sadece ihtiyaç duyulan portlara erişim yetkisi verilmelidir. Yetkili kullanıcıların erişimi için TELNET yerine SSH ve RDP gibi şifreli protokoller kullanılmalıdır.
* Kullanıcılara sadece yetkisi olduğu sunucularda erişim yetkisi verilmelidir.
* Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.
* Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir.
* Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, sshkey) ile yapılmalıdır.
* Kullanıcıların sunucu yönetim için sağlanan erişimde kısıtlı erişim yetkileri tanımlanmalıdır.
* Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir.
* Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri, Bilgi İşlem Birimine teslim edilmelidir. Bilgi İşlem Birimi nezaretinde ve tarafından yürütülmelidir.
* Kurumun yedekleme sistemlerine sadece kurum personeli erişim yapmalıdır. Firmaların yapacakları tüm işlemler Bilgi İşlem Birimi nezaretinde yürütülmelidir.
* Ağ cihazlarının şifreleri default şifrelerde bırakılmamalı ve kompleks şifreler (parola güvenliği ilkelerine uygun olarak) kullanılmalıdır.
* Kullanıcı bilgisayarlarına uzak bağlantıda kullanılan uygulamalarda (Netsupport, anydesk, radmin vb. programlarda) Bağlantı sağlanacak kullanıcının onayı ile bağlantı sağlanmalıdır. Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.
* Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeler yapılmış olmalıdır.
* Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

**6.1.3. Kablosuz erişim:**

 Hastanenin bazı bölüm ve birimlerinde mevcuttur. Hastane bölümlerinde çalışan tüm personelin otomasyon sistemine girdiği, kullanıcı adı ve parolası şifreli bir şekilde veri tabanında tutulmaktadır. Her kullanıcının yetkileri otomasyon üzerinden birim yöneticisi tarafından onaylanarak belirlenir. Hastane içinde içeriği hasta mahremiyetini etkileyecek olan bilgiler otomasyon sisteminde yetkilendirilip, kimseye gösterilemez. Yalnızca başhekimliğin onay verdiği kullanıcılara görme yetkisi verilir. Kullanıcıların sisteme kaydettiği nitelikli hizmetlerin hiçbiri yönetim onayı olmadan, bilgi işlem personeli haricinde hiçbir personel tarafından silinemez.

Gün içerisinde hastane internet ağına bağlı olan tüm bilgisayarların hangi zamanda, hangi internet sitesine bağlandığını, ne kadar süreyle o sayfada kaldığı gibi tüm bilgiler Çorum İl Sağlık Müdürlüğü bünyesinde bulunan güvenlik duvarında yedeklenip log cihazında log’ları kayıt altına alınmalıdır. Oluşabilecek virüs saldırıları için Çorum İl Sağlık Müdürlüğü bünyesinde bulunan merkezi anti virüs lisansı ile bilginin güvenliği sağlanmalıdır. Fiziksel güvenlik duvarı ve anti virüsün güncellemelerini ve üst versiyon yüklenmelerini Çorum İl Sağlık Müdürlüğü bünyesinde bulunan yönetim konsolu üzerinden takip edilip yapılmaktadır.

**6.2.FİZİKSEL VE ÇEVRESEL GÜVENLİK**

Hastanemizde sunucuların bulunduğu oda şifreli kapı ile kilitlenmektedir. Hastane yönetimi tarafından yetkilendirilmiş kişiler **SUNUCU ODASI GİRİŞ ÇIKIŞ KONTROL FORMU** ile sunucu odalarına giriş ve çıkış yapabilmektedirler. Sunucu odasında sel ve su basmaları için gider bulunmaktadır. Yangın durumları için FM 200 gazlı söndürme sistemi yerleştirilmiş olup yangına müdahale edilebilmektedir. Elektrik kesintilerinden etkilenmemesi için sunucular hastanemiz kesintisiz güç kaynağına bağlıdır. Sunucuların sıcaklık ve nemden etkilenmemesi için günde 2 kez olarak **SICAKLIK NEM VE ISI TAKİP FORMU** ile takip edilmektedir. (Sıcaklık: 18-22 ℃ Nem Oranı: %45 - %70 aralığında olmalıdır.) Sunucu üzerinde çalışan sistemler kötü yazılımlardan antivüris programları ile korunmakta ve antivüris programlarının güncelliği bilgi işlem birimi tarafından takip edilmekte ve sağlanmaktadır.

Sunucular dışardan erişimini engellemek için güvenlik duvarının ardında bulunmaktadır.

**6.3.İLETİŞİM GÜVENLİĞİ**

Hastanemizde iletişim güvenliği 6/07/2019 tarih ve 30823 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri kapsamında sağlanmaktadır.

Hastanemizde kritik veriler internete kapalı, fiziksel güvenliği sağlanmış bir ağda tutulmaktadır. Bu verileri kullanabilen cihazlara erişim kontrolü sağlanmakta ve log kayıtları değiştirilmeye karşı şifreli bir şekilde koruma altına alınmaktadır.

Hastanemize ait veriler, yedekleri kendi ağ sistemimiz ve offline ortamda saklanmakta. Bulut depolama hizmetlerinde saklanmamaktadır.

Sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmamaktadır.

Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler hastanemizde yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda (dizüstü bilgisayar, mobil cihaz, harici bellek vb.) bulundurulmamaktadır.

BYS firması ile gizlilik sözleşmesi yapılmakta ve firmadan sistemin ulaşılabilir bir arka kapısı olmadığına dair taahhüt alınmaktadır.

**6.4. BİLGİ GÜVENLİĞİ İHLAL OLAY YÖNETİMİ**

Bilgi güvenliği ile ilgili olaylar derhal rapor edilmelidir. Raporun verileceği ve bilgi sunulacak bölümler aşağıda belirtilmiştir. Kurum politikalarına uymayan her tür davranış, kurum bilgi güvenliği prensipleri ve talimatlarına aykırı her tür bilgi paylaşımı, uygunsuz bilgisayar/laptop kullanımı, yetkisiz girişler, uygun olmayan yerde yetkisiz personelin görülmesi, bilgisayar varlıkları ile ilgili arıza, hırsızlık, kaybolma vb. olumsuzluklar bilgi güvenliği olayı kapsamına girmektedir.

Hastanemizin web sitesinde tek tık ile ulaşabilecekleri bilgi güvenliği ihlal bildirimi alanı mevcuttur.

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

Olay halinde web sitesi üzerinden, kurum bilgi güvenliği yetkilisine bildirilerek işlem yapılmalıdır.

İhlal bildirimi hakkında tüm kullanıcılara bilgi güvenliği eğitimleri veya resmi yazı ile farkındalık oluşturmak için bildirimler yapılmalıdır.

Virüs, izinsiz giriş, trojen, spware vb. bulguları için, sistem sunucu servis problemleri için, donanım ve network problemleri için, veri kaybı bilgilere yetkisi erişim durumlarında, hırsızlık kaybolma, yanma, kırılma vb. durumlar için, uygunsuz davranışlar ve politikaya uymayan kişiler için, ağ üzerinden saldırılar için, her türlü bilgi güvenliği ihlal olayları durumunda belirtilen iletişim kanalları yöntemiyle ihlal bildirimi yapılmalıdır.

Kullanıcı, Kurumun e-posta sistemini taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Kullanıcılar bu tür özelliklere sahip bir mesaj alındığında kurum bilgi güvenliği sorumlusuna haber verilmelidir. Ayrıca kurumların web sitelerinde yer alan Olay Bildirim Formunu kullanarak veya “<https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir>” adresinden ihlal bildirimi yapılmalıdır.

**6.5. KİŞİSEL VERİLERİN KORUNMASI**

 Kullanıcılar, hasta ile ilgili bilgileri girilir, muayene ve reçete girildikten sonra hasta kaydı kapanır. Tekrar kullanıcılar bilgileri değiştirmek istediklerinde kaydı tekrar açarlar ve bu değiştirme işlemleri log kayıtlarında ayrı bir veri tabanında saklanır. Kişisel bilgiler kişinin kendisi veya mahkeme tarafından istenildiği takdirde verilir.