1. **AMAÇ:** Hastanemizde bulunan bilgi yönetim sistemleri ile ilgili dış ortamdan iç ortama erişim kurallarının tanımlanmasıdır.
2. **KAPSAM:** Bilgi İşlem Birimi

**3. KISALTMALAR:**

**SSL=** SSL internet ortamında çok karşılaşılan kavramlardan biridir. Genellikle alışveriş sitelerinde oldukça sık rastlanmaktadır. SSL’in açılımı **Secure Socket Layer**‘dır. Türkçe anlamıysa **Güvenli Giriş Katmanı**‘dır.

**VPN=** Sanal özel ağ, uzaktan erişim yoluyla farklı ağlara bağlanmayı sağlayan internet 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.

**4. TANIMLAR:**

Netsupport, anydesk, radmin=Uzak masaüstü bağlantı programları

**5. SORUMLULAR:** Bilgi İşlem Personelleri, Hastane Yönetimi

**6. FAALİYET AKIŞI:**

* 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.
* Yapılan bağlantılarda “***DIŞ ORTAMDAN İÇ ORTAMA BAĞLANTILARDA TUTULAN KAYIT FORMU*”** na kayıt edilmelidir. Kayıtlar Sağlık Bakanlığı Arşiv Mevzuatına göre saklanmalıdır.