1. AMAÇ

Bu prosedürün amacı, T.C. Sağlık Bakanlığı ..... Hastanesi bilgi erişimi için kullanılacak yöntemlerin oluşturulması ve uzaktan erişim ile ağa bağlanacak yabancı kaynakları belli kurallara tabi tutarak bilgi ve bilgi sistemleri güvenliğinin sağlanmasıdır.

2. KAPSAM

Bu prosedür, T.C. Sağlık Bakanlığı ..... Hastanesinin, bütünüyle bilgiye erişimi kurallarını kapsamaktadır.

3.SORUMLULUKLAR

Bu sürecin işletilmesinden ise BGYS Ekibi ve T.C. Sağlık Bakanlığı ..... Hastanesi makamı sorumludur.

4. UYGULAMA

4.1. Erişim Kontrolü

..... Hastanesi tarafından, Bilgi Güvenliği Prosedürü'ne uygun olarak, Erişim Kontrol Politikası oluşturulmuştur.

4.1.1.4.2. Erişim Kontrolü İçin İş Gereklilikleri

4.1.2.Erişim Kontrolü Politikası

..... Hastanesi bilgi güvenliği için alınabilecek tüm önlemleri alarak sağlıklı bir ağ yapısı ve bilinçli kullanıcılarla desteklenmiş bir kullanıcı grubu edinmeyi amaçlamaktadır. İl sağlık müdürlüğü bilgi güvenliği politikalarına tam uyumlu server ve HBYS alt yapısı kullanarak oluşturulan tüm parola, erişim, eposta kullanım prosedürlerine bağlı kalmak şartıyla uzaktan erişim yapacak herhangi bir kullanıcı bilgi işlem sorumlusu kontrolünde bilgisayarlara erişebilecektir.

4.1.3.Ağlara ve Ağ Hizmetlerine Erişim

..... Hastanesinde 1 adet ağ bulunmaktadır. İl Sağlık Müdürlüğü ve Müdürlüğü bağlı Sağlık tesisleri ile SBA (Sağlık Bilişim Ağı) üzerinden belirli protokollerle haberleşmektedir. Erişimler SBA devleri arası ve bu ağlardan dışarıya verilen internet ulaşımıdır. Misafir bağlantısına izin verilmemektedir

4.1.4.Kullanıcı Erişim Yönetimi

4.1.5.Kullanıcı Kaydetme ve Kayıt Silme

Kullanıcı oluşturma ..... Hastanesi Bilgi İşlem birimi tarafından ilgili loglar kullanılarak kayıt edilmekte ve istihdamın sonlandırılmasında da İşten ayrılış ekranı kullanılarak kullanıcı pasif hale getirilmektedir.

4.1.6.Kullanıcı Erişimine İzin Verme

Kullanıcı oluşturulduktan sonra, çalışacağı birime göre SBYS yetki ve rolleri tanımlanmaktadır. Birim değişikliğinde HBYS Yetki Değişikliği sadece bilgi işlem departmanı tarafından uygun görüldüğü gibi sağlanmaktadır.

4.1.7.Ayrıcalıklı Erişim Haklarının Yönetimi

Ayrıcalıklı erişim hakları, bilgi işlem alt yapısında kullanılan tüm cihazlar üzerinde yalnızca sistem-ağ yöneticisine verilmektedir. Diğer personelin ayrıcalıklı erişim hakları kısıtlanmıştır. Sunucu üzerinde yönetici (administrator) olarak yalnızca sistem yöneticisi ayrıcalıklı erişim hakkına sahiptir. VTYS ayrıcalıklı erişim hakları, hizmet alınan yüklenici firma sorumluluğundadır. Yeni bir erişim hakkı tanımlanması durumunda AYRICALIKLI ERİŞİM HAKKI TALEP FORMU kullanılmaktadır

4.1.8.Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi

..... Hastanesi, kimlik doğrulama PAROLA YÖNETİM POLİTİKASI kullanılarak yapılmaktadır. Her kullanıcı kurumun sistemlerine belirlenen kullanıcı adı ve parolasıyla girmektedir.

4.1.9.Kullanıcı Erişim Haklarının Gözden Geçirilmes

Kullanıcı erişim hakları Yönetimin Gözden Geçirme toplantılarında gözden geçirilerek gerekli değişiklikler sağlanır

4.1.10. Erişim Haklarının Kaldırılması veya Düzenlenmesi

Erişim hakları ..... Hastanesi personel istihdamının sonlandırılması durumunda İşten Ayrılma Prosedürü kullanılarak erişim hakları kaldırılır. Erişim haklarının gözden geçirilmesi sonucunda herhangi bir düzenleme yapılması durumunda SBYS yetki ekranları ile düzenlenir.

4.3. Kullanıcı Sorumlulukları

4.3.1.Gizli Kimlik Doğrulama Bilgisinin Kullanımı

..... Hastanesi kullanıcılara teslim edilen parolaların ifşa edilmeyeceğine dair taahhüt Personel Gizlilik Sözleşmesi ile alınmaktadır.

4.4.Hizmet Alımlarında Sistem ve Uygulama Erişim Kontrolü

4.4.1.Bilgiye Erişimin Kısıtlanması

Hizmet alınan yüklenici tarafından yapılacak erişimler KURUMSAL GİZLİLİK TAAHHÜTNAMESİ kullanılarak yapılmalıdır. Yüklenici personeli tarafından erişimler kurum tarafından oluşturulmuş kimlik doğrulama bilgisi (parolalar) kullanılarak sağlanmaktadır.

4.4.2.Güvenli Oturum Açma Prosedürleri

Sunucu, SQL Server ve ORACLE VTYS ‘ ne erişim kimlik doğrulama ile yapılmaktadır.

4.4.3.Parola Yönetim Sistemi

..... Hastanesi personeli tarafından kullanılmakta olan parolalar işletim sistemi parolalarıdır. Bu parolaların kullanımına ilişkin PAROLA YÖNETİMİ POLİTİKASI oluşturulmuş ve kullanılmaktadır.

4.4.4.Ayrıcalıklı Destek Programlarının Kullanımı

Hizmet alımlarında yüklenici personelleri tarafından sistem ve uygulamaların kontrollerini geçersiz kılabilecek programlarının kullanılmaması konusunda taahhüt, KURUMSAL GİZLİLİK TAAHHÜTNAMESİ ile kayıt altına alınmaktadır.

5. SORUMLULUK

Bu politikanın işletilmesinden ..... Hastanesi Bilgi Güvenliği Ekibi ve Bilgi Güvenliği Yetkilisi Personeli sorumludur.