UZAKTAN ERİŞİM PROSEDÜRÜ

1.AMAÇ: Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumlar kapsamındaki bilgi ve bilgi işleme tesislerine yapılacak olan uzaktan erişimlerin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesine imkân verecek bir sistemin işlem basamaklarını tanımlamaktır.

2.KAPSAM: Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumlar bünyesindeki bilgi ve bilgi işleme tesislerine uzaktan erişim sağlanması işlem basamaklarını kapsar.

3.KISALTMALAR:

BGYS: Bilgi Güvenliği Yönetim Sistemi

KVKK: Kişisel Verileri Koruma Kurumu

SBA: Sağlık Bilişim Ağı

4.TANIMLAR:

Truva Atı: Faydalı program gibi görünen fakat çalıştırıldığında bilgilerimize veya diğer programlarımıza zarar veren yazılımdır.

5.SORUMLULAR:

Bu sürecin işletilmesinden ise BGYS Komisyonu ve Hatay İl Sağlık Müdürlüğü makamı sorumludur.

6.FAALİYET AKIŞI:

6.1 6698 sayılı kanunun açıklanması amacıyla KVKK tarafından yayımlanan 2018/10 sayılı karar uyarınca, özel nitelikli verilerin işlendiği, muhafaza edildiği elektronik ortamlara uzaktan erişim yapılırken, en az iki kademeli kimlik doğrulama sistemi kullanılması yasal bir zorunluluktur. Diğer sistemler için de çok faktörlü kimlik doğrulama yapılması tercih edilir.

6.2. Erişim kontrollerinin uygulanabilmesi maksadıyla, hedef bilgisayarlara sabit IP adresi verilir. Yapılacak erişim "erişim yapacak kişi, hedef bilgisayar IP adresi (VLAN adresi) ve kullanılacak port/uygulama" bazında sınırlandırılır.

6.3. Uzak bağlantı yapılacak uygulamalara/kaynaklara erişimin daha kontrollü olarak yapılması gerekiyorsa, bağlantılar bu amaçla ayrılan bir terminal/vekil sunucu üzerinden de yapılabilir.

6.4. Uzak bağlantı yapacak istemci bilgisayarların IP adresleri/blokları biliniyorsa, hedef bilgisayara sadece belirtilen IP adreslerinden erişim yapılması için gerekli ayarlar yapılır.

6.5 Uzak erişim için yapılan bağlantıda boşta kalma süresi (herhangi bir işlem yapılmadığı takdirde connection time out süresi) 1 (bir) saati geçemez.

Bağlantı yapan kişinin, hedef bilgisayarda oturum açma iznine sahip bir kullanıcı olması gerekir.

6.6. Bağlantı yapan kişinin, hedef bilgisayarda oturum açma iznine sahip bir kullanıcı olması gerekir.

6.7. Hedef bilgisayarda uzak bağlantı için kullanılan servis/ara yüz vasıtasıyla, bilgisayara erişecek kullanıcılar "kullanıcı adı ve/veya IP adresi" bazında sınırlandırılır. Bu yöntemle sadece yetki verilen kullanıcıların/bilgisayarların uzaktan erişim yapması sağlanır.

6.8. Bağlantı yapan kullanıcının hedef bilgisayardaki oturum açma, oturum kapatma gibi kullanıcı hareketleri kayıt altına alınır ve söz konusu iz kayıtları en az 1 (bir) yıl süre ile saklanır.

6.9. Uzaktan çalışma; ağırlıklı olarak yükleniciler, tedarikçiler, iş ortakları çalışanları gibi Müdürlüğümüz ile geçici olarak iş ilişkisi olan kişiler tarafından yapılır.

6.10. Uzaktan çalışacak kişi, Müdürlüğümüz birimleri ile sözleşme imzalayan üçüncü taraf personeli ise kuruma ait bilgisayar verilemiyorsa, uzak çalışma için hangi tip cihaz kullanılacağı ve cihazlarla ilgili tedbirler ilgili sözleşme ve protokolde bulundurulmalıdır. Bu cihazlarla ilgili bilgiler kuruma resmi olarak bildirilmelidir.

6.11. Doğrudan uygulama erişimleri dahil uzaktan çalışma hiçbir çeşidinde sahibi bilinmeyen, herkes tarafından erişilebilen (internet kafe, otel bilg. Kiosklar vb. kullanılmaz. Uzaktan erişim daha önce bildirilmiş sabit İP ye sahip güvenli (ev, işyeri ağı gibi) bir ağ üzerinden bilgileri verilen bir bilgisayar ile yapılmalıdır. Güvensiz ağ üzerinden, kişisel veya sahibi bilinmeyen/herkes tarafından erişilebilen cihazlar ile uzak masaüstü yapılması durumunda gerekli yasal ve idari yaptırımlar uygulanır.

6.12.*Uzak çalışma için kullanılacak cihazlarda asgari düzeyde aşağıda belirtilen güvenlik tedbirleri alınmış olmalıdır:*

6.12.1 Cihazlara kişisel güvenlik kurulu ve aktif halde olmalıdır.

6.12.2. İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamaları otomatik güncelle seçeneği seçilerek güncel halde tutulması sağlanmalıdır.

6.12.3. Virüs, fidye yazılımları, truva atları ve benzeri zararlı yazılımlardan korunmak için uygun bir korunma yazılımı tedarik edilmeli ve yazılım ile imza dosyaları güncel tutulmalıdır.

6.12.4. Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip kullanıcı açılmalı, yönetici yetkisi ile uzaktan çalışma yapılmamalıdır.

7.İLGİLİ DOKÜMANLAR: