TAŞINABİLİR ORTAM YÖNETİMİ PROSEDÜRÜ

1.AMAÇ: Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumlar bünyesinde çalışan personele tahsis edilen veya personel tarafından kullanılan taşınabilir medya ve mobil cihazların kullanımında risklerin önlenmesi ve bilgi güvenliği kurallarını tanımlamaktır.

2.KAPSAM: Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumlar bünyesinde çalışan personele tahsis edilen veya personel tarafından kullanılan taşınabilir medya ve mobil cihazların kullanımında risklerin önlenmesi ve bilgi güvenliği kurallarını kapsar.

3.KISALTMALAR:

BGYS: Bilgi Güvenliği Yönetim Sistemi

4.TANIMLAR:

Bitlocker: Windows işletim sistemlerinde sunulan bir veri güvenliği, dosya şifreleme sistemidir.

LUKS ve LVM: Linux işletim sistemlerinde sunulan bir veri güvenliği, dosya şifreleme sistemidir.

File Vault: Apple Mac OS İşletim sistemlerinde sunulan bir veri güvenliği , dosya şifreleme sistemidir.

5.SORUMLULAR:

Hatay İl Sağlık Müdürlüğünde faaliyet gösteren tüm personel sorumludur, bu sürecin işletilmesinden ise BGYS Komisyonu ve Hatay İl Sağlık Müdürlüğü makamı sorumludur.

6.FAALİYET AKIŞI

6.1.Müdürlüğümüz, İlçe Sağlık Müdürlükleri ve bağlı sağlık tesisleri bünyesinde yürütülmekte olan iş ve işlemler için envantere kayıtlı, fiziki olarak bir noktadan başka bir noktaya iletilebilen tüm taşınabilir medya cihazlarını (Taşınabilir Sabit Disk, USB Hafıza ünitesi, CD/DVD v.s.)ve tüm taşınabilir Bilgi işleme yapabilen elektronik aygıtları [diz üstü bilgisayar, tablet(mobil bilgisayar ve akıllı cep telefonlarını)] ifade eder.

6.2. Taşınabilir Medya Cihazlarında "Gizli Bilgi" ve "Çok Gizli Bilgi" bulundurulmamalıdır, bulundurulması gerekli ise şifrelenmelidir. Şifreleme yapılırken kullanılacak algoritmalar en az AES256 veya SHA256 'yı içermelidir.

6.2.1. Taşınabilir Bilgi İşleme Cihazları, kullanılmak üzere bir başka kişiye verilmemelidir.

6.2.2. Taşınabilir cihazlar üzerinden Hatay İl Sağlık Müdürlüğü, İlçe Sağlık Müdürlükleri ve bağlı sağlık tesisleri dışındaki kablosuz ağlara bağlanmak gerekirse, kablosuz ağın güvenli (*WPA-2/PSK veya WPA-2/Enterprise)* olup olmadığı kontrol edilmeli, değilse bu bağlantı gerçekleştirilmemelidir. Kurum dışında kullanılan kablosuz ağlarda "https" olmayan web sitelerine kesinlikle bilgi girişi yapılmamalıdır.

6.2.3.Tüm taşınabilir bilgi işleme cihazları anti-virüs korumalı olmalı ve bu yazılımlar hiçbir şekilde devre dışı bırakılmamalıdır.

6.2.4. Taşınabilir bilgi işleme yapan cihazlar araba ve diğer ulaşım araçları, otel odaları, konferans merkezleri ve toplantı salonları gibi yerlerde hırsızlığa karşı gözetimsiz bırakılmamalıdır.

6.2.5. Taşınabilir bilgi işleme yapan cihazlara lisanssız, görevle alakası olmayan, sisteme zarar verme ihtimali olan yazılımlar yüklenmemelidir.

6.2.6. Taşınabilir bilgi işleme yapan cihazların kaybolması durumunda, zaman kaybetmeden Müdürlük Bilgi İşlem Birimine olay bildirimi yapılmalı ve Taşınır Kayıt Kontrol Birimine haber verilmelidir.

6.2.7. Taşınabilir bilgi işleme yapan cihazların açık alanlarda kullanımı sırasında omuz sörfüne (shouldersurfing) karşı dikkatli olunmalıdır. Sizden başka birinin ortamda bulunduğu durumlarda parola girilmemelidir. Zaruri durumlarda hızlı bir şekilde tuşlara basılarak işlem yapılır.

6.2.8.Bir sistemden diğer bir sisteme veri transferi ihtiyaçları hariç"Gizli" ve"Çok Gizli" bilgiler taşınabilir medya cihazlarında saklanmayacaktır. Bu kategorideki kritik bilgiler kurumsal dosya sunucularında veya kurumsal sistemlerde muhafaza edilir.

6.2.9.Bütün Taşınabilir medya cihazları kullanım öncesi virüs taramasından geçirilir.

6.2.10. Bakım amacı ile firma mahalline gönderilmesi gereken ve kritik bilgi içeren taşınır medya ve cihazlardaki verilerin yedeği alındıktan sonra; medya üzerindeki veriler bir daha geri döndürülemeyecek şekilde güvenli silme yöntemleri ile temizlenir.

6.2.11. Taşınabilir medya cihazları, sürücü şifrelenmesi yapılmamış ise, her kullanım öncesi disk biçimlendirilmeden içerisine veri aktarılmamalıdır.

6.2.12. Taşınacak verinin de tehdit unsuru içeren herhangi bir yazılım içermediğine emin olunmalıdır. Kaynağından emin değilsek, veri mutlaka anti-virüs taraması yapılmadan herhangi bir yere veri taşınamaz.

6.2.13. Veri USB disk ya da taşınabilir sabit disk ile taşınacaksa; bilgisayara takıldığında sağlıklı çalıştığından emin olunmalıdır. Yine aynı şekilde bu diskler bilgisayardan çıkartılırken de donanım, güvenli şekilde kaldır diyerek çıkartılmalıdır. Aksi takdirde veri kaybı oluşabilir.

6.2.14. Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir. Özellikle sabit diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır.

6.2.15.CD ve DVD'lerde veri saklamak için kaliteli medyalar kullanmalı, düşük hızla yazdırmalı, alt yüzeye mümkün olduğunca temas etmemeli, nem ve ışık almayan ortamlarda fazla sıkıştırmadan saklanmalıdır.

6.2.16. Taşınabilir medya cihazları çalışma masasında veya bilgisayarda güvensiz şekilde bırakılmamalıdır.

6.2.17. Kurum içinde ya da dışında bulunabilecek, sahibi belli olmayan, taşınabilir medya cihazları kurum bilgisayarlarına takılmamalı, bu materyaller ivedi olarak Bilgi İşlem Birimine teslim edilir.

6.2.18. Taşınabilir bilgi işlem cihazları kurum dışında kullanılacaksa bilgi güvenliği için mutlaka bütün disk şifrelenmelidir. Microsoft Windows İşletim Sistemleri için; BitLocker Sürücü Şifrelenmesi, GNU/Linux İşletim Sistemleri için; LUKS ve LVM ile Sürücü şifrelenmesi, Apple Mac OS İşletim Sistemleri için; File Vault Sürücü şifrelemesi kullanılır.

6.2.19. Hatay İl Sağlık Müdürlüğü Taşınabilir Medya ve Cihaz Kayıtları, bakanlığımıza hizmet veren Çekirdek Kaynak Yönetim Sistemi(ÇKYS) içerisindeki Malzeme Kaynak Yönetim Sistemi(MKYS) programı aracılığı ile takip edilir.

6.2.20. Taşınabilir medya ve cihazları, kullanan kişiler tarafından periyodik olarak şifreli şekilde yedeklenir.

6.2.21. Taşınabilir bilgi işlem cihazlarının yazılım sürüm ve yama güncelleştirmeleri periyodik olarak yapılır.

6.2.22. Bir bilgi sadece taşınabilir medya ortamında saklanıyorsa, bozulma/kaybolma gibi ihtimallere karşı bir başka medya ortamında da yedeklenmesi tavsiye edilir. Veriler çok kıymetli ise yedeklenen medya ortamı, doğal afet vb. tehditlere karşı önlem olmak üzere fiziksel olarak farklı bir yerde muhafaza edilir.

6.2.23.Yeni medya teknolojilerinin ortaya çıkması nedeniyle üç yıldan uzun süredir eski teknolojilerin kullanıldığı bir medya ortamında saklanan verilerin daha yeni bir medya ortamına taşınması tavsiye edilir.

6.2.24.Elektronik medya da dâhil tüm taşınabilir ortamlar, kullanılmadığı zamanlarda içinde bulunan verilerin gizlilik derecesi dikkate alınarak fiziki güvenlik tedbirleri alınmış kasa, dolap, çekmece gibi ortamlarda saklanır.

7.İLGİLİ DOKÜMANLAR: