T.C.
DENİZLİ VALİLİĞİ
İL SAĞLIK MÜDÜRLÜĞÜ
VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ

1. AMAÇ

Müdürlüğümüz ve Bağlı Sağlık Tesisleri çalışanlarının; kurum bünyesinde bulunan Sistem, Bilgi ve Varlıkların Gizlilik, Bütünlük ve Erişilebilirlik özelliğini garantilemek ve kurumun itibar ve güvenilirliğini zedelememek için yapması ve uyması gereken iş kurallarını tarif etmektir.

2. KAPSAM

Denizli İl Sağlık Müdürlüğü Bilgi Güvenliği Yönetim Sistemi Politika metninde yer alan kapsam maddesinde belirlenmiş olan kapsamdır.

3. TANIMLAR

İSM: İl Sağlık Müdürlüğü

4. SORUMLULUKLAR

Tüm Çalışanlar bu kurallara uymaktan, ilgili kurum yöneticileri ise çalışanların bu kurallara uyumunu sağlamaktan sorumludur.

5. UYGULAMA

5.1. Genel Koşullar

5.1.1. Çalışanlar günlük işlerinin ifasında istisnai durumlar hariç sadece kurum tarafından kendilerine tahsis edilmiş olan bilişim kaynaklarını (yazılım, donanım, erişim vb.) kullanacaktır.

5.1.2. İstisnai durumlarda, çalışanın bağlı bulunduğu en üst düzey yönetici ve Sağlık Bilgi Sistemleri Biriminin ortak kararı ile kurumsal işlerde şahsi cihaz ve bilişim kaynakları kullanılabilir.

5.1.3. Bilgisayarlara ek bir donanım kurulumu sadece Sağlık Bilgi Sistemleri Biriminin sorumluluğundadır. Sağlık Bilgi Sistemleri Biriminin onayı olmaksızın ek donanım kurulumları hiçbir şekilde ve sebeple çalışanlar tarafından yapılamaz.

5.1.4. Kurumun iş gereği tahsis etmiş olduğu masaüstü bilgisayarlar, dizüstü bilgisayarlar, tabletler, masa telefonları ve dect telefonlar iş gereği kullanılır, özel işlerde kullanılmaz, kurum bilişim kaynakları üzerinde kişisel veriler bulundurulmaz.

5.1.5. Bütün masaüstü ve dizüstü bilgisayarlar mesai bitiminde kapatılır. Bu işlem ilgili işletim sistemindeki "Bilgisayarı Kapat" düğmesine basılarak yapılmalı, "Uyku" seçeneği seçilmemelidir.

5.1.6. Bütün masaüstü ve dizüstü bilgisayarlar kullanılmadıkları durumlarda otomatik olarak en fazla 10 dakika içerisinde şifreli ekran korumasına geçmelidir.

5.1.7. Çalışanlar; açık olarak korumasız şekilde bırakılan ve kendisinin kullanım ve erişim yetkisi olmayan bilgisayarları ve/veya diğer donanım ve erişimleri kullanamaz.

5.1.8. Çalışanlar, kurumda başka bir çalışanın kişisel bilgisayarının korumasız olarak bırakıldığını gördüğünde, derhal kişisel bilgisayarın sahibine ve/veya bu çalışanın bağlı olduğu bölümdeki yetkili kişiye durumu bildirerek gerekli önlemin alınması konusunda uyarıda bulunmalıdır.

5.1.9. Bütün Cep Telefonu ve PDA (Personal Digital Assistant) cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, vs.) özellikleri aktif halde olmamalıdır ve mümkünse antivirüs programları ile yeni nesil virüslere karşı korunmalıdır.

5.1.10. Çalışanlar, kurum bilişim kaynaklarını kullanarak herhangi bir suç unsuru içeren olaylara karışmamaya azami özen göstermelidir.
5.1.11. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (DoS saldırısı, port-network taraması, packet sniffing, packet spoofing vb.) eylemlere girişilmez.
5.1.12. Güvenlik duvarını aşmak için VPN, Proxy programları(Psiphon, Hotspot vb.) kullanmak kesinlikle yasaktır.
5.1.13. Kurumsal verilerin, çalışan gizliliğine ve mahremiyetine özel önem gösterilmelidir. Kurum bilgileri, çalışanlar ile ilgili bilgiler hiçbir şekilde ve sebeple kurum dışından üçüncü kişilerle paylaşılmaz.
5.1.14. Çalışanlar kendilerine verilmiş yetkiler çerçevesinde hareket eder; kurumdaki gizli ve hassas bilgileri görmeye, elde etmeye ve üçüncü şahıslar ile paylaşmaya teşebbüs kesinlikle yasaktır.
5.1.15. Kurumun güvenilirliğini ve üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak amacıyla her çalışan, görevi gereğince kendisinde bulunan ve yaptığı işlerle ilgili sahip olduğu her türlü belgeyi, veriyi ve bilgiyi korur ve kurum tarafından bu bilgilerin her zaman kendisinden istenebileceği ve alınabileceğini bilerek hareket eder.
5.1.16. Kurumda Sağlık Bilgi Sistemleri Biriminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb) sunucu niteliğinde bilgisayar ve cihaz bulundurulamaz.
5.1.17. Tüm faks-modem üniteleri ile haberleşme ve internet erişim donanım yazılımlarının kurulması ve ayarları sadece ilgili kurumun Sağlık Bilgi Sistemleri Biriminin yetkisindedir.
5.1.18. Sağlık Bilgi Sistemleri Birimi personeli ve Sağlık Bilgi Sistemleri Birimi tarafından diğer birimlerde yetkili kılınan teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilemez.
5.1.19. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilemez, ivedilikle Bilgi İşlem Birimine haber verilir.
5.1.20. Kurum bilişim sistemlerinde kullanılan yazılımların; yüklenmesi, silinmesi ve değiştirilmesi Sağlık Bilgi Sistemleri Biriminin sorumluluğunda olup bahsi geçen eylemler hiçbir şekilde ve sebeple çalışanlar tarafından gerçekleştirilemez.
5.1.21. Kurum bilgisayarlarına hiçbir şekilde ve sebeple Sağlık Bilgi Sistemleri Birimi tarafından belirlenmiş yazılımlar dışında farklı bir yazılım yüklenemez.
5.1.22. Kurum bilgisayarlarına hiçbir şekilde ve sebeple oyun veya eğlence amaçlı yazılımlar yüklenemez.
5.1.23. Sağlık Bilgi Sistemleri Biriminin bilgisi ve onayı olmadan herhangi bir yazılım, bir lisanslama yükümlülüğü olmasa bile (Freeware, Shareware, General Public License vb.), Internet, e-mail veya dışarıdaki bir network sisteminden kopyalanarak kurum bilişim sistemlerinde kullanılamaz.
5.1.24. Kurumda kullanılan yazılımlar çalışanlar tarafından hiçbir şekilde ve sebeple kopyalanamaz, çoğaltılamaz ve üçüncü şahıslarla paylaşılamaz.
5.1.25. Bütün bilgisayarda kurumun lisanslı anti virüs yazılımı yüklenmiş olmalıdır.
5.1.26. Anti virüs yazılımı yüklü olmayan bilgisayar ağa bağlanmaz ve hemen Sağlık Bilgi Sistemleri Birimine haber verilir.

5.1.27. Virüs bulaştığında, sistemin cevap verme zamanında yavaşlama, geri döndürülemeyen dosya kayıpları, değişiklik tarihlerindeki farklılıklar, dosya büyüklüklerinde artmalar, bilgisayarlarda donanım ve yazılım olarak tümden arızalar vb. şekilde belirtiler karşımıza çıkar. Bu durumlardan bir veya birden fazlasıyla karşılaşıldığında hemen Sağlık Bilgi Sistemleri Birimine haber verilir.
5.1.28. Kurum bünyesinde zararlı programlar (örneğin, virüsler, solucanlar, truva atı, e-mail bombaları vb.) oluşturulamaz ve dağıtılamaz.
5.1.29. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmaz, kaynakların paylaşıma açılması gerekliliği halinde gerekli güvenlik tedbirleri alınır.

5.2. Fiziksel ve Çevresel Güvenlik
5.2.1.1. Kurum üst yönetimi tarafından yetkilendirilmediği sürece hiçbir çalışan kurum binaları içinde ve dışında fotoğraflama, görüntüleme, ses kaydetme gibi kayıt araçlarını kullanamaz.
5.2.1.2. Çalışanlar, kurumun iş gereği kendilerine tahsis etmiş olduğu tüm kurumsal cihazı bozulmaması ve kaybolmaması amacıyla azami dikkat ve özen ile kullanmak zorundadır.
5.2.1.3. Kurum tarafından çalışanlarına günlük işlerinde kullanmak üzere tahsis edilmiş olan taşınabilir cihazların (dizüstü, tablet vb.) fiziksel güvenliğinden kullanıcıları sorumludur. Bu cihazların çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Birimine haber verilir.
5.2.1.4. Kurumda kullanılan hassas ve önemli iş bilgilerini içeren her türlü bilgi varlıkları (basılı belgeler, USB Bellekler, CD/DVD vb.) kullanılmadığında, özellikle de mesai saatlerinin dışında, çekmecelerde ve/veya diğer güvenli yerlerde kilitli olarak tutulur.
5.2.1.5. Gelen ve giden gizli bilgiler, gelişigüzel ya da güvenli olmayan bir şekilde, faks/yazıcı/fotokopi/tarayıcı cihazlar üzerinde bırakılamaz.
5.2.1.6. Bilgi işlem araç gereçlerinin yakınlarında ve sistem odalarında; yiyecek, içecek veya sigara kullanılamaz.
5.2.1.7. Bilgisayarlar, iletişim cihazları ve veri depolama cihazları, kullanım veya depolama amacıyla yerleştirilirken; cihaz üreticisinin belirttiği teknik standartlara uygun ortamlar sağlanır. Gerekirse, çevresel kontrollerle bu ortam gözlenir ve uygun aksiyonlar alınır.
5.2.1.8. Cihaz yerinde bakıma tabi tutulamayacaksa; bakıma gönderilmeden önce, içindeki bilgiler kontrol edilir, kritik bilgiler güvenceye alınır.
5.2.1.9. Hassas bilgileri içeren kayıt araçları, güvenli bir şekilde depolanır ve kullanımdan kaldırılacağı zaman imha edilir.
5.2.1.10. Medyalarda ve donanımlarda bulunan, kullanımına ihtiyaç kalmamış (yasal yükümlülükler veya iş gerekleri için saklanması gereken bilgiler dışında) kurumsal veriler ve yazılımlar silinir, gerekli görülüyorsa medya yok edilir.
5.2.1.11. Depolama ortamı içeren cihazların tüm öğeleri, örneğin takılmış sabit diskler, elden çıkartılmadan önce, tüm hassas verilerin ve lisanslı yazılımların kaldırılmış olduğunun veya üstüne yazılmış olduğunun temin edilmesi için, kontrol edilir.
5.2.1.11.1. Eğer taşınabilir depolama ortamı içerisinde saklanan bilgi artık ihtiyaç duyulmayacak bir veri ise, geri dönülemeyecek şekilde imha edilir.

5.2.1.11.2. Ortamın ya da ortam içerisindeki verinin kaldırılmasında onay gereksinimi var ise, imha öncesinde ve sonrasında denetim kaydı tutulur.
5.2.1.11.3. Taşınabilir ortamda veriler sadece iş gereksinimi mevcut ise tutulur.
5.2.1.12. Saklama ortamları, kullanımına ihtiyaç olmadığında güvenli ve tehlikesiz şekilde **Bilgi Saklama Ortamı Yok Etme Prosedürün**e uygun şekilde imha edilir.
5.2.1.13. Kuruma ait cihaz, yazılım ve veriler hiçbir şekilde ve sebeple izinsiz ve yetkisiz olarak kurum dışına çıkarılamaz.
5.2.1.14.Çalışanlar, yönetilen bilgi sistemleri üzerindeki hassas bilgiler ya da cihazlarla kurum dışında çalışmak zorunda kaldıkları durumlarda (yöneticileri tarafından yetkilendirildiklerinde), bütün sorumluluğun kendilerine ait olduğu konusunda bilgilendirilir.
5.2.1.15. Kurum cihazını kurum dışında kullanmasına izin verilen çalışan, aşağıdaki kontrollerin uygulanmasından sorumludur:
5.2.1.15.1. Cihazın fiziksel güvenliği sağlanır, var ise üreticinin koruma ve kullanım ile ilgili talimatları her zaman uygulanır;
5.2.1.15.2. Kurumsal varlık ve verilerin güvenliği sağlanır. Kurum alanı dışına çıkarılmış kurumsal varlık ve veriler özellikle de umumi alanlarda hiçbir zaman gözetimsiz ve korumasız bırakılmaz.
5.2.1.15.3. Bu prosedürün 5.3 maddesinde yer alan Taşınabilir Ortam Yönetimi kurallarına riayet edilir.
5.2.1.16.İçlerinde çok gizli/gizli/hizmete özel/kuruma özel gibi bilgiler bulunduran laptop, notebook, tablet, akıllı telefon vb. sahipleri, bu cihazları hiçbir zaman, diğer çalışanların ve/veya üçüncü şahısların kolayca erişebileceği yerlerde, korumasız bırakmaz.
5.2.1.17.Çalışanlara pozisyonları gereği tahsis edilmiş olan ve oturdukları yerleşim planına uygun kurulmuş olan tüm bilgisayar ve donanımlar Bilgi Sistemleri gözetimi ve bilgisi dışında hiçbir şekilde ve sebeple başka bir yere taşınmaz veya başka bir donanımla yeri değiştirilmez.
5.2.1.18. Kurumda kullanılan bilgisayarlar ve bunlara bağlı donanımlarının yer değişimi sadece Sağlık Bilgi Sistemleri Biriminin yetkisindedir.

5.3. Taşınabilir Ortam Yönetimi

5.3.1. Kaybolma, kolayca çoğaltma vb. nedenlerden dolayı özellikle elektronik medya (CD/DVD, USB girişli hafif taşınabilir bellekler, taşınabilir diskler, hafıza kartları, teyp kartuşları vb.) ve basılı evraklar (yazılar, dosya klasörleri, etüdler, çizimler, krokiler, proje evrakları vb.) olmak üzere taşınabilir ortamlarda saklanan her türlü bilginin korunması ve yetkisiz kişilerin eline geçmemesi için özel önlemler alınmalıdır.
5.3.2. Taşınabilir cihazlardaki bilgileri üçüncü taraflarla paylaşımında da gerektiği kadar bilgi verme prensibi göz önünde bulundurulmalıdır.
5.3.3. Personelin kullanımı için tahsis edilmiş olan taşınabilir ortamlar sadeci yetkilendirilmiş personel tarafından ve veriliş amaçları doğrultusunda kullanılmalıdır.
5.3.4. Elektronik medya kullanımı ile ilgili olarak aşağıdaki hususlar göz önünde bulundurulmalıdır.
5.3.4.1. Kuruma ait veriler, kişilere ait medyalar üzerinde saklanamaz. Verilerin bir taşınabilir ortama aktarılması ihtiyacı kaçınılmaz ise bu maksatla kuruma ait medyalar kullanılır.

5.3.4.2. Kuruma ait medyalar varlık envanteri içinde listelenir ve kimler tarafından kullanıldığı kayıt altına alınır. Görev devir teslimlerinde veya işten ayrılışlarda, kişilere teslim edilmiş olan medyaların iade edilmesi istenir veya ne şekilde sarf edildiği bilgisi sorgulanır.
5.3.4.3. ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL veriler, taşınabilir ortamda saklanamaz. Özellikle bu tür ortamlarda saklama zorunluluğu var ise şifreli olarak saklanır.
5.3.4.4. Bir bilgi sadece taşınabilir medya ortamında saklanıyorsa, bozulma/kaybolma gibi ihtimallere karşı bir başka medya ortamında da yedeklenmelidir. Veriler çok kıymetli ise yedeklenen medya ortamı, doğal afet vb. tehditlere karşı önlem olmak üzere fiziksel olarak farklı bir yerde muhafaza edilir.
5.3.4.5. 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.
5.3.4.6. Gizlilik derecesi taşıyan kurumsal verilerin saklandığı medya ortamları, kişisel (şahsın kendisine ait) bilgisayarlarda kullanılamaz. Bu tip veriler kişisel bilgisayarlarda işlenemez.
5.3.4.7. Tüm ortamlar üretici talimatında belirtildiği şekilde toz, nem vb. çevresel şartlardan etkilenmeyecek şekilde güvenli bir ortamda saklanır.
5.3.5. 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 saklanmalıdır.
5.3.6. Taşınabilir ortamların bir yerden başka yere taşınması esnasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı gerekli önlemler alınmalıdır. Bu çerçevede;
5.3.7. Güvenilir kargo/taşıma şirketleri ya da kuryeler kullanılır.

5.4. Antivirüs Yönetimi
5.4.1. İl Sağlık Müdürlüğümüz ve bağlı sağlık tesisleri ağına bağlı olarak çalışan bilgisayarlara lisanslı antivirüs yazılımının yüklenmesi zorunludur. Eğer kullaıncının bilgisayarında antivirüs yazılımı yok ise bunu Sağlık Bilgi Sistemleri birimine bildirmekle yükümlüdür.
5.4.2. Tüm bilgisayarlar lisanslı antivirüs yazılımı ile korunur. Antivirüs yazılımının virüs veritabanı güncel tutulur. Kullanıcı, antivirüs yazılımının güncelleme yapmadığını fark ederse derhal Sağlık Bilgi Sistemleri birimine bildirir.
5.4.3. Kullanıcı, bilgisayarındaki antivirüs yazılımını kapatmamalı yada devre dışı bırakmamalıdır.
5.4.4. Kullanıcı, bilgisayarına taktığı CD/DVD, USB, Taşınabilir Disk vb. ortamları mutlaka güncel antivirüs yazılımıyla taratmalı ve tarama tamamladıktan sonra kullanmalıdır.
5.4.5. Kullanıcıların, bilgi sistemlerine zarar verebilecek herhangi bir bilgisayar kodunun kasıtlı olarak yazmaları, çoğaltmaları, kopyalamaları, üretmeleri ve çalıştırmaları yada tanıtmaları yasaktır.
5.4.6. Güncelleme sırasında kapalı olan bilgisayarlar sunucu üzerinde listelenir ve açıldığı anda güncelleme gönderilip doğrulanır
5.4.7. Sunucu üzerinden periyodik güncellemeler, virüs taraması, zayıf noktalar (farklı programların açıkları) antivirüs yazılımının sürümü, durum bilgisi ve birçok yararlı bilgi sunucu üzerinden raporlanır.
5.4.8. Antivirüs sunucusunu yöneten personel ağda yönetilen tüm bilgisayarların antivirüs yazılımının ne durumda olduğunu görür ve ona göre müdahalelerde bulunur.

5.4.9. Antivirüs yazılımları bazı otomasyonların (hbys, pacs, tıbbi cihaz yazılımları vs) yoğun ağ trafiğini saldırı olarak görüp engelleyebilir. Bu durumda antivirüs yazılımına sunucu üzerinden ilgili yazılımın güvenli olduğunu gösteren "güvenilir uygulama" tanımlaması yapılır.

5.4.10. Antivirüs yazılımları her zaman güncel ve sunucuyla haberleşebilir durumda olmalıdır.

5.4.11. Yüklü olan antivirüs programının kullanıcı tarafından devre dışı bırakılması veya sistemden kaldırılmasını engellemek amacıyla parola koruması uygulanır.

6. YAPTIRIM

Bu prosedürün ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla BGYS Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.