T.C. AİLE VE SOSYAL HİZMETLER BAKANLIĞI

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Onay Tarihi

…/…/….

Hazırlayan	Kontrol Eden	Onaylayan
Çiğdem KÖSEOĞLU		

İçindekiler

AMAÇ

Kabul Edilebilir Kullanım Politikasının amaçları:

- Personelin bilgi ve bilgi teknolojileri kaynaklarını kullanırken ve bu kaynaklara ilişkin sahiplik ve kontrol sorumluluğu bulunduğunda bu kaynaklara yönelik tehditlere karşı yerine getirmesi gereken temel kontrol sorumluluklarını tanımlamak
- Ziyaretçilerin kurum kaynaklarına fiziksel veya mantıksal erişimi sırasında ziyaretçiden sorumlu personelin uygulaması gereken temel kontrol sorumluluklarını tanımlamak
- Temel sorumlulukların bilerek veya bilmeyerek ihlali durumunda izlenecek disiplin sürecini ifade etmektir.

Kabul Edilebilir Kullanım Politikasının ve Bilgi Güvenliği Yönetim Sistemi'nin nihai amacı bilgi güvenliğine ilişkin tehdit ve zafiyetlerden kaynaklanabilecek ve ASHB tüm paydaşlarını (kamu kurumları, personeli ve vatandaşları) olumsuz etkileyebilecek olayların engellenmesi veya minimize edilmesidir.

1 KAPSAM VE İLGİLİ BÖLÜMLER

Politikanın kapsamı tüm organizasyonu içermekte olup tüm personelin kabul edilebilir kullanım politikasına uyması zaruridir. Ayrıca ziyaretçiler de ilgili personel ile birlikte bu politika kapsamındadır.

Politikanın tebliği, periyodik eğitim programı dâhilinde iletimi, uyumun kontrolü ve gerekli disiplin faaliyetlerini yerine getirmekten aşağıdaki bölüm ve görevliler sorumludur:

- Personel Genel Müdürlüğü (Disiplin ve özlük işleri ile ilgili)
- Bilgi Güvenliği Yönetim Sistemi Yöneticisi (politikanın periyodik eğitim programı içinde iletişimi, uyumun takibi ve disiplin sürecinin başlatılması açılarından)
- Tüm Birim Yöneticileri (sorumlu oldukları personelin politikaya uyum açısından sürekli gözetimi ve yönlendirilmesi açılarından)
- Tüm personel (politika kurallarına uyum açısından)

2 TANIMLAR

- ASHB: Aile ve Sosyal Hizmetler Bakanlığı
- TOKEN: Tek kullanımlık şifre üreten cihaz
- P2P (Eşler Arası Ağ – Peer to Peer Network): İki veya daha fazla bilgisayarın merkezi olmayan biçimde doğrudan birbirine bağlandığı ağ mimarisine verilen addır. En çok görülen P2P ağları İnternet üzerinden dosya paylaşımı amacıyla oluşturulan ağlardır.

- XSS (Cross Site Scripting): İstemci bilgisayarlarında İnternet sitelerini görüntülemek amacıyla kullanılan İnternet tarayıcıları dinamik içerik sunabilmek ve istemci platformunda bazı işlemleri / kontrolleri yapabilmek için kod (script) çalıştırabilme özelliğine sahiptir. Bu özellik iyi niyetle kullanılabileceği gibi ilgili internet sitesinde konuyla ilgili zayıflık var ise kötü niyetle de kullanılabilir.
- BIOS (Basic Input Output System): BIOS bilgisayar ilk açıldığında çalışan ve donanım parçaları arasındaki girdi / çıktı kontrolünü yapan yazılımdır. Bu sistem üzerinde bir "power on" (açılış) şifresi tanımlama imkanı vardır. Ancak bu kontrolün kararlı saldırganlar tarafından aşılabileceği unutulmamalıdır.
- Betik (Script) ve Makrolar: Son kullanıcılar veya bilgi teknolojileri profesyonelleri rutin işlerini otomatikleştirmek amacıyla bir takım işletim sistemi veya uygulama komutlarını betik veya makro adı verilen dosyalarda sıralayarak toplayabilir. Bu şekilde oluşturulmuş bir dosya "interpreter" adı verilen uygulamalara parametre olarak verilerek veya (belli bir uzantı ile adlandırıldıktan sonra) doğrudan işletim sistemi komut satırından çağrılarak tek adımda ardışık komutlar çalıştırılabilir. Bu tür dosyalarda güvenlik açısından kullanıcı adı ve parola bilgisinin kayıtlı olmaması gereklidir.
- Phishing (Oltalama): Phishing (Oltalama) saldırısında amaç (kimlik bilgileri, kart numarası gibi) kişisel bilgilerin ele geçirilebilmesi olup, temelde bir sosyal mühendislik yöntemi olan sahte e-posta ve Web sayfalarının kullanılmasıyla gerçekleştirilir. Phishing'de dolandırıcılar, tüketicilere tanınmış bir firmadan geliyormuş izlenimi verilmiş bilgi güncelleme talebi vb. içeren e-postalar göndermektedir. Bu e-postalarda genellikle cevap için e-postanın içindeki linkin (Web sayfası için kısa yol) tıklanarak gerekli siteye geçilebileceği belirtilmektedir. Ancak, verilen talimat uygulandığında gidilen site dolandırıcılar tarafında hazırlanmış ve gerçeğini taklit eden sahte bir Web sayfası olmaktadır. Bu sahte sitede elde edilen bilgiler mahiyetine göre daha sonra çeşitli dolandırıcılık faaliyetlerinde kullanılabilmektedir. Phishing yönteminde bankalar, mağazalar veya e-ticaret kurumlarının ve İnternet servis sağlayıcıların isimlerinin (kimliklerinin) kullanıldığı görülmektedir. Pharming adı verilen ve aynı amacı taşıyan bir diğer saldırı türü de DNS (İsim Sunucusu) sunucularının veya isim sorgularının yanıtlarının manipüle edilmesiyle kullanıcıların saldırgan tarafından düzenlenen bir siteye (kullanıcının bilgisi olmadan) yönlendirilerek kandırılması ve kişisel bilgilerinin çalınması şeklinde gerçekleştirilir.
- Nitelikli Elektronik Sertifika (NES): Asimetrik kriptolama yöntemi ile edinilen non-repudiation (mesaj göndericisinin inkar edilemezliği) ve gönderilen mesajın

bütünlüğünün korunduğu güvencesinin sağlanması için göndericinin public anahtarının doğruluğundan emin olunmalıdır. Bu güven mekanizmasının sağlayıcısına sertifika otoritesi adı verilir. NES Kanun çerçevesinde yetki almış Elektronik Sertifika Hizmet Sağlayıcılarından edinilebilir.

- Sosyal Mühendislik (Social Engineering): Bilgi güvenliği terminolojisine sosyal mühendislik adıyla giren saldırı veya gerçek saldırı öncesi aktiviteler insani duyguları (korku, aciliyet hissi, minnet, itaat, güven hissi, yardımcı olma güdüsü, vb. gibi) kullanarak bilgiye erişim yetkisi olan kişilerin yönlendirilmesi ve kullanılmasını içerir. Saldırgan farklı kimliklere bürünerek kurguladığı senaryo adımları ile kurbanını beklenen tepkileri vermeye yönlendirir. En temel sosyal mühendislik araçları telefon ve e-postadır.
- Kriptoloji: Bilgi alışverişini emniyetli olarak yapmasını sağlayan veya saklanan bilginin emniyetini korumak için uygulanan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür. Kriptolamanın içinde genel olarak algoritma(lar) ve anahtar(lar) bulunur. Kriptolama yöntemleri şu servislerden bir veya birden fazlasını sağlamak amacıyla kullanılır; Gizlilik, Bütünlük, Kimlik Doğrulama, İnkâr Edilemezlik.
- Güvenli Silme: Normal dosya silme işlemi genellikle dosyanın dizin üzerinde tanımlı girdisinin silinmesidir, ve dosyanın disk üzerindeki yeri temizlenmez. Disk üzerindeki silinmiş dosyalar nitelikli programlar ile başlangıç ve bitiş bölümleri incelenerek tespit edilebilir ve tekrar okunabilir. Bu nedenle fiziksel güvenlik riski olan yerlerde bulunacak veri saklama cihazları üzerindeki dosyalar güvenli biçimde silinmeli, yani disk üzerindeki dosya bilgileri de ezilmelidir.
- Çipli / Akıllı Kart: Çipli kartlar genellikle kredi kartı büyüklüğünde veya daha küçük bir plastik karta gömülü bir entegre devre ve elektronik hafıza içerir. İçinde mikro-işlemci içeren çipli kartlara akıllı (smart) kart adı verilir. Çeşitli kullanım alanları olan çipli kartlar güvenlik özelliklerini de barındıran kripto-işlemci ve güvenli dosya sistemi de içerebilir.

3 POLİTİKA

3.1 Genel İlke ve Sorumluluklar

3.1.1 Hesap Verebilirlik

Kullanıcıya atanmış olan parola, çipli/akıllı kart, sertifika, tek kullanımlık parola (OTP) TOKEN cihazı, PIN kodu, fiziksel geçiş kontrol kartı v.b. erişim araçları hiçbir şart altında teknik personel dahil kimseyle paylaşılmamalıdır. BTGM ve yardım masası personeli, hiçbir zaman

kullanıcılardan parola, e-imza cihazı paylaşımı vs. bilgileri yazılı iletmelerini, fiziksel erişim araçlarının verilmesini (görevden ayrılma veya erişim aracının değişim durumları hariç) istemeyecektir. Yardım Masası personeli destek ihtiyacı olduğu durumlarda sadece kullanıcı adını sorabilir. Eğer kullanıcılar erişim ile ilgili konularda destek için telefon ile iletişim kuruyorsa, özelikle karşı tarafın (teknik personel olduğunu belirten kişinin) araması durumunda, telefonun diğer ucundaki kişinin kimlik doğrulamasını yapmalıdır. Şüpheli telefon aramaları veya mesajlar, edinilmesi mümkün olan detay bilgiyle birlikte Bilgi Güvenliği Ekibine raporlanmalıdır.

3.1.2 Kullanıcı Kimliği

Kullanıcıların, Bakanlık bilişim sistemleri üzerinde kendilerine ait olmayan kullanıcı kimliklerini kullanmaları veya kullanıcı kimliklerini çeşitli yöntemlerle gizleyerek, anonim kullanıcı olarak davranmaları yasaktır. Bu çerçevede e-posta iletilerindeki gönderen kısmı da bir kimlik bilgisi olup bu alanın yanıltıcı biçimde değiştirilmesi yasaktır. Kullanıcılar jenerik / ortak hesap kullanımından kaçınmalı, kişiye özel kullanıcı hesabı kullanımında teknik kısıtlar olması durumunda Bilgi Güvenliği Ekibine çözüm talebiyle başvurmalıdır. Ortak kullanıcı hesabı kullanımı sadece teknik imkansızlık veya çözümün maliyet etkin olmaması durumunda, izleme kontrollerinin uygulanması şartıyla Bilgi Güvenliği Ekibinin ve İlgili Daire Başkanının onayı ile mümkündür.

3.1.3 Parola (Password) Kriterleri

Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) ve kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 90 (doksan) günde bir değiştirilmelidir.

Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.

Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir ve otomatik parola anımsama seçenekleri işaretlenmemelidir.

Kullanıcı, parolasını başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazması durumunda güvenliğini sağlamalıdır.

Bakanlık uygulamalarında bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır:

- En az 8 haneli olmalıdır.
- İçerisinde en az 1 tane küçük ve 1 tane büyük harf bulunmalıdır. (a, b, C...)
- İçerisinde en az 1 tane rakam bulunmalıdır. (1, 2, 3...)
- Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, abababab...)

- İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^,+,$,#,&,/,{,*,-,],=,...)

Uyulması tavsiye edilenler;

- Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)
- Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)

Bütün parolalar Bakanlığa ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.

Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki “parola hatırlama” seçeneği kullanılmamalıdır.

Parola kırma ve tahmin etme operasyonları belli aralıklar ile bilgi güvenliği yetkililerince yapılabilir.

Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.

3.1.4 Bilgi Paylaşımı

Kurum içi bilgi paylaşımı sadece görev gereği ilgili veriye ulaşması gereken kullanıcılar arasında olmalıdır. Kolluk kuvvetleri ve kamu kurumları ile bilgi paylaşımı bu irtibat görevini yerine getirmek üzere atanmış personel tarafından gerçekleştirilmelidir. İlgili bilgi istekleri sadece görevli personele yönlendirilmelidir.

3.1.5 Veri Sahipliği ve Sınıflandırılması

Kullanıcılar kendileriyle ilgili iş verilerinin sahibi olup bu varlıkların korunmasından nihai olarak sorumludur. Veri sahipleri kendileriyle ilgili iş verilerinin sınıflandırılmasından ve gerektiğinde yeniden sınıflandırılmasından sorumludur. Verinin çevrim içi (online, sunucular üzerinde) saklanabileceği gibi, çevrim dışı (yedek alınan kartuş, CD, USB bellek gibi ortamlarda) ve basılı doküman halinde de saklanabileceği unutulmamalıdır. Veri sınıflandırma hakkında daha detaylı bilgi için Bilgi Sınıflandırma, Etiketlendirme ve İşleme Kılavuzu’na (KLVZ-002) bakınız.

3.1.6 Kurumsal Verinin Saklanması

Kullanıcılar sahibi oldukları iş verilerinin yasal yükümlülükler veya iş gereklerinden doğan saklanma süre ve şart ihtiyaçlarını Bilgi Güvenliği Ekibine bildirmekle yükümlüdür. Basılı dokümanlar üzerinde bulunan veriler de bu maddenin kapsamı içindedir. Genel prensip olarak üzerinde çalışılan dosyalar **Hizmete Özel** ve daha üstü dosyalar hariç, kişisel bilgisayarlarda saklanabilir, ancak kritik dosyalar üzerinde çalışılmadığı durumlarda kişisel bilgisayarlardan silinmeli ve sunucularda saklanmalıdır. Kullanıcılar veri saklama konusunda Sistem Yönetimi Ekibinin merkezi veri saklama yöntemlerini kendi yöntemlerine tercih etmeli, sahibi oldukları kritik verilerin kurumsal yedekleme prosedürlerine dâhil olduğundan emin olmalıdır.

Kullanıcılar taşınabilir veri saklama araçlarını yedekleme amacıyla kullandıklarında **"Taşınabilir Veri Saklama Araçları"** bölümünde bahsedilen önlemleri uygulamalıdır. Benzer biçimde basılı doküman saklama konusunda kurumun merkezi arşivleme prosedür ve yöntemleri kişisel yöntemlere tercih edilmelidir.

3.1.7 Temiz Masa, Temiz Ekran Politikası

Kullanıcılar masaları başında olmadıklarında hassas bilgi içeren basılı dokümanları masa üstünde bırakarak ve bilgisayar ekranlarını açık bırakarak terk etmemelidir. Hassas bilgi içeren basılı dokümanlar kullanılmadıklarında masadan kaldırılmalı ve gerekiyorsa kilit altında tutulmalıdır. Kullanıcılar kurum dışında basılı doküman, bilgisayarlar ve veri saklama cihazlarının fiziksel güvenliği konusunda daha hassas davranmalı, asla kontrolsüz biçimde açıkta bırakmamalıdır. Kurum dışında bilgisayar ekranından veya basılı dokümanlardan hassas bilgilerin başkalarınca izlenme riskinin daha yüksek olduğu unutulmamalı, halka açık mekanlarda hassas bilgiler görüntülenmemelidir.

3.1.8 Telefon Görüşmeleri

Bakanlık çalışanları özellikle kurum dışında hassas bilgileri içeren telefon görüşmesi yapmamaya gayret etmelidir. Hassas bilgilerin iletişimini gerektiren bir görüşme yapılması gerekiyorsa kendilerine ait cep telefonlarını diğer şahıslara / kurumlara ait telefonlara, kapalı ve yalnız bulunulan mekânlar tercih edilmelidir.

3.2 Taşınabilir Cihaz ve Veri Saklama Araçları Kullanım Kuralları

3.2.1 Diz Üstü Bilgisayarlar ve Tabletler

Kullanıcılar, hassas kurum verilerini diz üstü bilgisayarlar ve tabletlerde saklamaktan kaçınmalıdır. Hassas kurum verisinin iş amacıyla diz üstü bilgisayarlarda saklanması gerekiyorsa kriptolanmış biçimde saklanmalıdır. Kullanıcılar kriptolama çözümü için Donanım Teknik Destek Ekibi'ne başvurabilir. Diz üstü ve tablet bilgisayarlar taşınabilir olmaları ve kurum dışında da bulunabilmeleri dolayısı ile çalınma tehdidine daha açıktır. Bu nedenle bu cihazların kullanıcıları özellikle halka açık mekânlarda ve bu mekânlarda park edilen araçlarının içinde cihazlarını terk etmemeli ve fiziksel güvenliğini sağlamalıdır. Taşınabilir cihazlar kurum iletişim ağına uzaktan erişim için kullanılıyorsa erişim için kullanılan kullanıcı adı ve parola bilgileri bilgisayar üzerinde herhangi bir dosya içinde kriptolanmamış biçimde saklanmamalıdır.

3.2.2 Kurum Dışına Gönderilen Bilgisayarlar ve Veri Saklama Araçları

Eğer kişisel bilgisayarlar (diz üstü bilgisayarlar dahil) veya bu bilgisayarlara ait depolama birimleri tamir veya hibe amacı ile kurum dışına gönderilecekse, bu bilgisayarların kullanıcıları bilgisayar üzerinde bulunan hassas verilerin silinmesi ve gerekiyorsa yedeklenmesinden nihai

olarak sorumludur. Normal yöntemler ile silinen dosyalar tekrar elde edilebildiğinden kullanıcılar güvenli silme konusunda Bilgi Güvenliği Ekibine başvurmalı ve teknik destek talep etmelidir. Kurum dışına gönderilen diğer bilgisayarlar (sunucular, ortak kullanılan bilgisayarlar, vd.) için veri temizleme sorumluluğu sunucunun sahibi olan birime aittir.

3.2.3 Taşınabilir Veri Saklama Araçları

Kullanıcılar Kurum içinde kendilerine ait taşınabilir veri saklama araçlarını kullanmamalıdır. Kurum tarafından sağlanan CD, USB veri saklama cihazı, v.b. gibi malzemeler kurum içinde kullanılmalı ve gerekmediği sürece ofis dışına çıkarılmamalıdır. Taşınabilir veri saklama araçlarında bulundurulacak kritik veriler kriptolanmalı, bu konuda teknik destek için Donanım Teknik Destek Ekibine başvurulmalıdır. Taşınabilir olmaları nedeniyle çalınma tehdidiyle karşı karşıya olan taşınabilir veri saklama araçlarının, özellikle kritik veri barındırmaları durumunda, fiziksel güvenliği kullanıcılar tarafından sağlanmalıdır. Verinin saklanma ihtiyacı sona erdiğinde veriler silinmeli (güvenli silme konusunda Bilgi Güvenliği Ekibine başvurmalı ve teknik destek talep etmelidir), CD gibi tek kullanımlık araçların kullanımı durumunda araç imha edilmelidir (örneğin CDler için parçalayıcı (shredder) kullanılmalı ya da elle parçalara ayrılmalıdır).

3.3 İnternet ve Mesajlaşma Kaynaklarının Kullanımına İlişkin Kurallar

3.3.1 Kurum Ağına Uzaktan Erişim

Kurum ağına uzaktan erişmesi gereken kullanıcılar erişim için, zorunlu bir neden yoksa güvenlik yazılımlarının olduğu Kurumun verdiği diz üstü bilgisayarlar kullanmalıdır. Kullanıcılar uzaktan erişim araçlarını (parola, çipli kart, sertifika, tek kullanımlık parola (OTP) cihazı, PIN kodu v.b. gibi) koruma konusunda diğer erişim araçlarının korunmasına nazaran daha fazla hassasiyet göstermelidir. Uzaktan erişimde kimlik doğrulama için bir cihaz (OTP cihazı, akıllı kart, vd.) kullanılıyorsa kullanılan cihazların üzerine Kuruma veya kullanıcıyla ilgili bir erişim bilgisi (telefon numarası, sunucu adı, IP adresi, kullanıcı kodu, v.b. gibi) yazılmamalı / yapıştırılmamalıdır. Eğer Kurum bilgisayarı dışında bir bilgisayardan uzaktan erişim yapılması gerekiyorsa BTGM'den onay alınmalıdır. Kullanıcılar Kurum bilgisayarı dışında bir bilgisayar kullanmak zorunda olduklarında Bilgi Güvenliği Ekibinin önereceği kontrolleri uygulamakla yükümlüdür (çalışılan bilgisayar üzerinde iz bırakmamak için sanallaştırma (virtualization) yazılımı kullanmak, kullanılan bilgisayarın kişisel koruma duvarının olması, anti-virüs imzalarının ve işletim sisteminin güncel olması gibi). Halka açık bilgisayarların (internet cafe'ler, otellerin iş merkezi imkânları, vd.) uzaktan erişim için kullanımı her koşulda yasaktır. Destek amaçlı ayrıcalıklı uzaktan erişimler kurumun uygun gördüğü yazılımlar vasıtası ile yapılır.

3.3.2 Kurumsal ve Kişisel Bilgilerin İnternet Üzerindeki Web Sitelerine Verilmesi

Kullanıcılar İnternet üzerindeki tartışma gruplarına, sohbet odalarına ve forumlara yazmaları durumunda kurumun ve şahısların mahremiyetini korumalı, şirket adres ve telefon bilgilerini, personel isimlerini, unvanlarını, e-posta adreslerini ve diğer kişisel bilgilerini iş gerekleri ve kanuni gereklilikler dışındaki durumlarda İnternet üzerindeki herhangi bir web sitesine aktarmamalıdır.

3.3.3 İnternet'ten Dosya İndirme

Kullanıcılar, Bilgi Güvenliği Ekibi'nin onay vermesi dışındaki durumlarda İnternet'ten yazılım indirmemelidir. Kullanıcılar iş gereksinimleri için İnternet'ten veri dosyaları indirebilir, ancak anti-virüs imzaları ve işletim sistemi yamalarının güncelliğinden emin olmalıdır.

3.3.4 İnternet Üzerinden P2P Ağ Oluşturma ve Dosya Paylaşımı

İnternet üzerinden P2P ağlara katılım ve dosya paylaşımı yasaktır. Eğer İnternet üzerinden P2P ağ oluşumu veya dosya paylaşımı iş amaçları için gerekli ise, Bilgi Teknolojileri Genel Müdürlüğünden onay alınmalı, iletişimde kriptografik kontroller tercih edilmelidir.

3.3.5 İzin Verilen Mesajlaşma Çözümleri

İş amaçlı kullanılabilecek tek mesajlaşma çözümü şirket e-postasıdır. Dosya alış verişi bu maddenin kapsamı içinde değildir. Kurum tarafından kontrol edilmeyen, üçüncü taraflarca sağlanan web arayüzlü e-posta kullanımı tamamen kişisel kullanımla sınırlıdır. Web arayüzlü e-posta kullanımında bu politikada ortaya konan diğer yükümlülük ve veri koruma kurallarına uyulmalıdır. Anında mesajlaşma (instant messaging) kullanımı Bakanlığın izin vermiş olduğu programlarla yapılabilir.

3.3.6 Mesajlaşma Mahremiyeti

Kurumun sistemleri kullanılarak yapılan hiç bir elektronik iletişimin mahrem olacağı garantisi verilemez. Kullanıcılar elektronik ortamdaki her türlü iletişimin (telefon iletişimi dâhil), kullanılan teknolojiye özgü saldırı yöntemleri ile hedeflenen alıcıdan farklı alıcılara yönlendirilebilme, iletişim içeriğinin izlenebilme ve saklanabilme risklerine tabi olduğunu bilmelidir. Bu nedenle kritik kurum bilgilerini içeren iletişimin hem iletişim hattında hem de ulaştığı alıcı noktasında gizlilik ve bütünlüğünün korunabilmesi için kriptografik yöntemlerle yapılması gereklidir. Kullanıcılar gizlilik ihtiyacı olan iletişimleri için risk analizi ve teknik çözüm konusunda Bilgi Güvenliği Ekibine başvurmakla yükümlüdürler. Teknik olanaksızlık veya karşı taraftan kaynaklanabilecek uyumsuzluk nedeniyle kriptolaması mümkün olmayan kritik iletişimin yapılması Bilgi Güvenliği Ekibinin onayı ile gerçekleşebilir. Riskin önemine bağlı olarak Bilgi Güvenliği Ekibi, Genel Müdürden risk kabulü alınmasını uygun görebilir (Ayrıca İzleme ve Kayıt Aktiviteleri, Mahremiyet bölümüne bakınız.)

3.3.7 E-Posta Kullanım Esasları

BTGM, kurum kullanıcılarının e-mail adreslerine gelen istenmeyen e-posta ve virüs eklentilerine karşı teknik önlemleri uygulamaktadır. Buna rağmen kullanıcılar gerek teknik korunma yöntemlerinin göreceli olarak yeni olması, hata yapabilmesi ve hatta yemleme (phishing) gibi bazı saldırılara karşı yetersiz olması, gerekse kişisel iletişimi için kurum e-posta hesapları dışındaki hesapları da kullanıyor olmaları ihtimaline karşı genel e-posta güvenlik kurallarına uymalıdır.

Kullanıcılar e-posta içinde gelen linklere tıklayarak veya bu linkleri kopyalayıp tarayıcı hedef alanına yapıştırarak (kullanıcı kodu ve parolası başta olmak üzere) hiçbir kişisel bilgilerini girmemeli, HTML formatında gelen e-postalardaki resimleri görüntülemek için indirmemeli, e-posta içindeki herhangi bir linke tıklamamalı, güvenilir kaynaklardan gelmeyen e-postalardaki eklentileri indirmemeli, gönderen kısmındaki bilginin yanıltıcı olabileceğini unutmamalıdır. E-posta içindeki herhangi bir linke tıklamak veya e-posta içindeki resimleri görüntülenmek üzere indirmek, istenmeyen e-postanın varolan bir kullanıcıya ulaştığı bilgisini saldırgana verir, ayrıca resim indirme veya linki ziyaret etme işlemi resim işleyici uygulamalardaki açıklardan dolayı bilgisayarınızın zarar görmesine veya “Cross Site Scripting – XSS” adı verilen istemci tarafında çalışan betiklerin kötü niyetle kullanılması ve oturum hırsızlığı (yani kullanıcının hesaplarına ve erişim haklarına sahip olma) saldırılarına imkân verebilir.

Kullanıcılar Bakanlık tarafından kendilerine verilen e-postalarını iş dışı konularda (alışveriş siteleri vs.) kesinlikle kullanmamalıdır.

3.4 Ofis Ekipmanlarının Kullanımı ve Basılı Dokümanlara İlişkin Kurallar

3.4.1 Yazıcılar ve Fotokopi Makineleri

Kullanıcılar gizlilik gereksinimi yüksek bir dokümanı yazdırırken, bilginin yetkisi olmayan kişiler tarafından görülmesini veya ele geçirilmesini engellemek için yazdırma esnasında yazıcının yanında bulunmalıdır. Kullanıcılar gizlilik gereksinimi olsun veya olmasın makineye sıkışmış dahi olsa orijinal ve kopya doküman nüshalarını yazıcı ve fotokopi makinelerinde terk etmemelidir. Yazıcı ve fotokopi makinelerinin aşırı kişisel kullanımı yasaktır.

3.4.2 İhtiyaç Kalmayan Basılı Dokümanların İmha Edilmesi

İmha edilecek tüm hassas dokümanlar (gizli, özel, kişiye özel ve hizmete özel bilgi sınıfında bulunan dokümanlar), doküman parçalayıcı makine (shredder) ile parçalanmalıdır. Gizlilik gereksinimi olmayan diğer dokümanlar ofis içi veya dışında rast gele bölgelerde bırakılmamalı ve kağıt atık geri dönüşüm kutularına atılmalıdır.

3.4.3 Faks Makineleri

Kullanıcılar yüksek düzeyde gizlilik gereksinimi olan bilgilerin gönderiminde kriptografik yöntemleri faks gibi verinin açıkta gönderildiği ve hedef noktaya ulaştığında açık olarak görüntülenen teknolojilere tercih etmelidir. Bu tür gereksinimlerin doğması durumunda kullanıcılar Bilgi Güvenliği Ekibine çözüm üretilmesi için başvurmalıdır. Faks kullanımına imkân tanıyan veya faks kullanımını zorunlu kılan durumlarda şu kontroller uygulanmalıdır; Kullanıcılar faks mesajı gönderirken doğru numaranın çevrilmesine dikkat etmelidir, hassas dokümanlar alıcı tarafından alıcı cihazın başında beklenmesi durumunda gönderilmeli, otel veya postane gibi yerlerden mümkünse gönderilmemeli, eğer gönderilmesi gerekiyorsa hizmet personeline teslim edilmemelidir. Hassas bilginin iletildiği bilgisi en kısa zamanda alıcıya teyit edilmelidir. İmza içeren veya talimat nitelikli dokümanların kabulü durumunda dokümanların mutlaka orijinal nüshaları alınmalıdır (orijinal nüshaların takibi gereksinimi elektronik olarak taranmış dokümanlar için de geçerlidir).

3.5 Güvenlik Olayları ve Gözlenen Zayıflıkların Bildirilme Sorumluluğu

Kullanıcılar kendi sorumluluk alanlarında gerçekleşebilecek veya diğer alanlarda gözlemleyebilecekleri güvenlik olay ve zayıflıklarına karşı duyarlı olmalıdır. Fark edilen her zayıflık, riskin gerçekleşmesi zayıf bir olasılık olsa bile en kısa zamanda Bilgi Güvenliği Ekibine telefonla veya some@aile.gov.tr adresine e-pota atılarak bilgilendirilmelidir. (Güvenlik olay ve zayıflıklarının raporlanması hakkında daha detaylı bilgi için **Bilgi Güvenliği Olayları Tespit ve Müdahale Prosedürü'ne** bakınız). Güvenlik olay ve zayıflıklarına örnek olarak; kullanıcı bilgisayarlarında yakalanan virüs, kullanıcı parolasının öğrenilmiş olmasından şüphelenilmesi veya erişim araçlarının (çipli kart, sertifika, tek kullanımlık parola (OTP) cihazı, fiziksel geçiş kontrol kartı v.b. gibi) kaybedilmesi / çalınması, diz üstü veya avuç içi bilgisayar kaybedilmesi / çalınması, açıkta bırakılan hassas doküman ve veri saklama araçları, hassas bilgilere erişim kontrollerindeki zafiyet, davetsiz ve şüpheli misafir, kullanıcının sisteme girişinin reddedilmesi (bir parola saldırısı sonrası hesabı kilitlenmiş olabilir) ve hizmet kesintisi gibi beklenmeyen durumlar verilebilir. Diz üstü ve avuç içi bilgisayarların, hassas dokümanların ve veri saklama cihazlarının kaybı veya çalınması durumunda en kısa zamanda Bilgi Güvenliği Ekibi bilgilendirilmelidir.

3.6 İzleme ve Kayıt Aktiviteleri, İletişim Mahremiyeti

3.6.1 Kurum Sistemlerinde Saklanan veya İletilen Verinin Mahremiyeti

Kurum, düzenlemelerle korunan vatandaşa ait kişisel veriler hariç, kendi sistemleri üzerinde saklanan ve iletilen tüm bilgileri inceleme hakkını saklı tutar. Vatandaşlara ait kişisel veriler sadece görevi gereği ulaşması gereken kişiler tarafından incelenebilir.

3.6.2 Kayıtlar

ASHB, iç ve dış saldırılara karşı geliştirdiği iz kaydı (log kaydı) tutma stratejisini uygulamaktadır. İz kaydı tutma stratejisi özellikle kullanıcı faaliyetlerini izleme amacına yönelik olmamakla birlikte, kullanıcıların uygulamalar ve ASHB ağı üzerinde gerçekleştirdiği faaliyetlerin bir kısmı kayıt altına alınmaktadır. Kullanıcılar, ASHB sistemleri üzerinde veya bu sistemleri kullanarak yasal mevzuata veya kurum içi kurallara aykırı davranışlarından şüphe edilmesi halinde hukuki süreçlerde yetkili kişilerce talep olması durumunda sistemler üzerindeki faaliyetlerinin izlenebileceğinin bilincinde olmalıdır.

3.7 Diğer Konular

3.7.1 Kişisel Kullanım Politikası

ASHB bilgisayar ve iletişim sistemlerinin kişisel kullanımı gerekli olduğu durumlarla sınırlandırılmalıdır. Kişisel kullanım aktiviteleri, e-posta zincirlerinin yaratılması ve yayılmasını, uygunsuz veri ve resim alışverişini, mizah amaçlı iletilerin gönderilmesini, kullanıcının Kurum görevi harici bir iş için faaliyet göstermesini, iş arama, kumar oynama ve politik aktivitelerini içermemelidir. İş ile ilgisi olmayan kişisel dosyaların ASHB bilgi sistemlerinde saklanmasından sakınılmalıdır. BTGM personeli kişisel bilgisayarlar veya sunucularda saklanan iş dışı kişisel dosyaların silinmesini isteme veya silme hakkına sahiptir. İş ile ilgili olmayan çalıştırılabilir uygulama dosyaları hiçbir koşulda ASHB bilgi sistemleri üzerinde saklanamaz. (Daha fazla bilgi için Yazılım Kurulumu bölümüne bakınız.)

3.7.2 ASHB Kaynaklarının Yasalara ve Etik Prensiplerine Uygun Kullanımı

ASHB personeli, İnternet kullanımı ve sesli iletişim aktiviteleri dâhil olmak üzere, tüm bilgi sistemleri ve iletişim imkânlarının kullanım ve sağlanmasında, ilgili Türkiye Cumhuriyeti yasalarına, uluslararası hukuka ve genel etik kurallarına uymakla yükümlüdür. Kullanıcılar, bilgisayarlarında bulunabilecek standart iş ve ofis uygulamaları dışındaki yazılımlar için telif hakkı koruma düzenlemelerine uymakla şahsen sorumludurlar.

Diğer kullanıcıların kimlik doğrulama ve erişim kontrol araçlarını (parola, çipli kart, e-imza, sertifika, tek kullanımlık parola (OTP) cihazı, TOKEN, PIN kodu, fiziksel geçiş kontrol kartı v.b. gibi) ele geçirmeye çalışmak, ASHB kaynaklarını sabote etmek ya da üçüncü taraflara Kurum kaynaklarını kullanarak zarar vermek etik kurallarına ve yasalara aykırı olup kabul edilemez. Kullanıcılar teknik olarak mümkün olsa bile iş sorumlulukları gereği erişim ihtiyacı olmayan kaynaklara erişmeye çalışmamalıdır. Kullanıcılar erişim kontrollerinde bir zayıflık fark ederse Bilgi Güvenliği Ekibini bilgilendirmekle yükümlüdür. (Daha fazla bilgi için Güvenlik Olay ve Zayıflıklarını Raporlama bölümüne bakınız.)

Tüm iletişimde genel prensip olarak kurumsal ve genel etik ve nezaket kurallarına uyulmalı, kurum çalışanlarını, müşterileri ve diğer tarafları karalayıcı, hakaret içeren ifadeler kullanılmamalıdır. ASHB bilgi kaynaklarının personel tarafından yasal olmayan şekilde kullanımı halinde yasa uygulayıcılar ile işbirliği yapacaktır. (Ayrıca İzleme ve Kayıt Aktiviteleri, Mahremiyet bölümüne bakınız.)

3.7.3 Yazılım Kurulumu

İş ile ilgili olmayan yazılımların (kurulum dosyaları dâhil) ASHB bilgisayar sistemlerinde saklanması veya kurulması her koşulda yasaktır. Kullanıcılar, teknik olarak mümkün olsa bile, telif hakları kanunlarının çiğnenmesine ve teknik sorunlara neden olabileceğinden Bilgi Güvenliği Ekibinin onayı olmadan bilgisayarlarına yazılım yüklememelidir. İş amaçlı yazılım yükleme ihtiyacı olması durumunda Bilgi Güvenliği Ekibinin görüşü ve onayı alınmalıdır. Güvenlik analiz yazılımları ve sistem yönetim yazılımları gibi yazılımlar sadece Sistem Yönetimi Ekibi ile Bilgi Güvenliği Ekibi personelinin bilgisayarlarına kurulabilir.

3.7.4 Konfigürasyon ve Güvenlik Ayarları

Kullanıcılar teknik olarak mümkün olsa bile bilgisayarlarındaki güvenlik ayarlarının düzeyini düşürmemelidir. Güvenlik ayarlarına örnek olarak; MS Internet Explorer ve MS Outlook'u etkileyen güvenlik alanları ayarları (Internet Explorer security zone settings), virüs koruma program ayarları, işletim sistemi güncelleme ayarları, kişisel koruma duvarı (firewall) ayarları, BIOS ayarları ve diğer donanımsal ve yazılım güvenlik ayarları sayılabilir. Kullanıcılar teknik olarak mümkün olsa bile kişisel bilgisayarlarında yeni ağ servislerini (web sunucusu, veritabanı sunucusu gibi) çalıştırmamalı, bilgisayarları üzerinde yeni kullanıcı ve kullanıcı grubu tanımlamamalı, varolan kullanıcıların hakları ve kullanıcı gruplarını değiştirmemelidir. Eğer iş ihtiyaçları gereği konfigürasyon ve güvenlik ayarlarının değiştirilmesi gerekiyor ise Bilgi Güvenliği Ekibinin yorum ve onayına başvurulmalıdır. Konfigürasyon ve güvenlik ayar değişiklikleri sadece Sistem Yönetimi Ekibi veya Donanım Hizmetleri Ekibi Personeli tarafından ve gerekli olan süre için yapılabilir.

3.7.5 Kuruma Ait Olmayan Bilgisayarlar

ASHB'na ait olmayan bilgisayarlar sadece iş gereği ve Ağ Yönetim Ekibi Yöneticisinin onayı ile Kurum ağına bağlanabilirler. Eğer kullanıcı Kurum personeli değil ise ilgili kullanıcıdan sorumlu kurum personeli onay almakla yükümlüdür. Ağ Yönetimi Ekibi Yöneticisi, kurum ağına izinli bağlanacak Kuruma ait olmayan bilgisayarlarda teknik kontroller uygulama ve ayar değişiklikleri yapma / yaptırma hakkına sahiptir.

3.7.6 Kullanıcılar Tarafından Uygulama Geliştirilmesi

Kullanıcılar BTGM'nin onayı olmadan uygulama geliştiremezler. Excel çalışma sayfalarında kullanılan formüller, ofis dosyalarında otomatik çalışan betikler (veya makrolar) ve Ağ Yönetimi ve Sistem Yönetimi Birimleri personeli tarafından geliştirilen betikler (scriptler) bu maddede kastedilen uygulamalardan sayılmaz. Kullanıcılar herhangi bir bilgisayar dosyası içinde veya betik içinde kullanıcı kodu, parola, kripto anahtarları, ve diğer erişim kontrol bilgilerini saklamamalıdır. Pratik ihtiyaçlar dolayısı ile parolaların bilgisayar sabit diski veya taşınabilir bellekler üzerinde tutulması durumunda kriptolanmış dosyalarda tutulmaları gereklidir. Konuyla ilgili olarak Bilgi Güvenliği Ekibinden destek alınabilir.

3.7.7 Ofis Araç Gereçlerinin Fiziksel Güvenliği

Kullanıcılar yiyecek, içecek, sakız gibi gıda maddelerini bilgisayar ve ofis araçlarından uzak tutmalıdır. Bu tür maddeler dökülme, saçılma sonucunda cihazlara zarar verebilir. Kritik sunucular sistem odasında, kritik ofis ekipmanları güvenli alanlarda barındırılmalıdır. Kullanıcıların doğrudan sorumluluğunda veya ortak kullanımda olan bilgisayarlar ve diğer ofis araçlarını olumsuz etkileyebilecek çevresel etkenler (sıcaklık, nem, aşırı toz, v.b. gibi) Bilgi Güvenliği Yöneticisi'ne raporlanmalıdır. (Daha fazla bilgi için Güvenlik Olay ve Zayıflıklarını Raporlama bölümüne bakınız.)

3.7.8 Nitelikli Elektronik Sertifika (NES) Kullanımı

Elektronik imza mevzuatı çerçevesinde değerlendirilecek kurumsal yazışmalarda / iletişimde nitelikli elektronik sertifika kullanımı sadece resmi olarak atanmış ve kurum içi mevzuata göre imza yetkisine sahip kullanıcılara özeldir. Nitelikli elektronik sertifika kullanıcıları sertifika kullanımı ve sertifikanın güvenliğinin sağlanmasında gerekli özeni göstermekle yükümlüdürler.

3.7.9 Elektronik Yazışmalarının Saklanması

Kullanıcılar, ilgili yasal ve kurum içi mevzuatın ve iş ihtiyaçlarının gereğine uygun olarak kendileri ile ilgili iletişim kayıtlarının saklama şart ve süre gereksinimlerini belirlemekten, bunlara ek olarak kayıtların saklanması için gerekli kontrollerin uygulandığından emin olmaktan nihai olarak sorumludur. Kullanıcılar saklama gereksinimlerini Bilgi Güvenliği Ekibine iletmelidir. (Daha fazla bilgi için Kurumsal Verinin Saklanması bölümüne bakınız.)

3.7.10 Daha Fazla Bilgi İçin

Kullanıcılar gerektiğinde bu politikada belirtilen ve açıklamaya ihtiyaç duyan konular veya bu politikada bahsi geçmeyen bilgi güvenliği konuları hakkında daha fazla bilgi / destek almak için Bilgi Güvenliği Ekibine danışmalıdır.

3.8 Denetim Hakkı

Bilgi Güvenliği Yönetim Sistemi Yöneticisi ve Bilgi Güvenliği Yönetim Sistemi için atanmış iç denetçi personele zimmetli de olsa bilgi kaynaklarına yönelik olarak kabul edilebilir kullanım politikasına uyum denetimi yapabilir.

3.9 Politikaya Aykırı Davranış Durumunda İzlenecek Disiplin Süreci

Bu politika, mevcut personele e-posta ile tebliğ edilir. Ayrıca ASHB web sitesinde, BTGM mevzuat kısmında yayınlanır.

Kabul Edilebilir Kullanım Politikasına isteyerek veya istemeyerek uygunsuz davranış personelin tabi olduğu ilgili mevzuat kapsamında değerlendirilir.

4 SORUMLULUKLAR

- Bilgi Güvenliği Ekibi: Periyodik bilgi güvenliği farkındalık eğitimlerinde politikanın gündem ve ihtiyaçlara yönelik bölümlerinin vurgulanması, politikanın uygulanması konusunda kullanıcılara sürekli destek verilmesi ve pratik çözümlerin geliştirilmesi, gerekli durumlarda politikaya uyumun denetlenmesi
- Personel Genel Müdürlüğü: Politikanın yeni işe başlayacak personele tebliğ edilmesi
- Sistem Yönetimi ve Ağ Yönetimi Ekipleri: Bilgi Güvenliği Ekibi ile koordinasyon halinde gerekli güvenlik ayarlarının ve çözümlerinin kullanıcılara sunulması
- Tüm BTGM Birim Yöneticileri: Sorumlu oldukları personelin politikaya uyumunun teşvik edilmesi, uyumun izlenmesi ve uyum konusunda örnek ve destek olunması
- Tüm personel: Politikaya uyulması, politikaya ve uyuma ilişkin Bilgi Güvenliği Ekibine geri bildirim ve destek talebinde bulunulması, tespit edilen / gözlenen güvenlik olay ve zayıflıklarının Bilgi Güvenliği Ekibine raporlanması

5 REFERANSLAR

- KLVZ-002 Bilgi Sınıflandırma, Etiketleme ve İşleme Kılavuzu
- PRSD-004 Bilgi Güvenliği Olayları Tespit ve Müdahale Prosedürü

6 KAYITLAR

- Risk Kabul Formu
- Onay formları

7 NOTLAR