Kolay Finansal Teknolojileri Anonim Şirketi
Bilgi Güvenliği Politikası

Amaç

Kolay Finansal Teknolojileri Anonim Şirketi **("BtcKolay"**) kurumsal olarak yürüteceği faaliyetleri kapsamında bilginin toplanması, değerlendirilmesi, raporlanması ve paylaşılması süreçlerinde güvenliğin sağlanmasına yönelik tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içerden veya dışardan kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak, son kullanıcı, idareci, sistem ve veri tabanı yöneticileri ve teknik personelin bilgi sistem ve ağları üzerinde yapacakları çalışmalarda bilgi güvenliği farkındalık, duyarlılık ve teknik bilgi düzeylerinin artırılması ile sistemsel güvenlik açıklarının ortadan kaldırılmasını sağlayarak, insan kaynaklı zafiyetlerin önlenmesi ve gizliliği, bütünlüğü ve erişilebilirliği sağlanmış bilişim alt yapısının kullanılması ve sürdürebilirliğinin temin edilmesi sureti ile; veri ve bilgi kayıplarının önlenmesi bu yolla ekonomik zarara uğranılmaması ve kurumsal prestij kaybı yaşanmaması ana ilke ve amaçlar olarak öngörülmektedir.

Kapsam

Bu doküman BtcKolay içerisinde çalışan her personeli bağlayıcı niteliktedir. Politikaların ihlali durumunda İnsan Kaynakları Disiplin Yönetmeliği kapsamında gerektiğinde kurum içinde ihlalde bulunan adına yasal işlem yapılabilir.

Bu politika bilgi güvenliğinin sağlanması için ve bilgi sistemleri tasarlarken veya işletirken uyulması gereken asgari kuralları açıklamaktadır. Ayrıca BtcKolay'da bu amaca yönelik olarak yayınlanmış tüm Bilgi Güvenliği politikaları için şemsiye oluşturmaktadır. Bu politikalar temel olarak aşağıda belirtilen hedefleri amaçlamaktadır.

- Bilgi Sistemlerinde paylaşılmakta olan her türlü verinin güvenliğini sağlamak
- İş devamlılığını sağlamak ve güvenlik ihlalinden kaynaklanabilecek kanuni riskleri en aza indirmek
- Kurumun itibarını ve yatırımlarını korumak

1- E-Posta Politikası

Bu politika şirket içerisinde e-posta altyapısına yönelik kuralları içermektedir. Kurum içerisinde kullanılan e-posta hesapları kurum kimliği taşımaktadır. Kurum bünyesinde oluşturulan e-posta hesaplarının tüm personeller için doğru kullanımını kapsamaktadır. E-Postlara şirket içi belirtilen kurallar ve düzenlemeler doğrultusunda kullanılmalıdır.

2- Şifre Politikası

Bu politikanın amacı güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve şifrenin değiştirilme sıklığı hakkında standartlar oluşturulmasıdır. Şifreler Bilgi Teknolojisi (BT) birimi tarafından oluşturulan kurallara göre oluşturulacak ve kullanılacaktır.

3- Anti-Virüs Politikası

Bu politika kurum içindeki tüm PC tabanlı bütün bilgisayarları kapsamaktadır. Bunlar tüm masaüstü ve dizüstü bilgisayar ve sunuculardır.

Anti virüs yazılımının sürekli olarak çalışır durumda olmasından ve güncellenmesinden Bilgi Sistemleri Yöneticileri sorumludur.

Tüm bilgisayarlar ve sunucularda standart ve tek anti-virüs yazılımı yüklüdür. Güncellemeleri otomatik olarak kullanıcı müdahalesi olmadan merkezi sunucu üzerinden yapılmaktadır.
Sunucu güncellemeleri standart anti-Virüs yazılımı firmasının tanımlanmış ilgili bağlantısından internet üzerinde yapmaktadır.
Kullanıcıların bilgisayarından anti virüs yazılımını kaldırmaları uzun ve kırılması güç şifreyle engellenmiştir.
Virüs bulaşan bilgisayar tam olarak temizlenmeden ağa eklenmez.

Anti-Virüs konusunda şirket standartları ve kullanıcıların uyması gereken kurallar Anti-Virüs Yazılımı Kullanımı başlığında detaylıca verilmiştir.

4- İnternet Erişim ve Kullanım Politikası

Bu politikanın amacı internet kullanıcılarının güvenli internet erişimi için gerekli olan kuralları kapsamaktadır. İnternet erişim politikası BT tarafından yayınlanmakta ve kullanıcılara aktarılmaktadır.

5- Sunucu Güvenlik Politikası

Bu politikanın amacı kurum bünyesindeki sunucuların temel güvenlik konfigürasyonlarının nasıl olması gerektiğini belirtir. Bu temel güvenlik konfigürasyonların yapılmasından ve işletilmesinden Bilgi Sistemleri sistem yöneticisi sorumludur.

Genel Konfigürasyon Kuralları

- Sunucular üzerindeki kullanılmayan servisler ve uygulamalar kapatılmaktadır.
- Uygulama servislerine erişimler loglanmakta ve erişim kontrol logları incelenmektedir.
- Sunucu üstünde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının, yönetim yazılımlarının vb. koruma amaçlı yazılımların kontrollü sürekli güncellenmesi yapılmaktadır. Anti virüs güncellemeleri otomatik, yama güncellemeleri sistem yöneticileri tarafından kontrollü şekilde yapılmaktadır. Bu yama güncelleme işlemi, değişiklik yönetiminden sayılmamaktadır.
- Sistem ve uygulama yöneticileri gerekli olmadıkça “administrator”, “root” vb. kullanıcı hesaplarını kullanmamaktadırlar. Windows ortamında gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmaktadırlar. Önce kendi kullanıcı hesapları ile giriş yapıp daha sonra genel yönetici hesaplarına geçiş yapmaktadırlar.
- Ayrıcalıklı bağlantılar teknik olarak güvenli kanallar (ssh veya ssl, ipsec vpn gibi şifrelenmiş ağ) üzerinden yapılmaktadır.
- Sunucular fiziksel olarak korunmuş sistem odalarında korunmaktadırlar.

6- Ağ Cihazları Güvenlik Politikası

Bu politika kurumun ağındaki yönlendirici (router) ve anahtarların (switch) sahip olması gereken minimum güvenlik konfigürasyonlarını tanımlamaktadır.

- Bilgisayar ağında bulunan tüm cihazların ip'leri ve mac adresleri aktif cihaz listesinde yer almaktadır.
- Yönlendirici ve anahtarlarda enable şifresi kodlanmış şekilde saklanmaktadır.
- Yönlendirici giriş portuna gelen IP adresleri kullanıcı şifresi ile kabul edilir.
- Yönlendirici ve anahtarlarda çalışan güvenli web servislerine erişim sadece Bilgi Sistemleri çalışanlarına verilmektedir.
- Yönlendiricilerde ve anahtarlarda SNMP kullanıldığı durumlarda varsayılan olarak kullanılan "public", community string'e farklı değerler atanmaktadır.
- İhtiyaçlar kontrollü şekilde eklenmektedir.
- Yazılım ve firmware'ler ilk önce test ortamlarında denendikten sonra çalışma günlerinin veya saatlerinin dışında canlı ortama taşınmaktadır.
- Cihazlar üzerinde varsayılan servisler kapatılacaktır (telnet, http). Bunların yerine güvenli protokoller ile bağlanılmalıdır (SSH, https).
- Her bir yönlendirici ve anahtarlama cihazında aşağıdaki uyarı yazısı yer almaktadır. Yönlendiriciye ulaşan kullanıcılar yasal veya yasadışı kullanıcılar uyarılmaktadır.

"Bu cihaza yetkisiz erişimler yasaklanmıştır. Bu cihaza erişim ve konfigürasyon için yasal hakkınızın olması gerekmektedir. Aksi halde gerekli yasal takip ve işlemler yapılabilir."

7- Ağ Yönetimi Politikası

Ağ yönetim politikası, ağın güvenliği ve sürekliliğini karşılayan kuralları belirlemekte, standartlaştırılmasını amaçlamaktadır.

- Bilgisayar ağlarının ve bağlı sistemlerinin iş sürekliliğini sağlamak için yedeklilik sağlanmaktadır.
- Ağ üzerinde kullanıcının erişebileceği servisler kısıtlanmaktadır.
- Sınırsız ağ dolaşımı engellenmiştir.
- İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmıştır (Firewall vb.).
- Ağ erişimi VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmıştır.
- Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmıştır.
- Ağ bağlantıları periyodik olarak kontrol edilmelidir.
- Ağ üzerindeki yönlendirme kontrol edilmektedir.
- Bilgisayar ağına bağlı bütün makinelerde kurulum ve konfigürasyon parametreleri kurumun güvenlik politika ve standartlarıyla uyumlu olarak yapılmaktadır.
- Bilgisayar ağındaki adresler, ağa ait konfigürasyon ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı bir şekilde saklanmaktadır.
- Firewall olarak kullanılan cihazlar başka amaç için kullanılmamaktadır.
- Bilgisayar ağıyla ilgili sorumlulukları desteklemek amacıyla ağ dokümantasyonu hazırlanmakta, ağ cihazlarının güncel konfigürasyon bilgileri saklanmaktadır.
- Bilgisayar ağı üzerinde gerçekleşen işlemler takip edilmektedir.

8- Uzaktan Erişim Politikası

Bu politikanın amacı herhangi bir yerden kurumun bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar yetkisiz kullanımdan dolayı kuruma gelebilecek potansiyel zararları en aza indirmek için tasarlanmış olup, uzaktan erişimin güvenli şekilde gerçekleşmesini amaçlamaktadır.

9- Kablosuz İletişim Politikası

Bu politika kurum bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını (dizüstü bilgisayar, akıllı cep telefonları, PDA, tablet vs.) kapsamaktadır. Kablosuz cihazların gerekli güvenlik tedbirleri alınmaksızın kurumun bilgisayar ağına erişimini engellemeyi amaçlamaktadır.

10 - İş Sürekliliği Yönetimi Politikası

Bilgi güvenliği ve iş sürekliliğiyle ilgili standartlar belirlenmektedir.
Bu kapsamda;

- Bilgi sisteminin kesintisiz çalışması için gereken önlemler alınmıştır.
- Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlanması için aynı ortamda kümeleme (cluster), uygulanmaktadır. Risk işleme planı ile ele alınmış ve değerlendirilmiştir.
- Acil durumlarda sistem logları yedeklenmektedir.
- Bir güvenlik ihlali yaşandığında BT çalışanlarına acil olarak bilgilendirilmektedir.
- Acil durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır:
- Seviye A (Bilgi Kaybı): Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi.
- Seviye B (Servis Kesintisi): Kurumsal servislerin kesintisi veya kesintiye yol açabilecek durumlar.
- Seviye C (Şüpheli Durumlar): Yukarıda tanımlı iki seviyedeki durumlara sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.
- Her bir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin kuruma getireceği kayıplar ve bu risk oluşmadan önce ve oluştuktan sonra hareket planları risk işleme planı ile dokümante edilmiştir.
- Acil durumlarda şirket çalışanları Bilgi Sistemlerine rapor etmektedir, ihlal bildirimi doğrudan üst yönetime raporlanmaktadır.

11- Kimlik Doğrulama ve Yetkilendirme Politikası

Bu politika kurumun bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarını tanımlamaktadır. Bilgi sistemlerine erişen kurum çalışanları ve kurum dışı kullanıcılar bu politika kapsamındadır.

- Kurum sistemlerine erişebilecek kurumdaki kullanıcıların ve kurum sistemlerine erişmesi gereken diğer firma kullanıcılarının hangi sistemlere, hangi kimlik doğrulama yönetimi ile erişebileceğini tanımlamaktadır.
- Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri belirlenerek denetim altında tutulmaktadır.
- Gerekli minimum yetkinin verilmesi prensibi benimsenmektedir.
- Erişim ve yetki seviyeleri belirli periyotlarda kontrol edilip gerekli durumlarda güncellenmektedir.
- Tüm kullanıcılar kurum tarafından kullanımlarına tahsis edilen sistemlerdeki bilgilerin güvenliğinden sorumludur.

- Sistemlere başarılı ve başarısız erişim logları düzenli olarak tutulmaktadır. Log girişimleri incelenmektedir.
- Kullanıcı hareketlerini izleyebilmek için her kullanıcıya kendisine ait bir kullanıcı hesabı açılmaktadır.

12- Veri Tabanı Güvenlik Politikası

Kurumdaki veritabanı sistemlerinin kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlar. Tüm veritabanı sistemleri bu politikanın kapsamındadır.

- Veritabanı sistemleri envanteri ve bu envanterden sorumlu kişiler tanımlanmıştır.
- Veritabanı işletim kuralları belirlenmiştir.
- Veritabanı sistem logları tutulmakta, gerektiğinde bilgi işlem departmanı tarafından kontrol edilmektedir.
- Veritabanı yedekleme politikaları oluşturulmuş, yedeklemeden sorumlu sistem yöneticileri belirlenmiş ve yedeklerin düzenli olarak alındığı kontrol edilmektedir.
- Veritabanı erişim politikaları "Kimlik doğrulama ve yetkilendirme" çerçevesinde oluşturulmuştur.
- Hatadan arındırma, bilgileri yedekten dönme kuralları "İş sürekliliğine" uygun, kurumun ihtiyaçlarına yönelik olarak oluşturulmuştur.
- Bilgilerin saklandığı sistemler, fiziksel güvenliği sağlanmış sistem odasında tutulmaktadır.
- Yama ve güncellemeler yapılmadan önce bildirimde bulunulmakta ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmekte olup, değişim yönetiminden sayılmamaktadır.
- Veritabanı sunucularında sadece rdp, ssl ve orjinal veritabanı yönetim yazılımları kullanılmakta, bunun dışında ftp, telnet vb. clear text bağlantılara kapanmıştır.
- Veritabanı sunucusuna ancak zorunlu hallerde root ve administrator olarak bağlanılmaktadır. Root ve administrator şifresi yetkili kişilerde bulunmaktadır.
- Bütün kullanıcıların yaptıkları işlemler loglanmaktadır.
- Veritabanı yöneticiliği sadece bir kişidedir.
- Veritabanı sunucularına 3. tarafların destek amaçlı erişimleri için VPN ve/veya statik IP bağlantısı tahsis edilmiştir.
- Veritabanı sunucularına ancak yetkili kişiler erişebilmektedir.
- Veritabanı sunucularında kod geliştiren kullanıcıların dışında hiçbir kullanıcı bağlanıp sorgu yapamamaktadır.
- Şifreleri 60 günlük aralıklarla değiştirilmekte ve erişim şifreleri kapalı bir zarfta kurumun kasasında saklanmaktadır.

13- Teknik Açıklık Yönetimi Politikası

Bilgi sistemlerinde var olan teknik açıklıkların tespit edilmesi, açıklıkların değerlendirilip önlemlerin ortaya konması, uygun önlemlerin seçilerek uygulanması ve uygulama sonuçlarının gözlenmesine yönelik "Teknik Açıklık Yönetimi Politikası" yürürlüktedir. BtcKolay'da üçüncü parti bağımsız firmalarca penetrasyon testi yapılabilir.

14- Görevler Ayırımı

BtcKolay'ın de varlıklarının yanlışlıkla ya da kasıtlı olarak yanlış kullanım riskini azaltmak için yetkilendirmeler kurallara bağlanmıştır.

Kuruluş varlıklarının yanlış kullanımını azaltmak amacıyla çelişen görevler ve sorumluluklar ayrılır.
Bir olayın başlatılması onun yetkilendirilmesinden ayrılır. Bununla birlikte faaliyetlerin izlenmesi, denetim kayıtları ve yönetimin gözetimi gibi diğer kontroller dikkate alınır.

15- Değişim Yönetimi Politikası

Kurum bilgi sistemlerinde yapılması gereken konfigürasyon değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesine yönelik politikaları belirlemektedir.

16- Bilgi Sistemleri Yedekleme Politikası

Bu politika kurumun bilgi sistemleri yedekleme politikasının kurallarını tanımlamaktadır. Tüm kritik bilgi sistemleri ve bu sistemleri işletilmesinden sorumlu çalışanlar bu politika kapsamındadır. Ayrı bir 'Veri Yedekleme Politikası' belirlenmiştir.

17- Kişisel ve Harici Ekipmanların Kullanımı Politikası

Bu politika kurum çalışanlarının ve üçüncü parti firmaların kendi bilgi işleme ekipmanlarını BtcKolay'ın bünyesinde ya da uzaktan bağlantı yaparak iş amaçlı kullanmasındaki kuralları belirler.

- Prensip olarak BtcKolay'ın çalışanlarının kendi özel ekipmanlarını iş amaçlı kullanmalarına müsaade edilmez. İstisnai durumlarda bu türden ekipmanların iş amaçlı kullanımı yalnızca uzaktan bağlantı (VPN) altyapısıyla mümkündür.
- Tedarikçi firmaların ekipmanlarının kurum bünyesinde ya da uzaktan iş amaçlı kullanılması durumunda BGYS güvenlik gereksinimleri dikkate alınır.
- Bu türden bağlantılarla ilgili tüm kayıt altına alınma gereksinimleri dikkatlice ve noksansız yerine getirilir, aktivite geçmişi (loglar) düzenli bir şekilde takip edilir.
- "Erişim Politikası", "BG Kullanıcı El Kitapçığı" ve "Bilişim Kaynakları Kullanım Standartları" da öngörülen BGYS gereksinimleri bu türden bağlantılarda aksatmadan uygulanır.

18- Veri Transfer Politikası

Bu politikanın amacı üçüncü parti kişi ve kuruluşlarla ve kurum içi çalışanlarla bilginin taşınması sürecinde izlenecek yöntemleri belirlemektir.

- Tüm bilgi varlıklarının taşınması ve aktarılması varlık sahibinin bilgisi ve onayıyla mümkündür.
- Taşıma ya da aktarma sürecinde bilgi güvenliği gereksinimleri yerine getirilmeli. Bilginin bütünlüğü, gizliliği ve erişilebilirliğini etkileyebilecek riskler tespit edilerek bu risklerin bertaraf edilmesi yoluna gidilmelidir.
- Aktarma ortamlarında, taşıma kanallarında ve haberleşme tesislerinde güvelik standartlarına uyulmalıdır.
- Kullanılması gereken elektronik bilgi taşıma kanallarının seçiminde (Ör: e-posta, FTP, wetransfer, Dropbox vb.) BtcKolay'ın Bilgi Sistemleri departmanının onayına başvurulmalıdır. Güvenliği onaylanmamış ve bilinmeyen transfer yöntemleri kesinlikle kullanılmamalıdır.
- Verinin güvenli ve istenen şartlarda aktarıldığını temin için İletim, sevk ve alındı kontrolü yapılmalıdır.

- Bilgi transferinde Bilgi etiketleme kuralları göz önünde bulundurularak bilgi varlığının paylaşımında “Genel”, “Dahili”, “Gizli” ve “Kişisel” bildirim etiketlerine göre dağıtımı ya da aktarması yapılmalıdır. Örnek “Genel” etiketli bir bilginin dağıtımı yapılabilirken “Dahil” etiketli bilgi varlığının aktarılmasında mutlaka varlık sahibinin, “Gizli” ve “Kişisel” etiketli bilgi varlığı için Varlık Risk sahibinin onayı alınmalıdır. Bu konuda “PR- Bilgi Etiketleme ve İşleme Prosedürü” ne başvurulmalıdır.
- Bilgininin elektronik ortamda transferinde “Gizli” ve “Kişisel” etiketli veriler şifrelenmelidir.
- Bilginin gizlilik ve ifşa edilmemesi anlaşmaları kuruluşun çalışanları ve üçüncü parti firmalarla yapılarak yasak güvence altına alınmalıdır.
- Bilgi transfer sürecinde oluşabilecek her türlü bilgi güvenliği ihlal olayları anında BT çalışanlarına bildirilmesi ve BtcKolay bilgi transferlerinde oluşabilecek her türlü güvenlik ihlali BT çalışanlarına tarafından hızla ele alınarak önleyici tedbirler acilen hayata geçirilmeli ve kayıt altına alınmalıdır.

19- Risk Yönetimi Politikası

BtcKolay’da Risk Yönetimi; Kurumun Stratejik Hedeflerini gerçekleştirme sürecini olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir.
Buna göre kurumun temel risk yaklaşımı;

- BGYS Risk Yönetim Sisteminin üretim tesisi ile iş sürekliğini temin etmek,
- İç ve dış mevzuata uygun olarak tesis edilen Risk Yönetim Sistemini, kurumsal yapının entegre bir parçası haline getirmek,
- Risk yönetimini kurum stratejileri doğrultusunda yapmak, proaktif aksiyonlarla riskleri kabul edilebilir seviyelerde tutmak,
- Riskleri, katılımcı yönetim anlayışı ile tanımlamak ve risk portföyünü devamlı güncellemek,
- Her tehditte fırsatlar, her fırsatta tehditler olabileceği anlayışı ile risklere yaklaşmak,
- Risk tutumunu, değişen şartlar doğrultusunda güncelleyerek, doğru risklerin doğru miktarda alınmasını sağlamak,
- Etkin iletişim ve raporlama ile paydaşlar nezdinde itibar ve güven ortamını tesis etmek,
- Risk yönetim sisteminin performansını ölçmek, risk yönetim sistemi ve riskleri sürekli iyileştirerek, kurumsal yapıyı dinamik bir yapıda tutmak,
- Değişen ve gelişen şartlar doğrultusunda Risk Politikasını gözden geçirmek ve iyileştirmek.

Bu kapsamda Risk gerek varlık temelli ve gerekse de süreç bazlı olarak ele alınıp tehdit ve açıklıklardan hareketle risk değerlendirmesi yapılır.
Risk Değerlendirmesi yöntemi ve seçilen metodoloji “Risk Değerlendirme Prosedürü” de ele alınmıştır.

20- Kriptografik Kontroller ve Anahtar Yönetimi Politikası

20.1 Giriş
Veriyi korumanın yollarından biri de şifrelemedir. Hassas bilgiler bilinen ve test edilmiş şifreleme yöntemleri ile saklanmalıdır.
Süreç içerisinde kırılması uzun zaman alan algoritmalar daha kısa zamanda çözülebilmektedir, bu nedenle uygulama içindeki algoritmalar zamanla gözden geçirilmeli ve güncellenmelidir.

- BtcKolay’da Kriptografik Kontroller aşağıdaki maksatlarla kullanılır;

- Gizlilik: Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelemenin kullanılması,
- Bütünlük/Güvenilirlik: Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için sayısal imzaların veya mesaj doğrulama kodlarının kullanılması,
- İnkar edilemezlik: Bir olay veya faaliyetin oluşumu veya oluşmadığının kanıtını elde etmek için kriptografik tekniklerin kullanılması.

20.2 Uygulama

- Personelin gönderdiği maillerde, hiçbir şekilde yönetici, kullanıcı gibi hesap şifreleri bulundurulmamalıdır.
- İşletim sistemi üzerinde saklanan kullanıcı ve yönetici hesabı şifrelerinin kriptolu olarak saklandığı belirli zaman aralıklarında kontrol edilmelidir.
- Sunuculara kriptolu bağlantı ile bağlanılmalı, kripto kullanmayan yöntemler tercih edilmemelidir. Düz metin kullanarak veri alışverişi yapan yöntemlerin kullandığı portlar gerekirse kapatılmalıdır.
- Kripto kullanımı ile ilgili hangi iş bilgisinin korunacağı konusunda genel prensipler belirlenmelidir.
- Risk belirleme esasına dayalı olarak gereksinim duyulan koruma seviyesi ile şifreleme algoritmasının türü, gücü ve niteliği ortaya konulmalıdır.
- Taşınabilir ortam, cihaz ve iletişim hatlarında iletilen hassas bilginin korunması için şifreleme mekanizmalarının kullanımı belirlenmelidir.
- İçerik denetimi üzerinden yapılan kontrollerde şifrelenmiş bilgi kullanımının etkileri değerlendirilmelidir.
- Kriptografik anahtarların korunması, şifrelenmiş bilginin kaybolması, tehlikeye düşmesi veya hasar görmesi durumunda tekrar geri alınması ile ilgili metotları içeren anahtar yönetimi uygulanmalıdır.
- Politikanın uygulanması, anahtar üretimini de içeren anahtar yönetimi ile ilgili görevler ve sorumluluklar belirlenmelidir.

20.3 Anahtar Yönetimi

Anahtar yönetiminde aşağıda belirtilen ve üzerinde mutabık kalınan standartlar, prosedürler ve güvenli yöntemler seti dikkate alınmalıdır;

- Farklı şifreleme sistemleri ve farklı uygulamalar için anahtarların üretimi,
- Anahtarın alınmasını takiben nasıl faaliyete geçirileceği de dâhil kullanıcılara anahtar dağıtımı,
- Yetkili kullanıcıların anahtar erişiminin sağlanmasını da kapsayan anahtarların saklanması,
- Anahtarların ne zaman ve nasıl değiştirileceğinin kurallarını da kapsayan anahtarların değişimi ve güncellenmesi,
- Güvenliği tehlikeli bir duruma düşmüş anahtarlar,
- Anahtarların geri alımı ve kullanılmaz hale getirilmesini kapsayan anahtarın yürürlükten kaldırılması (Ör. Anahtarın güvenliğinin tehlikeli bir duruma düşmüş olması veya kullanıcının kuruluştan ayrılması durumları),
- Anahtarların arşivlenmesi ve imhası ,
- Anahtar yönetimi ile ilgili faaliyetlerin izleme kayıtlarının (log) tutulması.

21- Bilgi Sistemleri Kabul Edilebilir Denetim Koşulları Politikası

Amaç: Kurum Bilgi sistemlerine yapılan denetimlerin süreçler üzerinde yapacağı bilgi güvenliği etkilerini azaltmak.
Kapsam: Kurum Bilgi sistemlerine yapılan iç ve dış denetimler

- Sistemler ve veriye erişim için denetim gereksinimleri konusunda ilgili yönetim ile mutabık olunur.
- Teknik denetim testlerinin kapsamına karar verilir ve kontrol edilir.
- Denetim testleri, yazılım ve veriye sadece okunabilir erişim ile sınırlandırılır.
- Sadece okunabilir erişim dışında kalan erişim için, sistem dosyalarının ayrı bir ortamdaki kopyalarına izin verilir, bu kopyalar denetim tamamlandığında silinir veya denetim dokümantasyon şartları altında bu tür dosyaları tutmak için bir zorunluluk varsa uygun koruma sağlanır.
- Özel ve ek bir işleme için gerekler tanımlanır ve kararlaştırılır.
- Sistem erişilebilirliğini etkileyebilecek denetim testleri çalışma saatleri dışında çalıştırılır.
- Tüm erişimler izlenir ve referans kaydı oluşturmak için kaydedilir.

22- Fikri Mülkiyet Hakları Politikası

Kapsam
Fikri mülkiyet hakları; yazılım veya belge telif haklarını, tasarım haklarını, markaları, patentleri ve kaynak kod lisanslarını kapsar.
Uygulama

- Tüm çalışanların sorumluluğundadır. Kuruluşumuz ulusal ve uluslararası tüm yasa ve düzenlemelere uymayı taahhüt eder.

- Yazılım ve diğer ürünlerinin yasal kullanımını belirleyen fikri mülkiyet haklarına uyum İnsan Kaynakları politikasında ele alınmış olup tüm çalışanlara okutturularak imza alınmıştır.

- Yazılım ve lisanslar satın almaları telif haklarının ihlal edilmemesini temin etmek için sadece bilinen ve seçilmiş tedarikçilerden alınır.

- Fikri Mülkiyet Hakkının çalışan tarafından ihlali İnsan Kaynaklarının İlgili Disiplin Yönetmeliği kapsamında ele alınır

- Varlık envanterleri oluşturularak tüm lisanslar ve fikri mülkiyet hakkı kapsamındaki Bilgi varlıkları kayıt altına alınır.

- Lisansların, ana disklerin, kılavuzların ve benzerlerinin sahipliğine dair ispat ve delillerin muhafaza muhafaza edilir.

- Kurum bilişim ekipmanlarına yazılım ve lisanslı ürünlerin kuruluşu yalnızca yetkili BT ekibi tarafından yapılır.

- Telif hakkı yasası tarafından izin verilen dışında kitapların, makalelerin, raporların ve diğer belgelerin tam veya kısmen kopyalanmasına izin verilmez.