BİLGİ GÜVENLİĞİ POLİTİKASI

Amaç

Hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetimin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

Kapsam

Bu politika Kurum bünyesinde yapılan faaliyetlere ve bu işlemlere ilişkin Müdürlüklerin faaliyetlerinden elde edilen elektronik bilgi varlıkların korunması, Kurum bünyesinde tutulan kişisel verilerin kanun kapsamında işlenmesi, saklanması, korunması, gizliliğinin ve bütünlüğünün bozulmaması için kullandığı bilgi güvenliği süreçlerini kapsamaktadır.

Hedef Grup

Müdürlükler

Yürürlük Alanı

Çaycuma Belediyesi çalışanları, tüm kurum müdürlükleri

İÇERİK

1. Giriş ve Politikanın Amacı

Kurumumuzun sahip olduğu tüm fiziksel ve elektronik bilgi varlıklarının gizliliğinin ve bütünlüğünün korumasını taahhüt etmektedir.

2. Politikanın Kapsamı

Kurumumuz bilgi güvenliğinin sağlanması amacıyla gerekli olan alt yapısını oluşturmak ve sürekliliğini sağlamak için finansmanı, yeterli donanımı ve altyapıyı bulunduracaktır.

Bilgi güvenliği sistemi faaliyetlerimiz, acil durum planları, veri yedekleme prosedürleri, virüslerden ve bilgisayar korsanlarından sakınma, erişim kontrol sistemleri ve bilgi güvenliği ihlal bildirimi gibi konulardan oluşmaktadır.

Risk değerlendirmeleri sonucunda ihtiyaçları belirleyip bu amaçların başarılması için gerekli olan kaynaklar ve şartlar sağlanacaktır. Yapılan risk değerlendirmeleri sonucunda sistemde tespit edilen açıklar ve tehditler bertaraf edilerek personellerimiz ve hizmet sağladığımız müşterilerimizin bilgilerinin bilgi güvenliği politikamız gereği korunması sağlanacaktır.

Personelimizin, Bilgi Güvenliği politikamızı yerine getirmek için Bilgi Güvenliği Yönetim Sistemi şartlarını çalışma biçimi haline getirmeleri sağlanacaktır. Tüm personel ve üçüncü tarafların Bilgi Güvenliği Yönetim Sistemi ile ilgili uygun eğitimleri alması sağlanacaktır.

Bilgi güvenliği ile ilgili uygulanabilir şartlar ve bu şartların getirdiği fırsatlar ve gereklilikler yerine getirilecek ve bu şartlar sürekli iyileştirilecektir.

Personelimizin (Sözleşmeli çalışanlar dahil) ve tüm ilgili tarafların bu sisteme adaptasyonu sağlanacaktır.

3. Kısaltmalar ve Tanımlar

Kurum: Çaycuma Belediyesini ifade eder.
Personel: Çaycuma Çalışanını ve Sözleşmeli Çalışanı ifade eder.
BT: Bilgi Teknolojisi

4. Erişim Kontrol Politikası

Kurumumuzun iç taleplerine zamanında ve doğru çözümler bulabilmemiz için yasal mevzuata uygun şekilde verinin bütünlüğünün sağlanması için:

- Oryantasyon aşamasında personele gerekli bilgiler aktarılmış,
- Gerekli altyapı ve donanım belirlenmiş,
- Gerekli altyapı ve donanımın kesintisiz olarak sağlanması için, gerekli kaynaklar ayrılmış,

• Kurumumuzun, bilgilerinin korunması açısından yapılması gerekenler personelimize eğitimlerle aktarılmış, Kurum çalışanlarımıza “iş sözleşmeleri” ile sorumlulukları yazılı hale getirilmiş,
• Tüm verilerin yedeklenmesi amacıyla gerekli alt yapı belirlenip, sorumlular tanımlanmış,
• Network üzerinde gerekli erişim işlemleri sınırlandırılmış,
• Bilgi güvenliği konusundaki temel prensiplerimiz gizlilik, bütünlük ve yetkililerce erişilebilirlik olarak belirlenmiştir.

5. Temiz Masa Politikası

Temiz Masa Politikamızın amacı, normal çalışma saatleri süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar ve kaldırılabilir depolama ortamları ve kişisel bilgisayarlar için gerekli şartları tanımlamaktır.

Personelin aşağıdaki şartlara uygun davranmaları gerekmektedir.

Çalışma saatleri dışında bilgisayarlar kapalı ya da kilitli şekilde bırakılmalıdır.

Çalışma saatleri içerisinde başından ayrıldığında mutlaka bilgisayar kilitli bırakılmalıdır. (Ekran koruyucu 5-10 dk arasında devreye girmelidir ve şifre koruması olmalıdır.)

Yazıcıların üzerinde kişisel bilgileri ve gizli bilgileri içeren dokümanlar bırakılmamalıdır.

Yazıcı ile işlem tamamlandığından yazıcı kilit ekranına alınmalıdır.

Yazıcı şifreleri personel dışındakilerle paylaşılmamalıdır.

Mesai bitiminde çalışma masası üzerinde kurum veya kişisel bilgileri içeren bir evrak bırakılmamalıdır.

Kuruma ait dokümante edilmiş gizli bilgiler kilitli ortamda tutulmalıdır.

Gizlilik dereceli evraklar, işlevini tamamladıktan sonra imha edilmelidir.

Kuruma ait antetli kağıtlar kilitli dolaplarda tutulmalıdır.

Hassas ve sınıflandırılmış bilgi basıldığında yazıcıdan hemen temizlenir.

Bilgisayarların masaüstlerinde kuruma ait özel bilgiler içeren dokümanlar bulundurulmamalıdır.

Bilgisayarlara ait olan şifreler kesinlikle kâğıt ortamlara yazılı bir şekilde bırakılmamalıdır.

6. Güvenli Geliştirme Politikası

Güvenli geliştirme, güvenli hizmet için bir gerekliliktir. Bunun için öncelikle güvenli geliştirme ortamları kullanılacaktır. Yazılım geliştirme hizmetlerimizin yaşam döngüsü dâhilinde, tasarım aşamasında güvenlik gereksinimleri belirlenerek, bu güvenlik gereksinimlerinin uygulanması sağlanacaktır. Yazılım geliştirme hizmetlerimizde güvenlik kontrol noktaları oluşturularak yapılan testlerde bu güvenlik kontrollerine uyulması sağlanacaktır. Tüm geliştiriciler açıklıklardan kaçınma, açıklıkları bulma ve düzeltme konusunda kendilerini geliştireceklerdir.

7. Bilgi Güvenliği

Bilgi, diğer önemli ticari ve kurumsal varlıklar gibi, bir işletme ve kurum için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği iş sürekliliğini sağlamak, kayıpları en aza indirmek için tehlike ve tehdit alanlarından korur. Bilgi güvenliği, bu politikada aşağıdaki bilgi niteliklerinin korunması olarak tanımlanır:

Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek,

Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek,

Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek. Bilgi güvenliği politikası dokümanı, yukardaki korumaları ve gereksinimleri sağlayabilmek için oluşturulmuş denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtildiği dokümandır.

8. Bilgi Güvenliği Hedefleri ve Amaçları

Bilgi Güvenliği Politikası, personelin, Kurum güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini artırmak ve bu şekilde Kurumda oluşabilecek riskleri minimuma indirmek, Kurumun güvenilirliğini ve imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, teknik güvenlik kontrollerini uygulamak, Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla Kurumun tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarını korumayı hedefler.

9. Politikanın Genel Esasları

Kurum, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan

kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder.
Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BT prosedürleri ile düzenlenir. Belediye çalışanları ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür. Bu kural ve prosedürlerin, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.

Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001 "Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimler (Information Security Management Systems Requirements)" standardını temel alarak yapılandırılır ve işletilir. BT' nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların katkısıyla, **İnsan Kaynakları Müdürlüğü yürütür.** BT dokümanlarının gerektiği zamanlarda güncellenmesi Bilgi İşlem Müdürlüğü sorumluluğundadır. Ek, form, talimat gibi dokümanların güncellenmesi ise ilgili müdürlüklerin sorumluluğundadır. Kurum tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça Kuruma aittir. Kritik iş süreçlerini büyük felaketlerin ve işletim hatalarının etkilerinden korumak amacıyla iş sürekliliği yönetimi uygulanır. Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut Kurum çalışanlarına ve yeni işe başlayan çalışanlara verilir.

Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.

9.1. Temel BT Prensipleri

Gerekli durumlarda çalışanlar ve üçüncü taraflarla kurumun gizlilik ihtiyaçlarını güvence altına almayı amaçlayan gizlilik anlaşmaları yapılır. Dış kaynak kullanım durumlarında oluşabilecek güvenlik gereksinimleri analiz edilerek güvenlik şart ve kontrolleri şartname ve sözleşmelerde ifade edilir. Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır. Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir. İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır. Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır. Kuruma ait bilgi varlıkları için Kurum içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır. Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin

prosedür ve talimatlar geliştirilir ve uygulanır. Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır. Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır. Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir. Bilgi güvenliği ihlal olayları ve zayıflıklarının raporlanması için gerekli altyapı oluşturulur. İhlal olay kayıtları tutulur, gerekli düzeltici önleyici faaliyetler uygulanır ve düzenlenen farkındalık eğitimleri vasıtasıyla güvenlik olaylarından öğrenme sağlanır. Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır. Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.

9.2. Uyulması Gereken BT Kuralları

Uyulması Gereken Kabul Edilebilir Kullanım Kuralları, çalışanlar ve 3. taraflar için kurum iş süreçlerinde ve ilgili çalışmalarında bilgi depolama, iletim ve kullanım biçimleri ile ilgili uyulması gereken kuralları belirler.

Aşağıda yer alan davranışlar; aksi yönde açık ve net bir iş tanımı, talimat veya prosedür bulunmadıkça Bilgi Güvenliği Politikası' nın ihlali olarak değerlendirilir.

Kurum tarafından sağlanan bilgi işlem sistemleri ve uygulamalar iş amaçlı olarak kullanılır. İş süreçlerini engellemeyecek düzeyde ve Bilgi Güvenliği Politikası'nı ve BT prosedürlerini ihlal etmeyen kişisel kullanımlar kabul edilebilir kapsamda değerlendirilir.

Çalışma alanlarında, "Temiz Masa ve Temiz Ekran" prensiplerine uygun olarak, Genel özellikteki bilgiler dışında bilgilerin başkalarınca görülmesine imkân verilmeyecek şekilde önlemler alınmalıdır;

Genel olmayan belgeler, masalarda bırakılmamalıdır.

Genel olmayan dosyalar üzerinde çalışılırken bilgisayar ekranları herkesin görebileceği konumda bırakılmamalıdır.

Genel olmayan dokümanlar diğer kişilerce görülmesini engellemek amacıyla, kullanılmadığı zamanlarda masa üstlerinden kaldırılıp gerekli korumaları alınmış çekmece ve dolaplarda saklanmalıdır.

Genel olmayan belgeler dışında doğrudan işle ilgili olarak kendisine ulaştırılmayan ya da teslim edilmeyen Kurum belgelerini incelememeli, değiştirmemeli, saklamamalı, kopyalamamalı, silmemeli ve paylaşmamalıdır.

Kurum tarafından açıkça belirtilen durum ve yöntemler dışında 3. taraflar ile kurum bilgilerini paylaşmamalı, satmamalı, aktarmamalı, yayınlamamalı ve internet ortamında paylaşmamalıdır.

Birim çalışanları çalıştıkları ortamdaki masa ve dolap çekmecelerini kilitli tutmalı ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmamalıdır.

Bilgisayarlar, aktif kullanım dışında iken şifreli ekran koruyucular devreye alınmalıdır. Mesai zamanları dışında bilgisayar sistemleri kapalı tutulmalıdır.

Çalışanlar, kendilerine verilmiş olan kullanıcı adı ve şifreleri sadece kendileri kullanmalıdır.

Çalışanlar, kendilerine verilmiş olan kullanıcı adı ve parola bilgilerini yetkilendirilmemiş kişilerin ele geçirmesine imkân verecek şekilde söylememeli, yazmamalı, kaydetmemeli ve elektronik ortamda depolamamalıdır.

Kurumun, bilgi ve haberleşme sistemleri ve donanımları (İnternet, e-posta, telefon, çağrı cihazları, faks, bilgisayarlar, mobil cihazlar ve cep telefonları vb.) Kurum işlerinin yürütülmesi için kullanılmalıdır. Bu sistemler yasadışı, Kurumun diğer politika, standart ve rehberlerine aykırı veya Kuruma zarar verecek herhangi bir şekilde kullanılmamalıdır.

Kuruma ait bilgi sistemleri üzerindeki kaynaklara erişecek tüm bilgisayarlar etki alanına dahil edilerek kullanılmalıdır.

Gerekmedikçe bilgisayar kaynaklarını paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde sadece ilgili kişilere yetki verilmelidir.

Gizli ve hassas bilgiler elektronik ortamda Belediye içine ve özellikle Belediye dışına gönderilmeden önce şifrelenmelidir.

Gizlilik dereceli bilgiler içeren belgeleri, elektronik ortamları ve bilgi işlem sistemlerini korumak için gerekli fiziksel önlemleri uygun şekilde yerine getirmemelidir.

Kuruma ait bilgi işlem sistemlerini, veri tabanlarını, dosyaları, ağ topolojilerini, cihaz konfigürasyonlarını ve benzeri kaynakları, Kurum tarafından açıkça

yetkilendirilmedikçe 3.taraflar ile paylaşmamalıdır.

Kurum çalışanları, çalıştıkları sürece veya Belediyeden ayrılmaları (emeklilik, istifa, vs.) durumunda Kurum bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur

Taşınabilir sistemlerin kullanıcıları, bu sistemlerin güvenliğini sağlamak üzere kendilerini sorumlu görmelidirler. Başta kullanıcı bilgisayarları ve sunucular olmak üzere mümkün olan tüm sistemler, zararlı yazılımlara karşı korunması için Virüslü ve Zararlı Yazılımdan Korunmak adına dikkatli davranmalıdırlar.

Gizlilik dereceli bilgilerin posta, faks, telefon, e-posta ve benzeri elektronik yöntemlerle iletiminde Bilgi İşlem Hizmetleri Prosedürü “ne uygun davranılmalıdır.

Herkese açık bilgiler dışındaki bilgileri internet üzerinde, haber gruplarında, posta listelerinde ve forumlarda paylaşmamalıdır.

Yeni bilgi sistemlerinin devreye alınması ve geliştirilmesi Bilgi İşlem Hizmetleri Prosedürü “ne uygun yapılmalıdır.

Sosyal medya ortam kullanımı Sosyal Medya Kullanım Prosedürü” kurallarına uygun olmalıdır.

Çalışanlara ve gerekli görülen durumlarda 3. taraflara tahsis edilen e-posta hesapları, E-posta Kullanım Prosedürü “ne uygun şekilde kullanılmalıdır. Bilgi işlem sistemlerinin teknik güvenlik gereksinimlerine uygun durumda bulunup bulunmadığı, Bilgi İşleme Prosedürü “ne uygun şekilde kontrol edilmelidir.
Kuruma ait bilgi işlem sistemlerini izinsiz olarak kullanım dışı bırakılmamalı, yeri değiştirilmemeli ve Kurum dışına çıkartılmamalıdır.

Kullanım gerekliliği Kurum tarafından yazılı olarak belirtilen güvenlik yazılımlarını (örn. Anti virüs, kişisel güvenlik duvarı, vb.) bilgi işlem sistemlerden kaldırmamalı veya devre dışı bırakmamalıdır.

İstemciden istemciye dosya paylaşım programlarını kurum bilgisayarlarına yüklememeli ve kullanmamalıdır.

Kuruma ait bilgisayarlara, Kurumun yasakladığı yazılımları yüklememeli ve çalıştırmamalıdır. Kurum tarafından lisanslanmış yazılımları çoğaltmamalı, paylaşıma

açmamalı ve Kurum dışına çıkarmamalıdır.

Etki alanına dahil olmayan sistemler ile etki alanına dahil olan sistemler arasında bilgi aktarımı yapılmamalıdır.

3. Taraflar ile gizlilik sözleşmesi imzalanmadan ve yetkili Kurum çalışanınca nezaret edilmeden kurum bilgi işlem sistemlerine ve donanımlarına bağlanmamalı ve çalışmalarına izin verilmemelidir.

Sunucu sistemleri üzerinde, kişisel bilgisayar uygulamalarını (örn; e-posta programları, ofis uygulamaları, yazılım geliştirme araçları, network test araçları, vb.) kurulmamalı ve kullanılmamalıdır.

İş süreçleri için gerekmeyen ve kullanılmasına izin verilmeyen sunucu hizmetlerini bilgi işlem sistemleri üzerinde çalıştırılmamalıdır. Kurum tarafından sağlanan ve kullanım amaç ve biçimleri yazılı olarak bildirilen kurum ağ bağlantı yöntemleri dışında bir yöntemle internete veya başka ağlara bağlanmak için kullanılmamalıdır.

Çalışanlar, Kurum içi ya da Kurum dışı bilgi sistemlerine yetkisi olmadığı halde zorla girmeye çalışmamalıdır.

Kuruma ait bilgi işlem sistemlerine şifreleme ve parola mekanizmalarını kırmaya yönelik program ve araçlarını yüklenmemeli ve kullanılmamalıdır.
Kuruma ait bilgi sistemleri üzerinde, Kurumun bilgisi ve izni olmadan değişiklik, yükseltme, genişletme yapılmamalıdır.
İşle ilgili olmayan veya telif hakları ile korunan dosyaları Kurum bilgisayarlarına ve bilgi sistemlerine indirilmemeli, depolanmamalı, çoğaltılmamalı ve paylaşıma açılmamalıdır.

Kurum bilgi işlem sistemlerini iş dışında, eğlence amaçlı (oyun vb.) kullanılmamalıdır.
Kurum e-posta hesabı ile zincirleme e-posta gönderilmemelidir.

10. Yaptırım

Kurum politika ve prosedürlerine uyulmadığının tespit edilmesi halinde, bu ihlalden sorumlu olan çalışan ya da 3. taraf için geçerli olan usul, esas ve sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.

11. Yönetim Sorumluluğu

Yönetim Taahhüdü

Belediye belirlediği hedef ve politikalarını gerçekleştirmek için Bilgi Güvenliği Yönetim Sistemini ISO/IEC 27001'de belirtilen gereksinimleri yerine getirecek şekilde kurarak yürütür

Bu taahhüdün sonucu olarak, Kurum genelinde bilgi güvenliği farkındalık programları düzenler ve alt yapı yatırımlarını sürdürür.

BT kurulurken üst yönetim tarafından BT Yönetim Temsilcisi ve BT Yöneticisi, atama yazısı ile atanır. BT Yönetim Temsilcisi ve BT Yöneticisi değiştiğinde, işten ayrıldığında üst yönetim tarafından doküman revize edilerek atama tekrar yapılır. BT Yöneticisini belirlemek ve değiştirmek üst yönetimin yetkisindedir.

Yönetim kademelerindeki yöneticiler güvenlik konusunda alt kademelerde bulunan personele sorumluluk verme ve örnek olma açısından yardımcı olurlar. Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, Kurumun en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden Kurumdaki yöneticilerin, gerek yazılı gerekse sözlü olarak güvenlik prosedürlerine uymaları, güvenlik konusundaki çalışmalara katılmaları konusunda güvenlik ile ilgili çalışmalarda bulunan personele destek olurlar.

Kurum üst yönetimi, bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

12. Yönetim Gözden Geçirmesi

Yönetim Gözden geçirme toplantıları BT Yürütme ve Yönetim Komitesi tarafından yapılır. Bu komite BT Yönetim temsilcisi katılımında yılda en az bir kez veya ihtiyaç duyulduğunda Bilgi Güvenliği Yönetim Sisteminin uygunluğunun ve etkinliğinin periyodik olarak değerlendirmesi için toplanır. Toplantılar Yönetimin Gözden Geçirmesi Prosedürü ’ne uygun olarak yapılır.

13. Üçüncü Şahısların Bilgiye Erişimi

Kurum çalışanı olmayan 3. tarafların, bilgi sistemlerini kullanma ihtiyacı olması durumunda (ör: Belediye dışı bakım onarım çalışanları) BT Yöneticisi, bu kişilerin Kurum ile ilgili bilgi güvenliği politikalarından haberdar olmalarından sorumludur. Bu amaçla geçici ya da sürekli çalışma sözleşmelerinde sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları yapılmalıdır. Gerektiği takdirde üçüncü taraf personelinin politikaya uyması için süre tahsis edilmelidir.

14. Dış Kaynak Sağlanması

Bilgi ağı ve/veya kullanıcı bilgisayarı ortamlarının yönetimi dış kaynaklara verilirken, bilgi güvenliği ihtiyaçları ve şartları her iki taraf arasında kabul edilmiş bir sözleşmede açıkça yer almalıdır.

15. Politikanın Güncellenmesi ve Gözden Geçirilmesi

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BT Yöneticisi sorumludur. Bilgi Güvenliği Politikası organizasyonel değişiklikler, iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından değerlendirilir.

Bilgi Güvenliği Politikası Dokümanı, en az yılda bir kez gözden geçirilmelidir.

Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa versiyon değişimi olarak kayıt altına alınmalı ve her versiyon üst yönetime onaylatılmalıdır. Her versiyon değişikliği tüm kullanıcılara e-mail, sunucu üzerinden ya da yazılı olarak yayımlanmalıdır.

Gözden geçirmelerde;

Politikanın etkinliği, kaydedilmiş güvenlik arızalarının yapısı, sayısı ve etkisi aracılığıyla gözlemlenmelidir.

Politikanın güncelliği teknolojik değişimlerin etkisi vasıtasıyla gözlemlenmelidir.

Politika, sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra gözden geçirilmelidir.

16. Yürütme

Bu politikayı ihlal ettiği tespit edilen herhangi bir çalışan, işten çıkarma da dahil olmak üzere disiplin yönetmeliğindeki disiplin cezalarına tabi olabilir.

17. Dış Referans Yolları

Kişisel Verilerin Korunması Kanunu, Yönetmelikler, Tebliğler, Kurul Kararları ve sair mevzuatlar,

18. Önceki Versiyondaki Değişiklik

Yok