1. Amaç / Genel

Bu doküman, Kuruluştaki ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi kapsamındaki tüm bilgi varlıklarının güvenliğinin sağlanması, BGYS'nin kurulması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi için yönetimin desteğinin belirtildiği, BGYS'nin politika ve prosedürlerine uygun davranılmaması sonucunda oluşacak yaptırımların tanımlanması amacıyla oluşturulmuş, kapsam dahilindeki tüm personelin gereğini yerine getirmesi gereken üst seviye bir dokümandır.

2. Uygulandığı Alanlar (Departmanlar / Bölümler)

Bu politika Çelikel A.Ş.'nin tüm bölümlerini ve birimlerini kapsar.

3. Kavramlar / Kısaltmalar

Kuruluş: Çelikel A.Ş.

BGYS: Bilgi Güvenliği Yönetim Sistemi

Politika: Bir şirket, Kuruluş veya kişinin görüş, felsefe, amaç ve tutumunun belirli şekilde ifadesini, bu görüş, felsefe veya amaç doğrultusunda bir hareket planını içeren doküman tipidir.

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:

4. Yetkiler / Sorumluluklar

Bu prosedürde konu edilen faaliyetleri yürütme sorumluluğu 5 no'lu Uygulama / anlatım maddesinde detaylı olarak verilmektedir.

5. Uygulama / Anlatım

5.1. Bilgi Güvenliği Nedir?

Bilgi, diğer önemli Kuruluş varlıkları gibi, Kuruluş 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. Bilgi Güvenliği Politikası ve Bilgi Güvenliği kapsamında hazırlanan her türlü doküman kapsam dâhilinde yer alan tüm kişilerin uyması gereken esasları içermektedir.

5.2. Risk Yönetim Çerçevesi

Kuruluşun ISO/IEC 27001 risk yönetim çerçevesi; Bilgi Güvenliği ve Hizmet Yönetimi risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Risk Analizi ve Risk İşleme Planı Bilgi Güvenliği risklerinin nasıl kontrol edildiğini tanımlar. Risk İşleme Planının yönetiminden ve gerçekleştirilmesinden BGYS Komitesi ve Risk sahipleri sorumludur. Risklerin yönetimi "PRS.BGYS.02.XX Risk Değerlendirme ve Risk İşleme Prosedürü" dokümanında tanımlanmıştır.

5.3. Bilgi Güvenliği Politikası

Bilgi varlıklarımızın gizliliğini, bütünlüğünü ve erişilebilirliğini temin etmek için uyulması gereken temel kurallar aşağıda tanımlanmıştır. Ayrıca BGYS kapsamında oluşturulan diğer alt politikalarda ve prosedürlerde de uyulması gereken kurallar tanımlanmıştır.

5.3.1. Genel Esaslar

a) Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS prosedürleri ile düzenlenir. Kuruluş çalışanları ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

b) Bu kural ve prosedürlerin, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.

c) Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001:2013 " Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği Yönetim Sistemleri - Gereksinimler (Information technology - Security techniques - Information Security Management Systems - Requirements) standardını temel alarak yapılandırılır ve işletilir.

d) Kuruluş 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 Kuruluşa aittir.

5.3.2. Temel BGYS Prensipleri

a) Çalışanlar ve üçüncü taraflarla yapılan sözleşme/iş sözleşmelerinde kuruluşun gizlilik ihtiyaçlarının güvence altına almayı amaçlayan sır saklama taahhütnameleri bulunur.

b) Dış kaynak kullanım durumlarında oluşabilecek güvenlik gereksinimleri analiz edilerek güvenlik chart ve kontrolleri şartname ve sözleşmelerde ifade edilir.

c) İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.

d) Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.

e) Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.

f) Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.

g) Kuruluşa ait bilgi varlıkları için Kuruluş içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.

h) Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.

i) 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.

j) Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.

k) 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.

l) Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.

m) 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.

n) Yönetimin Gözden Geçirmesi toplantıları yılda en az 1 kez yapılır.

5.3.3. Uyulması Gereken Kabul Edilebilir Kullanım Kuralları

Uyulması gereken kurallar BGYS Kapsamında hazırlanan politika ve prosedürlerde belirtilmiştir. Tüm kurallar esas olarak "Varlıkların Kabul Edilebilir Kullanımı Politikası" dokümanında yer almaktadır. BGYS kapsamı dâhilinde yer alan tüm çalışanlar ve 3. Taraflar belirtilen kurallara uymak zorundadır.

5.3.4. Yaptırım

Kuruluşta BGYS 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 maddelerde belirlenen yaptırımlar uygulanır. Cezai yaptırımlarda öncelik hukuki, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere aittir. Tüm cezai şartlar "Yasal Gereksinimlere Uyum ve Kontrol Prosedürü" 'nde yer almaktadır.

5.3.5. Yönetimin Taahhüdü

Kuruluşun belirlediği hedef ve politikaları gerçekleştirmek için Kuruluş, Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001:2013'de belirtilen gereksinimleri yerine getirecek şekilde kurarak yürütür.

Kuruluş Üst Yönetimi, 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 taahhüdün sonucu olarak, Kuruluş genelinde bilgi güvenliği farkındalık programları düzenler ve alt yapı yatırımlarını sürdürür.

BGYS Üst Yönetim Temsilcisi ve Yönetim temsilcisi değiştiğinde veya işten ayrıldığında, Kuruluşun Üst Yönetimi tarafından doküman revize edilerek atama tekrar yapılır.

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

Kuruluş Üst Yönetimi, bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

5.3.6. Üçüncü Tarafların Yönetimi

Kuruluş çalışanı olmayıp bilgi sistemleri kaynaklarına erişim sağlayan her türlü kişi 3. Taraf olarak kabul edilir. 3. Tarafların uyması gereken kurallar ve yönetim şekli BGYS kapsamlı dokümanlarda 3. Taraf olarak ayrıca belirtilmiştir. 3. Taraf tanımına uyan her türlü kişi ya da Kuruluşla yapılacak geçici ya da sürekli çalışma sözleşmelerin imzalanması ile düzenli olarak takip edilir. Sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları hazırlanıp Kuruluşlarla Kurumsal gizlilik sözleşmesi, 3. Taraf çalışanlarıyla bireysel gizlilik sözleşmesi yapılır. Gerektiği takdirde üçüncü taraf çalışanlarının politikaya uyması için süre tahsis edilir.

5.3.7. Politikanın Güncellenmesi ve Gözden Geçirilmesi

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden Yönetim Temsilcisi sorumludur. Bilgi Güvenliği Politikası Dokümanı, en az yılda bir kez gözden geçirilir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilir ve herhangi bir değişiklik gerekiyorsa versiyon değişimi olarak kayıt altına alınır ve her versiyon Üst Yönetim'e onaylatılır. Her versiyon değişikliği intranet üzerinden yayımlanır ve yönetim temsilcisi tarafından kapsamdaki tüm kullanıcılara duyurulur.

Gözden geçirmelerde;

a) Politikanın etkinliği, kaydedilmiş güvenlik arızalarının yapısı, sayısı ve etkisi aracılığıyla gözlemlenir.

b) Politikanın güncelliği teknolojik değişimlerin etkisi vasıtasıyla gözlemlenir..

c) Bilgi Güvenliği Politikası organizasyonel değişiklikler, iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından gözlemlenir..

d) Politika, sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra gözden geçirilir.

6. Dokümantasyon

Bu doküman "PRS.KYM.07.xx DOKÜMAN ve VERİ KONTROLÜ PROSEDÜRÜ" dosyasında belirtildiği şekilde işlenir (gözden geçirilir, saklanır, revize edilir, onaylanır vb.).

7. Birlikte Geçerli Diğer Dokümanlar

Risk Değerlendirme ve Risk İşleme Prosedürü (PRS.BGYS.02)

Varlıkların Kabul Edilebilir Kullanımı Politikası (PLT.BGYS.06)

Yasal Gereksinimlere Uyum ve Kontrol Prosedürü (PRS.BGYS.05)

İş Sürekliliği Planı (FRM.BGYS.05)

Risk Analizi ve Risk İşleme Planı (FRM.BGYS.07)

Yönetimin Gözden Geçirmesi Toplantı Tutanağı (FRM.KYM.135)

Doküman Ve Veri Kontrolü Prosedürü (PRS.KYM.07)

8. Ekler

BGYS Politikası - Özet