1. Amaç, kapsam ve kullanıcılar

Bu dokümanın amacı, Kuruluşun değerli bilgi varlıklarının yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kuralların ve uygulamaların belirlenmesidir. Bu dokümanda Kuruluşun bilgi güvenliği ihtiyacını ve bilgi güvenliği kavramını Kuruluşun bilgi kaynaklarını kullanan her kişiye anlatma amaçlanmıştır. Bu dokümanla; organizasyon içerisinde, güvenlik standartları ve etkili güvenlik yönetimi uygulamaları geliştirmek için, yaygın bir temel ve iş ilişkilerinde güven sağlamak amaçlanmıştır.

Bu politika, Kuruluş Bilgi İşlem altyapısını kullanmakta olan tüm birimleri, tüm çalışanları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

Bu dokümanın kullanıcısı tüm kuruluş çalışanları ve ilgili taraflardır.

2. Referanslar ve ilgili dokümanlar

- ISO/IEC 27001 standart, madde5.2, 6.2, A.5.1

3. Tanımlar

Bilgi: Diğer önemli ticari varlıklar gibi, Kuruluş için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi birçok biçimde bulunabilir. Kâğıt üzerine yazılmış ve basılmış olabilir, elektronik olarak saklanmış olabilir, posta yoluyla veya elektronik imkânlar kullanılarak gönderilebilir, filmlerde gösterilebilir veya karşılıklı konuşma sırasında sözlü olarak ifade edilebilir.

Bilgi Güvenliği: Bilgi güvenliği, bu politikada, kuruluştaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

1. Gizlilik (Confidentiality)

2. Bütünlük (Integrity)

3. Erişilebilirlik (Availability)

Gizlilik: Bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir,

Bütünlük: Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması,

Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduğunda, bilgiye ve ilişkili kaynaklara erişebileceklerini garanti etme;

BGYS: Bilgi güvenliği yönetim sistemi

Risk Değerlendirmesi: Bilgiye ve bilgi işleme vasıtalarına karşı var olan tehditlerin değerlendirilmesi; bu tehditlerin ortaya çıkma olasılıkları, oluşma sıklıkları ve bilgi üzerine etkilerinin tespitidir.

Risk Yönetimi: Bilişim sistemlerini etkileyebilecek olan güvenlik risklerinin; uygun bir maliyette tanımlanması, kontrol edilmesi ve en aza düşürülmesi veya ortadan kaldırılması sürecidir.

4. Doküman İçeriği

4.1 Bilgi Güvenliği Politikası:

Tüm Kuruluşta çalışanların, Kuruluşun bilgi kaynaklarına ulaşmak isteyen kullanıcıların, anlaşmalı iş ortaklarının, diğer kamu Kuruluşlarının çıkarlarını BT güvenliği konusunda oluşabilecek arızalar ve ihlaller sonucu görecekleri zarardan korumak için, gerekli kontrolleri uygulamak ve önlemleri almak;

BT güvenlik arızalarının ve ihlallerinin oluşumunun mümkün olduğunca engellenmesi, bu arızaların mümkün olduğunca izole edilerek, diğer sistemlerin devamlılığının sağlanması, arıza oluşması durumunda iş ve süre kaybının en aza indirilmesi ve arızanın en kısa sürede ve kalıcı olarak düzeltilmesini sağlamak;

Bilinen ve sezilen güvenlik tehditlerine karşı, bu tehditlerin oluşma olasılığını ortadan kaldırmaya yönelik önlemlerin alınarak, gerekli kontrollerin uygulanmasını temin etmek;

Kuruluş içinde, bilgi güvenliğine yönelik sorumlulukların tayinini ve bilgi güvenliğini ilgilendiren olayların izlenebilirliğini sağlamak;

Bilgi güvenliğine yönelik istenmeyen olayların oluşma riskini azaltmak için, yönetim ve çalışanların; yeterli seviyede uyarılması, bilgilendirilmesi ve beceri kazanmasını sağlamak;

BT güvenliğinin sağlanmasına yönelik tekniklerin araştırılarak; tutarlı, etkili ve yararlı ürün ve servislerin, birimlere sunulması, birimlerde çalışanların, diğer kamu Kuruluşların ve vatandaşların Kuruluşa karşı duydukları güven unsurunun devamını sağlayarak, arttırılmasına çalışmaktır.

4.2 Amaçlar

Kuruluşun bilgi ve bilgi içeren kaynaklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin iş hedeflerini karşılar ve politikalarına uyumlu hareket eder durumda kalmasının sağlanmasıdır. Bu bölümde, mevcut finansal dönemdeki belli başlı iş hedefleri ve bu iş hedefleri doğrultusunda oluşturulmuş BGYS hedefleri bulunmaktadır.

4.2.1 İş Amaçları

- Genel ve mesleki ahlaki değerlerden ödün vermemek.
- Bütün faaliyetlerimizi yasa ve yönetmeliklere uygun olarak icra etmek.
- Yeniliklere açık olmak, en son teknolojileri uygulamak ve hedeflerimize ulaşmak için her zaman daha iyisini aramak.
- Kuruluş kültürümüze uygun olarak, çalışanlarımızı yaratıcı, gayretli ve dürüst olmaları doğrultusunda yetiştirmek ve özgüvene sahip, iletişime açık, kendilerine verilen yetkileri uygulamaya ve sorumluluk almaya hazır bireyler olarak çalışmalarına özen göstermek.
- Faaliyetlerimizin her yönden sürekli olarak gelişimi için çaba göstermek.
- Daima rekabet üstünlüğümüzü, teknik ve yönetsel becerilerimizdeki mükemmelliği gözetmek.
- Gümrükleme işlemlerinin hızlandırılması amacıyla Yetkilendirilmiş Yükümlü Sertifikası çalışmalarını gerçekleştirmek ve devan ettirmek.

4.2.2 Bilgi Güvenliği Amaçları

Kuruluş bünyesinde bir BGYS'nin kurulmasıyla, Kuruluş birimlerinin sahip olduğu bilgi varlıklarının korunması ve uygun bir biçimde yönetilmesi, Kuruluşun yasal zorunluluklara uyması, Kuruluşun üçüncü taraflar ile yapılan sözleşmelerde yer alan hükümlere uyması, Kuruluşun imajının ve güvenilirliğinin korunması amaçlanır. Ayrıca onaylanmış bir BGYS sisteminin bulunması, Kuruluşun yasal mevzuattan doğan Yetkilendirilmiş Yükümlü kapsamında gümrük işlemlerinin daha hızlı, kolay ve güvenilir olmasını sağlamakta, sorumlulukların yerine getirmesinde de (Gümrük ve Ticaret Bakanlığı'nın yayımladığı "GÜMRÜK İŞLEMLERİNİN KOLAYLAŞTIRILMASINA İLİŞKİN GÜMRÜK GENEL TEBLİĞİ") yardımcı olmaktadır.

Bu doğrultuda Kuruluş, Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) kurulması ve işletilmesini benimsemiştir ve mevcut sistemlerini bilgi güvenliği yönetim sistemi ile desteklemeyi, BGYS 'sini ISO/IEC–27001 standartlarına uygun olarak kurmayı amaçlamaktadır.

4.2.3 Hedefler

Kuruluşun bilgi güvenliği hedefleri Hedefler Formunda bulunmaktadır.

4.3 Üst Yönetimin Taahhüttü

Üst yönetim BGYS oluşturmak, uygulamak ve sürekli iyileştirmek adına; Bilginin izinsiz erişime karşı korunması, bilginin gizliliğinin korunması, yasama yürütme şartlarının yerine getirilmesi, tüm çalışanlara bilgi güvenlik eğitimlerinin verilmesi için kaynak ihtiyacı sağlamayı taahhüt eder.

Görev ve sorumlulukları:

- Bilgi güvenliği altyapısını oluşturmak için sunulacak projelere ait yönetim temsilcisini ve BG Kurulunu atamak

- Bilgi güvenliği yetkilileri tarafından hazırlanmış bilgi güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için hazırlanmış projelere gerekli kaynağı ayırmak

- Hazırlanan politikaları onaylamak

- Kontrol seçimlerine ve risk kabul kriterlerine onay vermek

- Belirli aralıklarla yapılacak olan bilgi güvenliği toplantılarına başkanlık etmek

4.4 Sürekli İyileştirme

Kuruluş; denetim sonuçlarını, izlenen bilgi güvenliği olaylarının analizini, penetrasyon testlerini, düzeltici faaliyetleri ve yönetim gözden geçirmelerini kullanarak BGYS'ni sürekli olarak iyileştirir.

5. Geçerlilik ve Doküman Yönetimi

Bu politika Kuruluşun Üst Yönetimi tarafından onaylanmıştır ve bu politikanın uygulanmasının sağlanması, denetiminin yapılması ve güvenlik ihlallerinde gerekli yaptırımın uygulanması konusundaki desteğinin bir ifadesidir.

Tüm kuruluş çalışanları ve gerekli görüldüğü hallerde iş ortakları, tedarikçiler ve müşteriler bu politikadaki maddelere uymakla yükümlüdür.

Bilgi güvenliğinin yönetiminden, denetiminden, politikaların onaylanmasından BG Kurulu sorumludur.

Güvenlik ihlal olaylarının araştırılması, soruşturulması ve gerekli önlemlerin alınmasında Yönetim Temsilcisi sorumludur.

Bilgi güvenliğini ilgilendiren tüm konularda politikaları, standartları ve kılavuzları oluşturmak, bunların uygulanmasını koordine etmek ve denetlenmesini takip etmekten Yönetim Temsilcisi sorumludur.

Bu politika yılda en az bir kez gözden geçirilir ve gerekirse güncellenir.

6. REVİZYON BİLGİSİ

Revizyon Numarası	Revizyon Tarihi	Revizyon Yapılan Madde	Revizyon Nedeni
00	14.05.2018		İlk Yayın
01	13.12.2018		Dosya formatında düzenleme