P00 BİLGİ GÜVENLİĞİ POLİTİKAMIZ

1. AMAÇ VE KAPSAM

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

2. SORUMLULUK

Bilgi Güvenliği Politikasının hazırlanması, gözden geçirilmesi ve güncellenmesinden BGYS Yöneticisi ve/veya BGYS Temsilcisi sorumludur. TCDD Taşımacılık A.Ş. yönetimi Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar.

3. POLİTİKA DETAYI

3.1. TANIMLAR

3.1.1. Bilgi Güvenliği Yönetim Sistemi - BGYS

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

3.1.2. BGYS Yöneticisi

Bilgi Güvenliği Yönetim Sistemi'nin operasyonundan ve sürekli iyileştirilmesinden sorumludur. BGYS Yöneticisi, Sistem Yöneticisidir.

3.1.3. Bilgi Varlığı

TCDD Taşımacılık A.Ş.'nin sahip olduğu, işlerini aksatmadan yürütebilmesi için önemli olan varlıklardır.

Bu politikaya konu olan bilgi varlıkları şunlardır:

a. Kâğıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri
b. Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım
c. Bilginin transfer edilmesini sağlayan ağlar
d. Bölümler, birimler, ekipler ve çalışanlar
e. Tesisler ve Özel alanlar
f. Çözüm ortakları
g. Üçüncü taraflardan sağlanan servis, hizmet veya ürün

3.1.4. Bilgi Varlığının İş Sahibi

Bilgi varlıklarının üretimi, geliştirilmesi, bakımı, kullanımı ve güvenliğini kontrol etmek için onaylanmış yönetim sorumluluğu bulunan kişi veya varlıkları tanımlar. 'Sahip' terimi, gerçekten varlık üzerinde mülkiyet hakları olan kişi anlamına gelmez.

3.1.5. Bilgi Varlığının Teknik Sahibi

Bilgi varlıklarının kurum içinde kullanılması için gerekli olan teknik operasyonda sorumluluğu bulunan kişi veya ekipleri tanımlar.

3.2. POLİTİKA

Bilgi kaynakları, tesisler ve cihazlar gibi TCDD Taşımacılık A.Ş. açısından büyük önem taşıyan varlıklardır. Bilgi varlıklarını ve kaynaklarını kullanan veya bilgi sağlayan herhangi bir kişi, bilgi varlıklarını korumakla yükümlüdür.

Ortak bilgi varlıklarını kullanan tüm çalışanların, gereken duyarlılığı göstermesi ve diğer meslektaşlarını, kurum çalışanlarını ve kurumsal değerleri gözeterek hareket etmesi beklenir.

Kurumsal değerlerin gereği olarak gizliliğe önem verilir, her türlü kişisel bilgi en yüksek güvenlik standartlarına sahip sistemlerle korunur. Bilginin sahibi istemedikçe, yetki verilmedikçe veya yasal gereklilikler oluşmadıkça bilgi paylaşılmaz.

TCDD TAŞIMACILIK A.Ş. için tüm bu bilgi varlıkları ve kaynakları içerisinde en kritik olanı, özenle korunması, gizliliğinin sağlanması, ihtiyaç duyulduğu anda erişilmesi

gereken bilgi varlıkları, **demo sistemleri ve TCDD Taşımacılık A.Ş. yazılım kataloğunu içinde barındıran sunucu sistemi ve bu sistemi barındıran sistem odasıdır.**

Bilgi varlıkları ve kaynakları farklı konumlarda veya ortamlarda bulunabilir. Hangi konumda veya ortamda olursa olsun müşteri iletişim gereksinimleri ve kurumsal değerler bu varlıkların ve kaynakların kullanımını belirler.

Bilgi güvenliği, sadece bilginin gizliliğinin değil, bütünlüğünün ve kullanılabilirliğinin de sağlanması ile mümkündür. Bilginin gizlilik gerekliliği, sadece yetkilendirme dâhilinde gereken bilgi varlıklarına erişim verilmesi anlamına gelir. Bilginin bütünlüğü, tüm bilgi varlıklarının tamlığını ve doğruluğunu sağlamayı gerektirir. Bilginin kullanılabilirliği, bilgi varlıklarının ihtiyaç duyulduğu anda ulaşılabilir ve kullanılabilir olması anlamına gelir.

Bilginin kullanımı, yerleşimi ve korunması ile ilgili ihtiyaçların karmaşıklığı ve çokluğu, kapsamlı ve geniş bilgi güvenliği süreçlerinin ve politikalarının tanımlanmasını zorunlu kılmaktadır. Bu nedenle belirlenen süreçler doğrultusunda bilgi güvenliği riskleri, bilgi varlığından sorumlu olan kişiler tarafından değerlendirilir, risklerin önceliği belirlenir ve gereken önlemler alınır.

Sistem odası ve sunucuların güvenliğinin sağlanması öncelikli olarak ele alınır. Varlık envanterinin ve bu envanterin olası risklerinin önceden belirlenerek müşterilerin güven içinde ve kesintisiz hizmet almaları için çalışılır.

Karar ve eylemlerde, güvenilir nesnel bilgiler ile teknolojinin tüm olanaklarının kullanılmasına önem ve öncelik verilir. Hareketler sezgilere, duygulara ya da doğru görünene göre değil; bilimsel ve teknolojik gerçeklerin ortaya koyduğu objektif esaslara göre düzenlenir. Bunu sağlamak için bilgi dünyadaki en ileri kaynaklardan transfer edilir, benimsenir ve mesleki uygulamalar bu doğrultuda yapılır. Kaynaklar verimli kullanılarak teknolojiye yatırım yapılır, gelişim bu doğrultuda sürdürülür.

Bu nedenle bilgi güvenliği yönetim sisteminin planlama, uygulama, izleme ve iyileştirme adımları ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına ve bu standardı destekleyen standartlara uygun olarak yürütülür.

3.2.1. Bilgi Varlıklarının ve Kaynaklarının Kullanımı

TCDD Taşımacılık A.Ş.'de yürütülen yazılım ve danışmanlık hizmetlerinin doğası gereği, bilginin gizliliğinin korunması öte yandan bilginin ve fikirlerin paylaşılması ve yaygınlaştırılması gerekir. Bilginin hassasiyeti ve güvenliği ile ilgili ihtiyaçlar

gözetilirken, aynı zamanda bilgiye ihtiyaç anında hızla ulaşılması büyük önem taşımaktadır. O nedenle, bilgi kaynaklarının değerinin iyi tespit edilmesi, bilginin korunmasını sağlayacak çaba ve maliyetin bilginin hassasiyeti ile orantılı olması gerekir.

TCDD Taşımacılık A.Ş. bilgi kaynaklarını kullanarak etik dışı veya yasalara karşı faaliyetlerde bulunmak, hiç kimse için kabul edilemez.

Bu politikanın asgari gereği olarak,

- Verinin kasıtlı olarak değiştirilmesi;
- Kasıtlı olarak veride hataların oluşmasına veya veri kaybına neden olunması;
- Bilgi kaynaklarının yasaları ihlal eden bir faaliyet için kullanılması;
- Bilgi güvenliğinin ihlal edilmesi veya suiistimal edilmesi;
- Cihazların, yazılımların veya herhangi diğer bir bilgi kaynağının çalınması, tahrip edilmesi;
- Bilgi kaynaklarının bilişim sistemlerinin performans kaybına sebep olacak şekilde kullanılması;
- Tesislerin, fiziksel cihazların, ağların tahrip edilmesi kabul edilemez.

Bu ve benzeri faaliyetler ve teşebbüsler disiplin suçu olarak ele alınır, gereken disiplin süreçleri ve yasal süreçler Üst Yönetim tarafından uygulanır.

Belirtilen tarzda bilgi güvenliği ihlallerinin, ihlal teşebbüslerinin veya bu tür ihlaller ile sonuçlanabilecek zafiyetlerin, tespit edildiği anda zaman kaybetmeden Bilgi Güvenliği Yöneticisi ve/veya Bilgi Güvenliği Yönetici Yardımcısı'na bildirilmesi gerekir.

3.2.2. Rol ve Sorumluluklar

Bilgi varlıklarının teknik sahipleri bilginin gizlilik bütünlük ve kullanılabilirliğini sağlamak için;

- Bilgi varlıklarına yetkisiz olarak erişilmesini; bilgi varlıklarının yetkisiz olarak değiştirilmesini veya tahribatını önlemek suretiyle, bilgi varlıklarını korurlar.
- Operasyonun mümkün olan en kısa hizmet kesintisi ile devam etmesini sağlamak için gerekli süreçlerin tanımlanmasını ve uygulanmasını sağlarlar.
- Bilgi güvenliği gerekliliklerini gözetirken, ihtiyaç duyulduğunda bilgiye hızla erişilebilmesi için karmaşıklığı ortadan kaldıracak dengeyi kurarlar.

- Çalışanlarını ve birlikte çalıştıkları üçüncü taraf çalışanlarını bilgi güvenliği gereklilikleri, rolleri ve sorumlulukları konusunda bilgilendirirler ve bilinçlendirirler.

Bütün bu faaliyetlerin kurumsal ISO/IEC 27001 standardı ile uyumlu bir çerçevede ele alınması için, tüm kuruluşun süreç ve hizmetlerini kapsayan bir BGYS kurulmuş ve BT Birim Yöneticisi, "BGYS Ekip Lideri" olarak atanmıştır.

3.2.3. BGYS Ekibi

BGYS Ekibi aşağıdaki kişilerden oluşur:

- Bilgi Teknolojileri Dairesi Başkanlığı
- Personel ve Eğitim Dairesi Başkanlığı
- Satın Alma Dairesi Başkanlığı
- Mali İşler Dairesi Başkanlığı
- Yolcu Dairesi Başkanlığı
- Hukuk Müşavirliği
- Kurumsal Emniyet Yönetim Dairesi Başkanlığı
- İdari ve Sosyal İşler Dairesi Başkanlığı
- Araç Bakım Dairesi Başkanlığı

BGYS Ekibi, yılda bir kere, YGG toplantılarından 2-4 hafta önce gerçekleştirilir BGYS Ekip Lideri' nin oluşturduğu gündem çerçevesinde toplanır. Toplantılarda görüşülen konular aşağıda belirtilen maddeleri içerir, ancak bunlarla sınırlı kalmayabilir:

- Bilgi Güvenliği Politikasının gözden geçirilmesi
- Risk Yönetim Metodolojisinin onaylanması
- Güncel risk raporunun değerlendirilmesi
- Kabul edilebilir risk seviyesinin üst yönetim tarafından onaylanması
- Artık risklerin üst yönetim tarafından onaylanması

- Risk işleme planının üst yönetim tarafından onaylanması
- Güvenlik ihlal olaylarının değerlendirilmesi
- İş süreklilik stratejisinin gözden geçirilmesi
- İş sürekliliği tatbikat sonuçlarının değerlendirilmesi
- Bilgi güvenliği bilinçlendirme çalışmalarının gözden geçirilmesi
- İç denetim raporlarının değerlendirilmesi
- Kurumu etkileyebilecek önemli değişiklikler.
- Varlık Envanteri, varlık sahiplik ve kullanıcı erişim hakları.
- Sistem loglarının incelenmesi.
- Yedekli yazılım ve teçhizatların gözden geçirilmesi.
- Gizlilik ya da ifşa etmeme anlaşmalarının gözden geçirilmesi.

3.2.4. Yasal Şartlara Uyumluluk

TCDD Taşımacılık A.Ş. Türkiye Cumhuriyeti kanunlarına ve tüm uluslararası kanunlara uymayı kabul ve taahhüt eder. Bilginin saklanması, kullanılması ve ifşasında TCK 5846 (Fikir ve Sanat Eserleri Kanunu), TCK 5651 (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu), TCK 5237 (Kişi Hak ve Özgürlüklerini, Kamu Düzen ve Güvenliğini, Hukuk Devletini, Kamu Sağlığını ve Çevreyi, Toplum Barışını Korumak, Suç İşlenmesini Önleme Kanunu), TCK 5070 (Elektronik İmza Kanunu), TCK 5809 (Elektronik Haberleşme Kanunu), İş Kanunu olmak üzere tüm kanunlara uygun hareket eder. TCDD TAŞIMACILIK A.Ş. yönetimi, bu kanun ve yönetmeliklerine aykırı bir davranışta bulunan çalışanı veya tedarikçisi ile ilgili gerekli suç duyurusunda bulunmakla sorumludur.

5651 sayılı Internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun ile içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden

mücadeleye ilişkin esas ve usulleri düzenlenmiştir. Bu kapsamda 5651 sayılı kanun hem içerik, yer, erişim ve toplu kullanım sağlayıcıları ile ilgili düzenlemeleri hem de Internet ortamında işlenen suçlar ile ilgili cezai hükümleri ortaya koyan bir kanundur. Kanunla verilen görevler Bilgi Teknolojileri ve İletişim Kurumu bünyesinde bulunan Telekomünikasyon İletişim Başkanlığı'nca yerine getirilmektedir.

5070 sayılı elektronik imza kanunu ile birlikte güvenli elektronik imza, elle atılan ıslak imzaya eşdeğer kabul edilmiş ve aynı hukuki sonuçları doğuracağı belirtilmiştir. Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmelerinin güvenli elektronik imza ile gerçekleştirilemeyeceği kanunda ifade edilmiştir. (Örn: emlak alım satımı, veraset ve intikal, evlenme gibi işlemler) Elektronik sertifika hizmet sağlayıcıları, elektronik imzalarla ilgili hizmetleri sağlarlar. Elektronik sertifika hizmet sağlayıcılarının elektronik imza kanununun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Bilgi Teknolojileri ve İletişim Kurumu tarafında yerine getirilmektedir.

5809 sayılı elektronik haberleşme kanunu elektronik haberleşme sektöründe düzenleme ve denetleme getiren bir kanundur. Bu düzenleme ve denetleme unsurları içerisinde bilgi güvenliği ile ilgili hususlar da yer almaktadır. Örneğin, kanunun dört numaralı maddesinde ilgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde "bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi" ilkesinin göz önüne alınması gerektiği ifade edilmektedir. Kanunla verilen düzenleme ve denetleme görevleri Bilgi Teknolojileri ve İletişim Kurumu tarafından yerine getirilmektedir.

Bu politika TCDD Taşımacılık A.Ş. Yönetimi tarafından gözden geçirilmiş ve onaylanmıştır.

TCDD Taşımacılık A.Ş. uyulması zorunlu tüm yasal şartlar Dış Kaynaklı Doküman Listesinde tanımlanmıştır.

4. POLİTİKA LİSTESİ

- ✓ P01 BİLGİ SİSTEMLERİ GENEL KULLANIM POLİTİKASI
- ✓ P02 PERSONEL GÜVENLİĞİ POLİTİKASI

- ✓ P03 İNTERNET ERİŞİM POLİTİKASI
- ✓ P04 E-POSTA POLİTİKASI
- ✓ P05 ANTİ-VİRÜS POLİTİKASI
- ✓ P06 ŞİFRE POLİTİKASI
- ✓ P07 KABLOSUZ İLETİŞİM POLİTİKASI
- ✓ P08 UZAKTAN ERİŞİM POLİTİKASI
- ✓ P09 KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI
- ✓ P10 FİZİKSEL GÜVENLİK POLİTİKASI
- ✓ P11 SUNUCU GÜVENLİK POLİTİKASI
- ✓ P12 AĞ CİHAZLARI GÜVENLİK POLİTİKASI
- ✓ P13 AĞ YÖNETİMİ POLİTİKASI
- ✓ P14 RİSK DEĞERLENDİRME POLİTİKASI
- ✓ P15 DONANIM VE YAZILIM ENVANTERİ OLUŞTURMA POLİTİKASI
- ✓ P16 VERİTABANI GÜVENLİK POLİTİKASI
- ✓ P17 DEĞİŞİM YÖNETİMİ POLİTİKASI
- ✓ P18 GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI
- ✓ P19 SANAL ÖZEL AĞ (VPN) POLİTİKASI
- ✓ P20 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI
- ✓ P21 BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI
- ✓ P22 BAKIM POLİTİKASI
- ✓ P23 BİRLİKLER İÇİN UZAKTAN ERİŞİM POLİTİKASI
- ✓ P24 YAZILIM GELİŞTİRME
- ✓ P25 PERSONEL VE EĞİTİM
- ✓ P26 BELGELENDİRME
- ✓ P27 KABUL EDİLEBİLİR KULLANIM POLİTİKASI
- ✓ P28 ORTAMIN ELDEN ÇIKARILMASI POLİTİKASI
- ✓ P29 TEÇHİZATIN ELDEN ÇIKARILMASI POLİTİKASI
- ✓ P30 TEMİZ MASA TEMİZ EKRAN POLİTİKASI
- ✓ P31 KRİPTOGRAFİK KONTROLLER POLİTİKASI
- ✓ P32 ZİYARETÇİ KABUL POLİTİKASI
- ✓ P33 TAŞINABİLİR MOBİL CİHAZ POLİTİKASI
- ✓ P34 SİBER SALDIRI POLİTİKASI
- ✓ P35 BİLGİ VE YAZILIM ALIŞVERİŞİ POLİTİKASI
- ✓ P36 ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI
- ✓ P37 VARLIKLARA YÖNELİK SORUMLULUK POLİTİKASI
- ✓ P38 BASILI ÇIKTI VE DAĞITIM POLİTİKASI
- ✓ P39 BİLGİ SINIFLANDIRMA VE ETİKETLEME POLİTİKASI
- ✓ P40 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI
- ✓ P41 GÜVENLİ YAZILIM GELİŞTİRME POLİTİKASI