1. AMAÇ

Ant Teknik Bilgi Güvenliği Prosedürleri ‘ne uymak amacıyla bilgi sistemlerini kullanan çalışanların topluluğun bilgilerinin gizliliğini korumak, doğruluğunu güvence altına almak ve bilgilere ihtiyaç duyulduğunda yetki sahibi çalışanların erişimini sağlamak amacıyla uyması gereken kuralları ve süreçleri tanımlamaktadır.

2. KAPSAM

Bu politika Ant Teknik Cihazlar Pazarlama ve Dış Ticaret A.Ş. bilgi güvenliğinin temel gereksinim ve uygulamalarını kapsamaktadır ve uyumdan tüm çalışanlar sorumludur. Ant Teknik BGYS’ nin kapsamı şirketin tüm birimleri, süreçleri ve lokasyonlarıdır.

3. SORUMLULAR

Tüm Ant Teknik çalışanları dijital, kâğıt veya sözel her türlü bilginin bu dokümanda tanımlanan değerlendirmeye uygun olarak korunmasından sorumludurlar.

BGYS ne uyum için gerekli aksiyonların alınmasından ve koordinasyonundan Ant Teknik üst yönetimi adına DPO sorumludur. Ant Teknik üst yönetimi uyum için destek verir ve gerekli kaynakları sağlar.

4. İLGİLİ DOKÜMAN VE EKLER

Ant Teknik KVKK Dokümanları

5. YÜRÜRLÜLÜK VE DEĞİŞİKLİK

Bu prosedür 10.01.2022 tarihi itibariyle yürürlüğe girmiştir.

6. GİRİŞ

Bu politika, Ant Teknik BGYS süreçlerin temel prensiplerini içermektedir.

GÜVENLİK POLİTİKASI

7. Güvenlik Politikası

7.1. Bilgi Güvenliği Politikası

Bu politikanın amacı bilgi güvenliği için, iş gereksinimleri, ilgili yasa ve düzenlemelere göre çalışanların bilgilendirilmesidir.

7.2. Gizlilik Anlaşmaları

Ant Teknik çalışanları ve 3. taraf çalışanlar ile gizlilik anlaşmaları yapılmalıdır.

7.2.1. Otoriteler ile İletişim

Ant Teknik ve Grup Şirketleri, gerekli durumlarda ilgili kuruluşlar ile iletişime geçer Bu kurumlar bilgi güvenliği hizmeti temin edilen kuruluşlar, yazılım ve donanım sağlayıcıları ve KVKK Kuruludur.

7.2.2. Müşterilerle Çalışırken Güvenliği İfade Etme

Müşteriler ile çalışmaya başlamadan önce gerekli güvenlik tedbirleri alınmalıdır.

7.2.3. Üçüncü Taraf Anlaşmalarında Güvenliği İfade Etme

Üçüncü taraflar ile çalışmadan önce gerekli güvenlik önlemleri alınmalıdır ve üçüncü taraflar ile gizlilik sözleşmeleri imzalanmalıdır.

Not: Eğer firmaların gizlilik sözleşmeleri var ise kullanmalarında herhangi bir sakınca yoktur.

7.3. Bilgi Güvenliği Yönetim Sistemi (BGYS) İzleme ve İnceleme

7.3.1. İzleme: Bilgi güvenliği olayları, tehditler ve zayıf noktalar düzenli olarak izlenir ve kayıt altına alınır. Bilgi güvenliği kontrollerinin etkinliği sürekli izlenir ve gözden geçirilir.

7.3.2. İnceleme: BGYS yıllık olarak gözden geçirilir ve gerekli durumlarda güncellenir. Bu inceleme, bilgi güvenliği olayları ve denetim sonuçlarına dayanarak gerçekleştirilir.

VARLIK YÖNETİMİ

8. Varlık Yönetimi

8.1. Varlıkların Sorumluluğu

Bu bölümün amacı Ant Teknik bilgi varlıklarının uygun bir biçimde nasıl sınıflandırılacağını ve korunacağını tanımlamaktır.

8.2. Ekipmanlara ve Verilere Erişim

Bu başlık; Ant Teknik'te çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların bilgi güvenliğine ilişkin tehditler ve kaygıların ve kendi sorumluluklarının farkında olmalarını ve normal çalışmaları sırasında kurumsal güvenlik politikasını desteklemek ve insan hatası riskini azaltmak üzere donatılmasını sağlamaları bu prosedür kapsamında ele alınır.

Çalışanlar, şirketlerimizin her türlü strateji, yatırım projeleri ile ilgili bilgileri, mali verileri, şirkete özel bilgi içeren proses ve ürünlerle ilgili endüstriyel veriler, çalışanlarla ilgili veriler, müşteriler ve rekabet ile ilgili bilgiler vb. verileri en öncelikli korur ve şirket dışına çıkartmazlar.

Bilgi güvenliği ve / veya 5651 numaralı yasa gereği tüm internet girişleri, USB benzeri cihazlara veri transferleri, dropbox benzeri bulut uygulamaları veri aktarımları ve kişisel e-posta adresleri dahil dışarıya atılan tüm e-postaların gerektiğinde kontrol edilmek üzere kayıtları tutulur.

İş için kritik tüm verilerinizi, kişisel bilgisayarlarda tutulmayıp, file server ya da kurumsal portal MS SharePoint veya MS One Drive'da yedeklenmesi gereklidir.

İş için ya da kişisel bilgilerinizin güvenliği için kritik dosyalarınızı şifreli kaydetmeniz ya da kriptolu saklamanız gereklidir.

Bilgi güvenliği açısından önemli olan basılı belgeleri ilgisiz / yetkisiz kişilerin erişemeyeceği şekilde saklamak, çalışma sonrası bu tür bilgileri ortada bırakmayarak temiz masa uygulaması çalışanların kişisel sorumluluğudur.

Çalışanların hangi verilere ve sistemlere erişim sağlayacağı ilgili bölüm müdürleri tarafından belirlenir ve bilgi sistemlerine iletilir.

Şirketin kritik verileri arşivde saklanır ve buraya sadece üst yönetim ve yetkili mali işler çalışanları erişim sağlayabilir.

Dijital verilerin saklandığı fiziksel ortamlara ise idari işler ve bilgi sistemleri sorumluları erişim sağlayabilirler.

8.2.1. Bilgi Güvenliği Eğitim ve Farkındalık

- Ant Teknik ve Grup Şirketleri düzenli olarak çalışanları için bilinçlendirme programları düzenler. Bu programlar Bilgi Güvenliği konusunda çalışanlar arasında farkındalık yaratmak için tasarlanır.
- Tüm personelin yılda en az bir kez bu programa katılımı esastır. Bununla birlikte Ant Teknik bilgi güvenliği politika ve prosedürlerinde önemli derecede bir değişiklik olmamışsa ve eğitim içeriği değişmemişse Ant Teknik yönetimi kararı ile katılımcıların her sene aynı içeriği alması zorunlu tutulmayabilir.
- İnsan Kaynakları departmanı tarafından Farkındalık kapsamında, e-posta ya da portal aracılığı ile tüm personele güncel bilgi güvenliği tehditleri hakkında ya da katılımcıların bilgilerini tazelemek adına belirli dönemlerde (yılda en az bir kez olmak üzere) bilgilendirme mesajları iletilir.
- Ant Teknik Bilgi Güvenliği Yönetim Sistemi politikası ve eğitimlerine https://antteknik.info adresinden tüm çalışanlar ulaşmakla yükümlüdürler. Bu iletişim platformunun yönetiminden ve güncellenmesinden DPO sorumludur.

8.2.2. Disiplin Prosesi

Ant Teknik ve Grup Şirketleri çalışanlarının bilgi güvenliği, etik ve KVKK gerekliliklerine uymaması konusunda insan kaynakları gerekli uyarıları yapar, düzeltici aksiyonları alır ve gerektiğinde disiplin sürecini uygular.

8.3. İstihdamın Sonlandırılması veya Değiştirilmesi

Çalışanın çıkış işlemlerinin ne şekilde yapılacağı İK departmanı tarafından tanımlanır ve uygulanır.

8.4. Varlıkların İadesi

İşten çıkarılan kişinin varlıkları İK departmanı tarafından ya da bilgi sistemleri tarafından iade alınır.

8.4.1. Erişim Haklarının Kaldırılması

Çıkartılan kişinin tüm mantıksal erişimleri BT bölümü tarafından ve fiziksel erişimleri fiziksel güvenlikten sorumlu bölüm tarafından iptal edilir.

Kullanıcının paylaşımlı hesapların şifrelerine erişimi var ise bu şifreler personelin ayrılmasından sonra değiştirilir.

Çalışanın işten ayrılmasında gerekli bildirimlerin yapılması İK departmanı sorumluluğundadır. Mantıksal erişim (sistem ve uygulamalara erişim) haklarının

kaldırılmasının sorumluluğu BT bölümünde, fiziksel erişim haklarının kaldırılmasının sorumluluğu ise İdari İşler bölümü ya da bu görevi yazılı olarak atandığı bir bölümdedir.

İşten ayrılmalarda ayrılma öğrenildiği an vakit kaybedilmeden İK bilgi sistemlerine bildirim yapar.

- Hemen ilişki kesilecekse kullanıcı derhal kapatılır.
- Bir süre verilmemişse kullanıcı DLP kapsamında izlemeye alınır.

8.5. Bilgi Varlıklarının Sınıflandırılması ve Etiketlenmesi

Sınıflandırma: Bilgi varlıkları gizlilik, bütünlük ve erişilebilirlik kriterlerine göre sınıflandırılır. Bu sınıflandırma, varlıkların korunması için gerekli kontrollerin belirlenmesine yardımcı olur.

Etiketleme: Bilgi varlıkları uygun şekilde etiketlenir ve bu etiketler doğrultusunda korunur.

8.6. Veri Yedekleme ve Geri Yükleme

8.6.1. Yedekleme: Kritik bilgiler düzenli olarak yedeklenir ve yedeklerin güvenliği sağlanır. Yedekler iş gereksinimlerine göre, bilgi sistemleri tarafından yerinde, saha dışı ve USB harici diskler üzerine ya da Office 365 bulut ortamına alınır.

Yedeklerin doğruluğu ve geri yükleme işlemlerinin etkinliği periyodik olarak test edilir.

8.6.2. Geri Yükleme: Yedeklemeler iş gereksinimlerine göre günlük ya da aylık yapılabilir. Mevcut yapıda bulut ve Nas yedekleme sistemi günlük olarak yapılmaktadır.

8.6.3. Felaketten Kurtarma: Ant Teknik olası felaket ve risklerden en az etkilenilmesi için kritik verilerini başta MS Office 365 olmak üzere bulut sistemlerde tutmaktadır. Buna ek olarak sistemlerde aksaklık yaşamak adına imaj ve dosya şeklinde yedekleme yapılması esastır. Sistemde olabilecek aksaklıklara karşı daha düşük kapasitelerde harici donanım yedeği bulundurulur ve yılda bir kez kritik sistemler harici donanıma restore edilerek test edilir.

DİJİTAL, FİZİKSEL VE ÇEVRESEL GÜVENLİK

9. Güvenlik

Şirketin kritik verileri arşivde saklanır ve buraya sadece üst yönetim ve yetkili mali işler çalışanları erişim sağlayabilir.

Dijital verilerin saklandığı fiziksel ortamlara ise idari işler ve bilgi sistemleri sorumluları erişim sağlayabilirler. Kritik bilgilerin saklandığı fiziksel ortamlar; arşivler server odaları vb.. ilgili yangın söndürme ve soğutma sistemlerine sahiptirler ver erişimler kontrol altındadır.

9.1. Güvenli Alanlar

9.1.1.Genel Kurallar

Bu prosedür Ant Teknik lokasyonlarının fiziksel ve çevresel güvenlik alanlarının belirlenmesini ve gerekli önlemlerin alınmasını tanımlar.

9.1.2. Teçhizatın Güvenli Olarak Elden Çıkarılması Tekrar Kullanımı

Saklama ortamları, kullanımına ihtiyaç olmadığında güvenli ve tehlikesiz şekilde imha edilir. Saklama ortamları yeterli özen gösterilmeden imha edildiğinde, hassas bilgi başka kişilerin eline geçebilir. Riski en aza indirmek amacıyla veri depolama ortamlarının güvenli imha edilir.

Aşağıdaki liste güvenli imhası gereken malzemeleri listelemektedir:

- Kâğıt dokümanlar
- Manyetik kasetler
- Program dökümü
- Sistem dokümantasyonu
- Optik depolama ortamları (tüm formlar ve yazılım dağıtıcı ortamlar da dahil)
- Ses veya diğer kayıtlar
- Çıktı raporları
- Çıkarılabilir disk ve kasetler
- Test verisi

Hassas malzemelerin imhasına yönelik denetim izi tutulur.

İmha için malzeme toplanması sırasında, gizli olarak nitelendirilmeyen bilginin miktarı artarak bir grup gizli bilgiden daha hassas ve daha kritik bir hale dönüşebilir. Bu yığın etkisine özel olarak dikkat edilmektedir.

9.2. Kötü Niyetli ve Mobil Koda Karşı Koruma

Bu prosedürün amacı Ant Teknik'te kullanılan tüm yazılım ve bilginin bütünlüğünü korumaktır.

Tüm bilgisayar, laptop ve mobil cihazlarda sadece yetkilendirilmiş yazılımların çalıştırılmasına müsaade edilir. Yetkilendirilmemiş yazılımların yüklenmesi engellenmelidir.

Ant Teknik bilgi sistemleri anti-virüs programları başta olmak üzere tüm cihazlarda güvenlik yazılımlarının kurulmasından ve güncel tutulmasından sorumludur. Kullanıcılar bu yazılımlarda meydana gelen sorun ve eksikliklerin zaman kaybetmeden bilgi sistemlerine bildirmekle yükümlüdürler.

Ant Teknik ayrıca DDoS atakları için aylık servis sağlayıcı raporu almakatadır.

Kullanılan yazılımların etkin yönetimi için güncellemeler ve yamaların yayınlanmasını müteakip üç ay içinde yüklenmesi ve gerekli güncellemelerin yapılması esastır. Bu güncellemelerin ve yama yönetiminin yapılmasından bilgi sistemleri ve DPO sorumludur.

9.3. Elektronik Mesajlaşma

Elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır. Bu mesajlarda başta hassas nitelikli kişisel bilgiler, müşterilerin ve tedarikçilerin ticari sırları ve sözleşmelerde ya da ek bilgilendirmelerle yaptıkları gizli bilgiler olmak üzere bilgilerin korunması ve sadece gerekli personel ve kişilerle paylaşılması esastır.

Bunun dışında yukarıda belirtilen kapsamdaki bilgilerin şifrelenerek gönderilmesi ve şifrelerin de ayrı bir iletişim kanalı ile iletilmesi (SMS, WhatsApp) mesajların gizliliğinin korunması açısından önemlidir.

9.4. Firewall : Ant Teknik, (BGYS) bir parçası olarak firewall yönetimi süreçlerini dikkatle yönetir. Firewall, ağı dış tehditlere karşı koruyan kritik bir savunma hattıdır. Bu bağlamda, firewall kuralları ve yazılımları düzenli olarak gözden geçirilir ve güncellenir. İzin verilen ve reddedilen trafik politikaları, iş gereksinimleri ve güvenlik tehditlerine karşı duyarlılıkla belirlenir. Herhangi bir güvenlik ihlali veya anomali tespit edildiğinde, olayın kapsamı değerlendirilir ve gerekli düzeltici önlemler derhal uygulanır. Ayrıca, firewall yapılandırmaları ve güncellemeleri kayıt altına alınarak, yetkisiz erişimlere karşı gerekli denetimler sağlanır. Bu süreçlerin etkin bir şekilde yönetilmesi, firma bilgilerimizin gizliliği, bütünlüğü ve erişilebilirliğini korumak için hayati öneme sahiptir.

9.5. Mobil Cihaz ve Uzaktan Erişim Güvenliği

9.5.1.Mobil Cihazlar: Mobil cihazlarda kurumsal bilgiler korunur ve cihazların güvenliği sağlanır. Kayıp veya çalıntı durumunda cihazların uzaktan silinebilmesi sağlanır.

9.5.2.Uzaktan Erişim: Uzaktan erişim için VPN kullanımı zorunludur ve erişim şifreleme ile korunur. Uzaktan çalışanlar için bilgi güvenliği eğitimleri düzenlenir.

ERİŞİM KONTROLÜ

10. Erişim Kontrolü

10.1. Erişim Kontrolü İçin İş Gereksinimi

Bu prosedürün amacı Ant Teknik'te bilgiye erişimin kontrolün nasıl yapıldığını açıklamaktır.

Kullanıcı Erişim Haklarının Gözden Geçirilmesi

- Bölüm yöneticisi erişim yetkilerini kendi bölümü için yılda en az bir defa gözden geçirir.
- BT Sorumluları çeşitli bilişim sistemlerdeki kullanıcıları, erişim yetkileriyle birlikte her sene gözden geçirir.
- BT Sorumluları, geçerlilik tarihinden sonra erişim yetkilerinin kaldırıldığını kontrol eder.
- BT Sorumluları, ayrıca onay olmadan erişim hakkı verilip verilmediğini kontrol eder.

10.2. Kullanıcı Sorumlulukları

Ant Teknik'te yetkisiz kullanıcı erişimini, bilgi ve bilgi işleme olanaklarının tehlikeye atılmasını ya da çalınmasını önlemek, başta bilgi sistemleri olmak üzere tüm çalışanların görevidir.

Çalışanlar, https://antteknik.info adresindeki politikaları ve prosedürleri öğrenmek ve uygulamak ve varsa ek gereksinimleri ve süreçlerindeki değişiklikleri DPO ya ve bilgi sistemlerine bildirmekle yükümlüdürler.

10.2.1. Temiz Masa ve Temiz Ekran Politikası

Ant Teknik çalışanları çalışma ortamlarında en az düzeyde kağıt evrak ve bilgi varlığı tutarlar. Benzer şekilde çalışanların masaüstü bilgisayarlarında en az düzeyde bilgi tutmaları ve şirket bilgilerini ortak klasörlerde ya da kurumsal portalde saklamaları esastır.

10.2.2.Oturum Zaman Aşımı

Kullanıcı bilgisayarları işlem yapmadıkları takdirde kilitlenecek şekilde ayarlanmalıdır.

10.2.3.Bağlantı Süresinin Sınırlandırılması

Yüksek önemliliğe sahip uygulamaların bağlantı zaman açıkları sınırlandırılır.

10.3. Uygulama ve Bilgi Erişim Kontrolü

Uygulama sistemlerinde tutulan bilgiye yetkisiz erişim önlenmelidir.

10.3.1. Bilgi Erişim Kısıtlaması

Erişim kontrolü politikası uyarınca kullanıcılar ve destek personeli için bilgi sistemleri fonksiyonlarına ve bilgilerine erişim kısıtlanmıştır. Kullanıcıların bilgiyi yazma, okuma, silme veya çalıştırma hakları düzenlenmelidir.

10.3.2. Hassas Sistem Yalıtımı

Kullanıcılar kendisine ait bilgisayarda çalıştırılması, ayrı ağ bölmesine yerleştirilmesi, ağ kaynaklarının ayrılması, sadece gerekli uygulamalar ile iletişim kurulması vb. izolasyon veya işlevsel olarak gerçekleştirilmelidir.

10.4. Şifre Politikası

10.4.1.Şifre Güvenliği: Şifreler güçlü ve karmaşık olmalıdır. Şifrelerin periyodik olarak değiştirilmesi sağlanır ve şifrelerin paylaşımı yasaktır.

10.4.2.İki Faktörlü Kimlik Doğrulama: Kritik sistemlere erişimlerde iki faktörlü kimlik doğrulama (2FA) kullanılır.

BİLGİ SİSTEMLERİ EDİNİM, GELİŞTİRME VE BAKIMI

11. Bilgi Sistemleri Edinim Geliştirme ve Bakımı

Ant Teknik iletişim ve kurumsal saklama alanı olarak MS Office 365 teknolojilerini kullanmaktadır.

Yeni teknolojilerin kullanıma alınması üst yönetim ve bilgi sistemlerinin sorumluluğundadır. Gerektiğinde güvenlik gereksinimleri için DPO dan görüş alınır.

11.1. Değişiklik Yönetimi

11.1.1.Değişiklik Talebi: Bilgi sistemlerinde yapılacak her türlü değişiklik yazılı olarak talep edilir ve onaylanır.

11.1.2. Değişiklik İzleme: Yapılan değişikliklerin etkisi izlenir ve değişiklik sonrası sistemlerin düzgün çalıştığından emin olunur.

BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

12. Bilgi Güvenliği İhlal Olayı Yönetimi

Bilgi olayı yönetimi prosedürünün amacı, Ant Teknik bünyesinde meydana gelecek bir olaydan sonra BT operasyonlarını normal seyrine mümkün olan en kısa ve en efektif şekilde dönmesini sağlanmaktır.

12.1. Tanımlar

Bilgi Güvenliği / Operasyonel Olayları

Aşağıdaki Bilgi Güvenliği Olayları ya da Operasyonel Olaylar olarak tanımlanır:

- BT kaynaklarının bir saldırıya uğraması veya bir tehdidin oluşması,
- BT kaynaklarına yetkisiz bir erişim / izleme ya da değişiklik olması,
- BT kaynaklarının organizasyon / kuruluş politikalarına, yasa ve yönetmeliklere uygunsuz kullanımından ötürü, BT kaynaklarının veya bilgilerinin gizlilik, bütünlük ve erişilebilirliğine zarar vermesi.

Bilgi Güvenliği Olayı Örnekleri:

- BT sistemlerinin veya altyapısının hizmet engelleme saldırılarına (denial of service (DOS)) uğraması ya da yetkisiz olarak devre dışı bırakılma,
- Başarılı ya da başarısız olarak sonuçlanan, içeriden ya da dışarıdan BT sistemlerine veya verilerine yetkisiz erişim girişimleri,
- Organizasyonun özel (gizli) verilerinin / belgelerinin kaybı,
- Sürekli olarak yanıltıcı uyarı mesajları (örn: sürekli hatalı virüs uyarı mesajları alan birinin gerçek virüs mesajlarını dikkate almaması.)

- Bölüm yöneticisinin bilgisi ya da onayı olmadan sistem donanımının, yazılım sürümünün ya da yazılımın değiştirilmesi,
- Zararlı yazılım saldırıları (virüs, trojan vb.)
- Sosyal mühendislik / gizli bilginin kişiler yanıltılarak ele geçirilmesi (örn: sistem güvenlik şifreleri vb.)

Operasyonel Olay Örnekleri:

- Firewall donanım hataları,
- Anti-virüs cihazlarının arızalanması,

Problem / Vaka:

Vaka; bir sistemde, ağda veya günlük operasyonlarda gözlenen veya gözlenebilen günlük olaylarda gözlemlenen ya da gözlemlenebilir durumdur.

Karşılaşılan vaka, eğer BT Sistemleri / altyapısı üzerinde olumsuz etkiye sahip ise ya da bir hadisenin otomatik olarak olumsuz bir etkiye sahip olduğu varsayılacak koşulları ifade eden, önceden kararlaştırılmış bir kriterden ötürü olumsuz olarak nitelendiriliyorsa “olay” (incident) olarak değerlendirilir.

Bir vaka, olay yönetiminden sorumlu ekibi (olay müdahale ekibi) tarafından analiz edildikten ve zararlı olarak değerlendirildikten sonra “olay” adını alır.

Bir vaka zararsız olarak sınıflandırılmadıkça “şüpheli olay” olarak isimlendirilir.

Ant Teknik’te bilgi güvenliği olayları DPO’ ya ilgili birim tarafından iletilir ve DPO tarafından dokümante edilir. Gerekli aksiyonların alınması için ilgili birim, İK, IT ve Üst Yönetim ile koordinasyon sağlanır. DPO gerektiğinde olayın tekrarlanma riskini yönetmek için konuyu risk yönetimi kapsamında değerlendirerek işbu prosedürün ilgili maddelerine uyum sağlayarak gerekli aksiyonları alır.

13. Risk Yönetimi

13.1. Risk yönetimi

Ant Teknik’in , iş sürekliliği hedefleri üzerinde herhangi bir olumsuz etkiden kaçınmak için potansiyel risklerin nasıl değerlendirildiğini ve azaltıldığını tanımlar.

Risk yönetimi bileşenlerini, kullanılan yaklaşımı ve araçları özetlemektedir. Bu temelde, bir olasılık/önem matrisi kullanılmakta, risklerin düzenli niteliksel değerlendirmesi yapılmaktadır.

Ant Teknik yönetimi ve DPO, bulunduğu hızlı değişen ortamın farkında olduğundan, riskler düzenli olarak izlenmekte, risk yönetim planları güncellenmekte ve gerekli aksiyonlar alınmaktadır.

13.2. Genel Prensipler

Ant Teknik, temelde birbiriyle ilişkili ve sürekli etkileşim halinde olan üç ana adımı içeren bir risk yönetimi çerçevesi kullanmaktır.

13.2.1 Risk Tanımı

Risk tanımlama, hedeflere ulaşılmasını etkileyebilecek riskleri tanımak, bulmak ve tanımlamak için kullanılan bir süreçtir. Risk tanımlamanın hedefi, riski etkileyebilecek olay ve koşullara ek olarak olası risk kaynaklarının farkında olmaktır. Olasılık, bir riskin gerçekleşmesinin göreceli olasılığını tanımlar ve çeşitli faktörlere bağlı olarak belirlenir.

Ant Teknik iş risklerinin değerlendirilmesi için aşağıdaki sınıflandırmalar tanımlanmıştır:

Olasılık;

- Yüksek: Her ay bir iki kez karşılaşılan ya da son 3 yıl içinde yılda ondan fazla karşılaşılmış olan riskler.
- Orta: Her yıl birkaç defa karşılaşılan ya da son 3 yıl içinde yılda 2-3 kez karşılaşılmış olan riskler.
- Düşük: Son 3 yıl içinde toplam 1-2 kez karşılaşılmış ya da daha az karşılaşılabilecek olan riskler.

Risklerin değerlendirilmesi sırasında yukarıda yapılan tanımlardan en uygun olan seçilir.

Etki, riskin gerçekleşmesi durumunda şirketin karşılaşabileceği sorunların önem derecesini ve sonuçlarını tanımlar:

- Yüksek: Risk, işin teknolojik ve finansal performansının yanı sıra işi büyük ölçüde etkileyebilir.
- Orta: Risk, işin teknolojik ve finansal performansını ve SLA'ları etkileyebilir.
- Düşük: Riskin, işin teknolojik ve finansal performansının yanı sıra SLA'lar üzerinde nispeten az etkisi vardır.

13.2.2 Risk Analizi ve İzleme

Risk analizi, tanımlanan risklerin doğasını, kaynaklarını ve nedenlerini anlamak ve risk düzeyini tahmin etmek için kullanılan bir süreçtir. Ayrıca, etkileri ve sonuçları incelemek ve mevcut kontrolleri değerlendirmek için de kullanılır. İzleme ise, denetlemek ve sürekli kontrol etmek anlamına gelir - mevcut durumu belirlemek için sürekli gözlem yapmayı içerir.

Risk yönetimi süreci, bir riskin meydana gelme olasılığı (orta/yüksek) ve iş üzerinde bir etkisi (orta/yüksek) olarak değerlendirildikten sonra başlar. Bu noktada, işletme sahibi, teknik lider ve koordinatör ile ilişki kurar ve şunları tanımlar:

- Karşı önlemlerin alınmasının gerekip gerekmediği.
- Riskle başa çıkmak için hangi proje seviyesinin uygun olduğu.

Prensip olarak, olasılık ve etki puanlarının çarpılmasıyla elde edilen risk yönetim puanı 3 ya da daha üzerinde ise bu riskin yönetimi için aksiyon alınması beklenmektedir. Bu kapsamda değerlendirilen riskler Yüksek, orta ve düşük için sırası ile 3,2,1 puan verilerek değerlendirilir. Planlar ve aksiyonlar yılda en az bir kere güncellenir.

13.2.3. Tedarikçiler: Ant Teknik tedarikçileri ve iş ortakları da BGYS ve risklerin yönetiminin ayrılmaz parçasıdır. Ant Teknik tedarikçileriyle ilgili, alınan ürünler ve hizmetleri kapsayacak şekilde riskleri belirler ve yönetir.

13.3 Risk Yönetimi ve Aksiyon Takibi

Ant Teknik iş risklerini aşağıdaki parametrelerle değerlendirir ve yılda bir kez günceller. Bu riskler iş risklerinin yanı sıra KVKK süreçleri için gerekli riskleri de içermektedir: Ant Teknik riskleri risk yönetim prosedürü ve ilgili tablo ile yönetir. (Ant_BGYS_07)

- Risk Tanımı
- Olasılık
- Etki
- Risk Puanı
- Aksiyon
- Sorumlu
- Statü
- Güncel Risk Puanı

14. Uyum

14.1. Yasal Gereksinimlere Uyum

Tüm Ant Teknik çalışanları, Türkiye Cumhuriyeti yasalarına, KVKK ve TCK'nın bilgi güvenliği ve kişisel verileri koruma kanunu ile ilgili maddelerine uymakla

yükümlüdürler. Ant Teknik bu konularda tedbirler alır ve eğitimler düzenler. Çalışanlar eğitimleri almakla ve kurallara uymakla yükümlüdürler.

14.2. Bilgi Varlıklarının Korunması

Ant Teknik çalışanları ve süreç sahipleri KVKK veri envanterindeki bilgiler başta olmak üzere müşterilerinin ürün bilgilerini, fiyat bilgilerini, tedarikçilerle ve müşterilerle yapılan sözleşmelerdeki ticari bilgileri ve bunlarla sınırlı olmamak kaydı ile müşterilerinin ve tedarikçilerinin halka açık olmayan ve Ant Teknik'te çalışmaları sebebiyle elde ettikleri bilgileri saklama yükümlülükleri vardır.

Ant Teknik çalışanlarına bu bilgileri saklamaları ve korumaları için en üst güvenlik tedbirlerine sahip ortamları sağlar.

14.3. Güvenlik Politikası ve Uyumun Bağımsız Kişiler Tarafından Gözden Geçirilmesi

Aşağıdaki politika ve prosedürlere uyum düzenli olarak gözden geçirilir:

- BGYS Politikası
- Varlık Envanteri
- Risk Yönetimi ve Aksiyon Takibi

Kullanılan sistemler, tanımlanan standartlarla uyumun kontrol edilmesi için BT personeli tarafından düzenli olarak izlenir. Her çeyrekte bir defa kullanıcıların yalnızca kendilerine verilen yetkiler ile işlem yaptığı kontrol edilir. Senede bir defa da o yetkinliğe sahip üçüncü parti tarafından teknik anlamda gözden geçirme yapılır.

HAZIRLAYAN	ONAY
DPO OĞUZ TÜRKKORKMAZ	**CEO**