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 prosedür Ant Teknik LTD. ŞTI. kapsamaktadır ve tüm çalışanlar sorumludur.

3. SORUMLULAR

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

4. İLGİLİ DOKÜMAN VE EKLER

Ant Teknik Bilgi Güvenliği Kalite El Kitabı

Ant Teknik KVKK Dokümanları

5. YÜRÜRLÜLÜK VE DEĞİŞİKLİK

Bu prosedür 10.01.2022 tarihi itibariyle yürürlüğe girmiştir.

HAZIRLAYAN	ONAY
DPO OĞUZ TÜRKKORKMAZ	**CEO**

6. GİRİŞ

Bu prosedür, Ant Teknik Bilgi Güvenliği Prosedürleri ve Bilgi Güvenliği Politikası içerisindeki süreçlerin detaylarını içermektedir. Bilgi güvenliği prosedürleri aşağıdaki bölümlerden oluşmaktadır:

- Güvenlik Politikası
- Bilgi Güvenliği Organizasyonu
- Varlıkların Yönetimi
- İnsan Kaynakları Güvenliği
- Fiziksel ve Çevresel Güvenlik
- Haberleşme ve İletişim Yönetimi
- Erişim Kontrolü
- Ağ Erişim Kontrolü
- İşletim Sistemi Erişim Kontrolü
- Sistem Planlama ve Sistem Kabulü
- Yedekleme ve Kurtarma
- Tedarikçi Yönetimi
- Bilişim Sistemleri Alımı, Geliştirme ve Bakımı
- Bilgi Güvenliği Olay Yönetimi
- İş Sürekliliği Yönetimi
- Uyum

GÜVENLİK POLİTİKASI

7. Güvenlik Politikası

7.1. Bilgi Güvenliği Politikası

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

7.1.1. Bilgi Güvenliği Politika Dokümanı

7.1.2. Gizlilik Anlaşmaları

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

(Bkz. GİZLİLİK SÖZLEŞMESİ)

7.1.3. Otoriteler ile İletişim

Ant Teknik ve Grup Şirketleri, gerekli durumlarda hangi kuruluşlar ile nasıl iletişime geçileceğinin tanımı yapılmalıdır.

(Bkz. ACİL DURUM PROSEDÜRÜ)

7.2.1. Müşterilerle İlgilenirken Güvenliği İfade Etme

Müşteriler ile çalışmaya başlamadan önce gerekli güvenlik tedbirleri alınmalıdır.

(Bkz. ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI)

7.2.2. Üçüncü Taraf Anlaşmalarında Güvenliği İfade Etme

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

(Bkz. GİZLİLİK SÖZLEŞMESİ)

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

VARLIK YÖNETİMİ

8. Varlık Yönetimi

8.1. Varlıkların Sorumluluğu

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

8.2. Çalışma Esnasında

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 portalimiz SharePoint veya 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.

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.
- Eğitimlerin değerlendirilmesine ilişkin esaslar Eğitim Prosedürü'nde belirlenmiştir.

8.2.2. Disiplin Prosesi

Ant Teknik ve Grup Şirketleri çalışanlarının prosedür, politika ve sözleşme gibi uygulamalara uymadığı takdirde karşılaşacakları yaptırımların tanımlandığı prosedürdür.

(Bkz. Ant Teknik Personel Yönetmeliği)

8.3. İstihdamın Sonlandırılması veya Değiştirilmesi

Çalışanın çıkış işlemlerinin ne şekilde yapılacağı İK departmanı tarafından hazırlanan "İşten Çıkış Prosedürü"nde tanımlanmıştır.

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.

FİZİKSEL VE ÇEVRESEL GÜVENLİK

9. Fiziksel ve Çevresel Güvenlik

9.1. Güvenli Alanlar

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

9.1.2. Teçhizatın Güvenli Olarak Elden Çıkarılması ya da 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. *(Bkz. KVKK İMHA VE ANONİMLEŞTİRME POLİTİKASI)*

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 edilmelidir. 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.

9.2.1. 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.

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 iki defa gözden geçirir.
- BT Sorumluları çeşitli bilişim sistemlerdeki kullanıcıları, erişim yetkileriyle birlikte her sene gözden geçirir.
- BT Sorumluları, bilişim sistemlerindeki kullanıcıların erişim yetkilerinin onaylarını ve dokümante edilen ile uygulamadaki yetkilerin aynı olduklarını kontrol eder.
- 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.

10.2.1. Temiz Masa ve Temiz Ekran Politikası

(Bkz. TEMİZ MASA TEMİZ EKRAN POLİTİKASI)

Oturum Zaman Aşımı

Kullanıcı bilgisayarları 20 dk. işlem yapmadıkları takdirde kilitlenecek şekilde ayarlanmıştır.

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.

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.

BİLGİ SİSTEMLERİ EDİNİM, GELİŞTİRME VE BAKIMI

11. Bilgi Sistemleri Edinim Geliştirme ve Bakımı

11.1. Sistem Test Verisinin Korunması

Bu prosedürün amacı Ant Teknik'te uygulama sistem yazılımı ve bilgisinin güvenliğini sağlamaktır.

11.1.1. Program kaynak koduna erişim kontrolü

11.1.2. Program kaynak koduna erişim kısıtlı olmalıdır.

BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

12. Bilgi Güvenliği İhlal Olayı Yönetimi

Bilgi olayı yönetimi prosedürünün amacı, topluluk 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.

UYUM

13. Uyum

13.1. 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.

13.2. 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.

13.3. Güvenlik Politikası ve Uyumun Bağımsız Kişiler Tarafından Gözden Geçirilmesi

Güvenlik politikalarına ve standartlarına uyum

Aşağıdaki politika ve prosedürlere uyum düzenli olarak gözden geçirilir:

- Varlık Yönetimi
- İnsan Kaynakları Güvenliği
- Fiziksel ve Çevresel Güvenlik
- Haberleşme ve İşletim Yönetimi
- Erişim Kontrolü
- Bilişim Sistemi Edinim, Geliştirme ve Bakımı
- Bilgi Güvenliği İhlal Olay Yönetimi
- İş Sürekliliği Yönetimi

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.