BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Bilgi Güvenliği ile ilgili sorumlulukları, tanımları, kural ve prensipleri belirlemek, kullanıcılara başvuru kaynağı olarak hizmet etmek.

2. KAPSAM

Bilgi Güvenliği Politikası; bilgi güvenliği konusunda genel güvenlik kavramlarının yanı sıra, kurum tarafından yürütülen işlerde bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması için uyulması gereken kuralları kapsar. Politika, kurumu riske atacak durumların öğrenilmesi ve benimsenmesi işlevini görür.

3. SORUMLULUKLAR

Onaylayan	: Perform Portföy Yönetimi A.Ş. Yönetim Kurulu
Kullanıcılar	: Perform Portföy Yönetimi A.Ş. personelleri

4. TANIMLAR

Ağ (Network)	: Kullanıcıların iletişim kurmasını ve kaynakları paylaşmasını sağlayan, birbirlerine iletişim kanalları ile bağlı bilgisayar ve cihazların tümüdür.
Bilgi İhracı	: Bilgi sistemlerinde kişiye amacına ulaşmak için sadece bilmeye ihtiyacı olan bilginin verilmesidir.
Bilgisayar Adı	: Bir ağda yer alan bilgisayarların kendine has adı (ismi) dır.
Bluetooth	: Kısa mesafe veri alışverişini sağlamak amacı ile kullanılan kablosuz ağ teknolojisidir.
BT	: Bilgi Teknolojileri
BT Ekipman	: BT tarafından yönetilen, tahsis edilen cihazlardır. (PC, Notebook, Network cihazları, projeksiyon, yazıcı v.b.)
Dahili e-posta Listeleri	: E-posta hesaplarının tutulduğu dizin, listeler.
Denetim İzleri	: Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayan kayıtların tamamıdır.
Depolama Cihazı	: Bilgiyi saklamaya yarayan sistemlerdir.
En Az Erişim Ayrıcalığı	: Kişiye iş yapmasına yetecek şekilde yetki verilmesi olarak tanımlanır.

PERFORM PORTFÖY

File Server : Ortak olarak kullanılması gereken dosya, klasörlerin tutulduğu bilgisayardır.

Güvenlik Duvarı (Firewall) : Network üzerinde yetkisiz erişimleri engelleyen, yetkilendirilmiş iletişim alanlarına izin veren araçtır.

Hata Ayıklama : Bir uygulama ya da donanım üzerindeki hataların azaltılması ve yine uygulama ya da donanım'ın beklendiği şekilde çalışmasını sağlamak için kullanılan süreçtir.

Injection : Kod enjeksiyonu, geçersiz verinin işlenmesi yolu ile bilgisayar hatasının istismar edilmesi işlemidir.

IP : Bir ağda internet protokolünü kullanan her bir cihaza iletişimde kullanmak üzere verilen numara etiketidir.

İ.K. : Perform Portföy Yönetimi A.Ş. İnsan Kaynaklarını ifade eder.

İşletim Sistemi : Bilgisayarın çalışmasını sağlayan ana yazılımdır. (Windows, Mac OS, Linux v.b.)

Kriptolama : Bir verinin gerekli araçlar veya anahtarlar olmadan okunamaz şekilde saklanmasını sağlayan, veriyi dönüştüren süreçtir.

Leased Line : İnternete açık olmayan, iki farklı lokasyon arasında özel iletişim ağı oluşturan bağlantıdır.

Network Time Protokol (NTP) : Ağ zaman protokolüdür, ağ bağlantısına bağlı tüm cihazların aynı saati göstermesini sağlayan zaman senkronizasyonudur.

Penetrasyon Testi : Ağın güvenliğinin test edilmesi amacı ile saldırı simüle edilmesi ve varsa açıkların tespit edilmesi amacıyla yapılan testtir. Zaafiyet testi olarak da ifade edilen bu test kurum içinden yapıldığında iç penetrasyon, dışından yapıldığında dış penatrasyon testi olarak ifade edilir.

Secure Ftp (SFTP) : Dosya kopyalama ve kopyalanan dosyanın yine aynı ortamdan alınabilmesini sağlayan bir dosya transfer protokolüdür.

Secure Hyper Text Transfer (https) : İletişim için kullanılan güvenli şifrelenmiş ağ protokolüdür.

Spam Mesaj : Genelde topluca gönderilen, pazarlama veya dolandırıcılık öğeleri içeren e-postalardır.

Taşınabilir Medya : Veri saklama için kullanılan, bilgisayara usb, bluetooth gibi bağlantı yöntemleri kullanılarak bağlanan cihazlardır.

Üçüncü Taraf : Üçüncü taraflar, resmi olarak Perform Portföy Yönetimi A.Ş. çalışanı olmayan ancak işlerini ifa etmesinde görev alan firmaları, kişileri ifade eder. Üçüncü taraflar 4 başlıkta ifade edilir.

1. Dış Kaynaklar : Kurum çalışanları dışında hizmet sözleşmesi imzalanan firmalarca her türlü faaliyetin yürütülmesidir.
2. İş Ortakları : İki ana başlıkta incelenir
    a. Teknolojik iş ortakları : Teknoloji anlamında Perform Portföy Yönetimi A.Ş. ile ortak çalışan, bakım, geliştirme v.b. çalışmaları gerçekleştiren kaynaklardır.
    b. İş birimi, iş ortakları : İş kapsamında ortak ürün çıkartılan, ortak pazarlama faaliyetleri yapılan kaynaklardır.
3. Destek Hizmeti Alınan Firmalar : Kurumun ana faaliyetlerinin uzantısı veya tamamlayıcısı niteliğinde olduğu değerlendirilen dış kaynak hizmeti alınan firmalardır.
4. Proje Geliştiren Firmalar : Perform Portföy Yönetimi A.Ş. adına kısa dönemli veya proje bazlı çalışan firmalardır.

Uzaktan Erişim : Fiziksel olarak farklı yerde olan bir cihaza bulunulan lokasyondaki bir cihazdan veri iletişim kanalları ile ulaşılmasıdır.

Üretim Ortamı : Ana faaliyete konu sunucuların, veri tabanlarının ve uygulamaların beraber çalıştıkları ortamdır.

Veri Yolu : Verinin farklı bilgisayar veya ağlara aktarıldığı iletişim ağıdır.

Zeroization : Verinin geri kurtarılamayacak, erişilemeyecek şekilde depolama aygıtlarının içeriğinin değiştirilmesi yoluyla elektronik olarak silinmesidir.

5. KURAL VE PRENSİPLER

5.1 SİSTEM ERİŞİM KONTROLÜ

Sistem erişimi kontrolü, çalışanların sistemler üzerine tanımlanması, kullanılacak şifrelerin özelliği, şifre kullanım prensipleri ve denetim izlerini kapsamaktadır.

5.1.1 Kullanıcı Tanımlanması

Her bilgisayar ve iletişim sistemine ait kullanıcı adı sadece bir kullanıcıyı tanımlar. Paylaşımlı yada grup kullanıcı adlarının kullanılması yasaktır. "administrator", "manager" v.b. genel kullanıcı adlarının günlük kullanımda kullanılmasına izin verilmemektedir.

Kullanıcı yetkileri, kullanıcının işini gerçekleştirebileceği en az düzeyde ve görevler ayrılığı ilkesi gözetilerek verilmelidir.

Kullanıcı Perform Portföy Yönetimi A.Ş.'den ayrıldığında kullanıcı adının tekrar kullanılmasına izin verilmez. İşten ayrılan çalışanların tüm uygulama ve sistemlerdeki kullanıcı hesapları ve erişim hakları aynı gün yada en geç 1 gün sonra kaldırılır. Uzun süreli izne ayrılan personellerin hesapları pasife çekilir. Ancak departman amirinin bilgisi ve izni halinde hesap açık bırakılır.

- Her çalışan kendisine verilen kullanıcı adı ve kimlik için sorumludur.
- Yeni kullanıcı adının tanımlanabilmesi için, işe giren personelin Perform Portföy Yönetimi A.Ş. Sistem yöneticisine İ.K. tarafından bildirilmesi gerekmektedir.
- Kullanıcıların kendi hesapları ile başkalarının işlem yapmasına izin vermesi ve başkalarının kullanıcılarının kullanılması yasaktır.
- Aksi durumlarda şirket İK politikaları gereği idari yaptırımlar uygular.
- Aksi belirtilmedikçe kullanıcı Yerel Yönetici (Local Admin) yetkisine sahip olamaz. Yerel yönetici yetkisi görevi açısından uygun görülen Bilgi Teknolojileri personelleri ile sınırlıdır. Bunun dışında bir yetki ihtiyacı olması durumunda Bilgi Güvenliği Sorumlusunun bilgisi ve onayı dahilinde kullanıcıya bu yetki verilebilir.

5.1.2 Oturum Açma Süresi

Tüm şifre ekranları kullanıcıya sadece kullanıcı adı ve şifresini sormalıdır. Tüm başarısız oturum açma denemeleri kayıt altına alınır.

Kullanıcılar bilgisayarlarını, iş istasyonlarını kilitlemeden veya çıkış yapmadan gözetimsiz bırakmamalıdır.

5.1.3 Şifre Yönetimi

Sistem yöneticisi tarafından ilk defa tanımlanan şifrenin kullanıcı tarafından ilk oturum açma denemesi sırasında değiştirilmesi esastır. Bu işlem yapılmadan sistem başka işlem yapılmasına izin vermez.

En fazla 5 adet başarısız deneme sonrasında kullanıcı yine sistem yöneticisi tarafından açılana kadar kilitlenir.

Şifre yönetimi kapsamında Perform Portföy Yönetimi A.Ş. çalışanları tarafından aşağıdaki konulara dikkat edilmesi gerekir.

- Şifrenin güçlü olması için en az 11 karakter kullanılır.
- Tahmini zor şifreler tercih edilmelidir. Şifrenin içerisinde aşağıdaki 4 karakter setinden en az 3'ünün bulunması gerekmektedir.
    - Büyük Harf (A-Z)
    - Küçük Harf (a-z)
    - Rakam (0-9)
    - Alfa nümerik olmayan karakterler (!@#$% v.b.)
- Şifrede Perform Portföy Yönetimi A.Ş. ismi, eş çocuk yada iş arkadaşlarının ismi geçmemesi tavsiye edilir.
- Hatırlanamayan / Kilitlenen şifreler için sistem yöneticisine bilgi verilmelidir.
- Şifreler her zaman gizli tutulur. BT personelleri dahil olmak üzere şifrelerin paylaşılmaması ve yazılı olarak saklanmaması gerekir.
- Açığa çıktığından şüphelenilen tüm şifreler değiştirilmelidir.
- Hiçbir durumda kullanıcı adı ve şifreler paylaşılmaz. Aksi durumda yapılan tüm işlemlerden aslen kullanıcının kendisi sorumludur.

5.1.4 Kullanıcı Ayrıcalığı Yönetimi

Kullanıcı ayrıcalığı kapsamında Perform Portföy Yönetimi A.Ş. tarafından aşağıdaki önlemler alınır.

- Tüm kullanıcıların, sistemlerin ve programların bilgisayar ve iletişim sistemleri ayrıcalıkları bilgi ihtiyacı çerçevesinde kısıtlanır.
- Çalışan, yüklenici ve danışman haricindeki kişilere kullanıcı adı verilmez.
- Kullanıcı ayrıcalıkları İç Kontrol Yöneticisi tarafından kontrol edilmek üzere kayıt altına alınır.
- Özel ayrıcalıkların kullanımı kısıtlanmalı ve sürekli olarak kontrol altında tutulmalı, izlenmelidir.

- Kullanıcıların kimlikleri kayıtların veya raporların ömrü boyunca izlenebilir olmalıdır.

Kullanıcı ayrıcalığı kapsamında Perform Portföy Yönetimi A.Ş. çalışanları tarafından aşağıdaki kural ve sınırlamalara uyulması gerekmektedir.

- Perform Portföy Yönetimi A.Ş. bilgi sistemleri sadece iş amaçlı kullanılmalıdır.
- Perform Portföy Yönetimi A.Ş. bilgi sistemlerini kullanan herhangi bir kullanıcının yetkisinin olmadığı diğer bilgi sistemlerine erişimi, bu sistemlerde değişiklik yapması, bir şekilde zarar vermesi veya sistemlerin işleyişini aksatması yasaktır.
- Perform Portföy Yönetimi A.Ş. 'den ayrılan kullanıcıların tüm ayrıcalıklı erişimleri BT politika ve prosedürleri çerçevesinde derhal sonlandırılır.
- İK çalışanların görevlerinde veya çalışma durumlarında önemli değişiklik olması durumunda sistem yöneticisini e-posta aracılığı ile bilgilendirir. İK nın talebine istinaden sistem yöneticisi BT prosedürlerine uygun olarak gerekli yetki ve erişim düzenlemelerini yapar. İK ve bilgilendirilmesi gereken yetkili grupları e-posta yolu ile bilgilendirir.
- İş akdi feshedilen çalışanlar işten el çektirilir, tüm Perform Portföy Yönetimi A.Ş. ekipmanı ve bilgisinin iadesi istenir. İK ayrılan çalışanın tüm erişim ayrıcalıklarının kaldırılmasının sağlanmasından sorumludur.
- Perform Portföy Yönetimi A.Ş. içerisinde geliştirilen, üretilen her tür bilgi, program, ürün v.b. Perform Portföy Yönetimi A.Ş.'ye aittir ve kullanıcılar ayrıldığında yine Perform Portföy Yönetimi A.Ş. 'de kalmalıdır. Ayrılan kullanıcının tüm sistem ayrıcalıkları ve bilgiye erişimi sistem yöneticisi tarafından derhal sonlandırılır. Ayrılan kişiye verilen bilgi varlığı geri alınır yada yok edilir.
- Müdür ve üzeri görev seviyesindeki çalışanlar, kendilerine bağlı çalışanların nakil, terfi ve ayrılmaları durumunda bilgi erişim yetkilerini izlemeli ve gözden geçirmelidir. Bilgi erişim yetkileri buna göre değiştirilmeli ya da iptal edilmelidir.
- Kullanıcılar Perform Portföy Yönetimi A.Ş. Güvenlik Prensipleri dökümanını işe giriş sırasında ve kullanıcı adı tanımlanmadan önce imzalamalıdır.

5.1.5 Ayrıcalık Sınırlamaları

Perform Portföy Yönetimi A.Ş.'nin bilgi sistemlerinin uygun şekilde çalışmasını olumsuz olarak etkileyennormal kullanımı dışındaki faaliyetlere izin verilmez.

Ayrıcalık sınırlamaları kapsamında Perform Portföy Yönetimi A.Ş. tarafından aşağıdaki önlemler alınır.

- Bir bilgisayar ve ağ erişim kontrol sistemi doğru şekilde çalışmıyorsa son kullanıcıların ayrıcalıkları kaldırılmalıdır.
- Sistemde yer alan zaafları test etmek için kullanılacak yazılımlar ve diğer araçlar bilgi sistemlerine zarar verebileceği için Perform Portföy Yönetimi A.Ş. onayıyla kullanılmalıdır.

- Kullanıcılar sistemde yer alabilecek zaaflardan yararlanarak yetkili olmadıkları bilgiye ulaşmamalıdır. Sistemde yer alan bu tür zaaflar konusunda Perform Portföy Yönetimi A.Ş. sistem yöneticisi bilgilendirilir. Sistem yöneticisi iletilen bildirime istinaden İç Kontrol / Teftiş yetkilisini bilgilendirir.
- Sistem yetkileri üretim ortamlarındaki veriyle doğrudan ilgisi olmayan (denetçi, bilgi güvenliği yöneticileri, güvenlik yöneticileri, uygulama geliştiriciler v.b.) kullanıcılara oparasyonel üretim verisini güncelleyemeyecek şekilde tanımlanır.

5.2 AĞ VE İLETİŞİM GÜVENLİĞİ

Ağların güvenliğini sağlamaya yönelik alınması gereken tedbirler aşağıda belirtilmektedir.

5.2.1 Genel Ağ Koruması

Güvenlik duvarı, IDS, IPS yönlendirici, switch gibi kritik sistemler Perform Portföy Yönetimi A.Ş. bünyesinde bulunur. Bu sistemlerin yönetilmesi, işletilmesi ve güvenliği Perform Portföy Yönetimi A.Ş. sorumluluğundadır.

Genel ağ koruması kapsamında kullanıcılar tarafından uyulması gereken kural ve sınırlamalara aşağıda yer verilmiştir.

- Gizli bilgi, güvenilir olmayan kurum dışı iletişim ağlarında uygulama seviyesinde olarak veya son kullanıcı tarafından kriptolu olarak iletilir. Son kullanıcılar kriptolama fonksiyonu için Perform Portföy Yönetimi A.Ş. yönetiminin onay verdiği ofis uygulaması özelliklerini kullanabilirler.
- Çok Gizli bilgi, yerel ağ boyunca ve kurum dışı iletişim ağlarında uygulamasal olarak veya son kullanıcı tarafından kriptolu olarak iletilir. Son kullanıcılar kriptolama fonksiyonu için Microsoft Office yazılım özelliklerini kullanabilirler.
- Hiçbir bilgisayar, iş istasyonu v.b. dahili ağlara bağlıyken aynı anda dışarıdaki bir ağa ADSL, çevirmeli modem, geniş bant hattı v.b. ile bağlanamaz. Takasbank, Borsa İstanbul, MKK gibi kurumlara iş amaçlı yapılan zorunlu bağlantılar bunun dışındadır.

5.2.2 Kablosuz Ağ Güvenliği

- Bağlanan cihazların antivirüs yazılımları Perform Portföy Yönetimi A.Ş. standartlarına uygun olmaktadır.
- Kablosuz ağa bağlıyken Bluetooth kapalı olmalıdır.
- Kablosuz ağa bağlıyken aynı anda başka bir ağa bağlanılması yasaktır.
- Sunucular kablosuz ağa dahil edilmemelidir.
- Erişim tanımı yapılmış kayıp/çalınmış bilgisayarlar en kısa sürede Perform Portföy Yönetimi A.Ş. sistem yöneticisine bildirilir. Bildirilen bilgisayarların erişim tanımları en kısa sürede iptal edilir.

5.2.3 Bluetooth Güvenliği

Perform Portföy Yönetimi A.Ş. tarafından sağlanan cihazlar bluetooth özelliği kapalı olarak teslim edilir. Bu cihazlarda bluetooth özelliği kullanılmamalıdır.

5.2.4 İnternet Güvenliği

Perform Portföy Yönetimi A.Ş. internet güvenliğini sağlamak için aşağıdaki tedbirleri alır.

- İnternet erişimi için kullanılan uygulama güvensiz sitelerde yer alan ActiveX ve Java script'lerini engelleyecek şekilde yapılandırılmalıdır.
- İnternet üzerinden iç servislere erişim, güvenli (SSL) oturum açma sürecinden geçer. Oturum açılmasından sonraki hareketleri aynı şekilde güvenli olmalıdır.

İnternet güvenliği konusunda kullanıcı (Perform Portföy personelleri ve dış hizmet unsurları) sorumlulukları aşağıdaki şekildedir.

- Uygulamalar, otomatik olarak arka planda çalışan internet teknolojileriyle güncellenmez. Kullanıcı tarafından onaylanması gerekir.
- İnternet üzerinden bilgisayara indirilen tüm dosyalar onaylanmış anti virüs programları tarafından taranır.
- Çalışanlar, hiçbir kodu veya yazılımı çalıştırmamalı, kurulum yapamamalıdır. Bu tür ihtiyacı olan çalışanlar Perform Portföy Yönetimi A.Ş. sistem yöneticisine talepte bulunur. Sistem yöneticisi onayına istinaden yazılım kurulumu yine sistem yöneticisi tarafından gerçekleştirilir.

5.2.5 Çevirmeli Ağ Bağlantısı Güvenliği

Kullanıcıların yerel ağa bağlı bilgisayarlara, iş istasyonlarına v.b. cihazlara dahili veya harici çevirmeli modem bağlaması yasaktır.

5.2.6 Uzaktan Erişim

Uzaktan erişim sadece iş amaçlı olarak kullanılabilir. Uzaktan erişim sağlayan cihazlar Perform Portföy Yönetimi A.Ş. ağının uzantısı olarak kabul edilir ve yerel ağda uygulanan tüm güvenlik politikaları bu cihazlar için de geçerlidir.

Personellere tebliğ edilmiştir.

5.2.7 Sanal Özel Ağ (VPN)

VPN kullanımına izin verilen çalışanlar aşağıdaki kural ve prensiplere uyar.

- Kullanıcılara en az yetki prensibine göre sadece gerekli olan kaynaklara / sunuculara ve gereken portlara erişim yetkisi verilir.

- Perform Portföy Yönetimi A.Ş. çalışanlarının kurum dışından sadece işyerindeki masa üstü bilgisayarlarına erişim yetkisi verilir. Kişisel bilgisayarlarından uzaktan erişim sağlayan çalışanlar kullandıkları bilgisayarın güncel bir virüs koruma programı ile korunmasını sağlamakla yükümlüdür.
- Kurum içinde iş tanımı itibari ile uzaktan erişim yapması gereken çalışanlar haricindeki çalışanlar uzaktan erişim ile başka bir bilgisayar veya sunucuya erişemez.
- VPN ile bir sunucuya erişenler, erişilen sunucu üzerinden uzaktan erişim kullanarak başka bir sunucuya erişemez.
- VPN ile Perform Portföy Yönetimi A.Ş. ağlarına bağlanan bilgisayarın bağlantı süresiince ağa bağlanmaya yetkisi olmayan kişiler tarafından kullanılmaması, erişime izin verilen kişinin sorumluluğundadır.

5.2.8 Kriptolama Kullanma

- Gizli veya Çok gizli olarak belirtilen Perform Portföy Yönetimi A.Ş. verisi iletişim ağı boyunca veya Perform Portföy Yönetimi A.Ş. ağları dışında bir ağa gönderilecekse bu bilgi şifrelenmiş olarak iletilmelidir.
- Çok gizli bilgiler CD, DVD, flash bellek, disket, harici hard disk gibi taşınabilir cihazlara kaydedilemez. Bu cihazlara atılan/atılacak tüm gizli veya çok gizli bilgi kriptolanmış olmalıdır.
- Microsoft Windows'un kriptolama özelliği kullanılarak dökümanlar kriptolanabilir.

5.2.9 Test Ortamları Güvenliği

Test ortamının güvenliğini sağlamak üzere Perform Portföy Yönetimi A.Ş. tarafından aşağıdaki durumlar sağlanır.

- Test ortamı ile üretim ortamları arasında bir güvenlik duvarı kuralı bulunmalıdır.
- Test ortamları üretim ortamı hizmeti veremez.
- Tüm kullanıcı şifreleri kurum bünyesinde kullanılan şifre politikaları ile aynı olmalıdır.
- Test ortamında kullanılan kullanıcı şifreleri üretim ortamı şifrelerinden farklı olmalıdır.
- Test ortamında üretim ortamına ait veriler kullanılması gerektiği durumlarda bu verilerin test ortamında maskelenmesi gerekmektedir.

5.3 VERİ GÜVENLİĞİ

Müşteri ve Perform Portföy Yönetimi A.Ş. yönetimine ait bilgilerin korunması, işlenmesi ve paylaşımı konusundaki prensipler aşağıda yer almaktadır.

5.3.1. Fikri Mülkiyet Haklarının Tahsisi

- Çalışanlar, danışmanlar ve yöneticiler tarafından Perform Portföy Yönetimi A.Ş. yararına yaratılan, sağlanan her tür program ve doküman, yazılı istisnalar haricinde Perform Portföy Yönetimi A.Ş.'nin malıdır.
- Perform Portföy Yönetimi A.Ş. bilgisayarlarında ve kendi ağ sistemlerinde saklanan dosyaların içeriğinin veya bu sistemler aracılığıyla iletilen tüm mesajların yasal sahibidir. Perform Portföy Yönetimi A.Ş. daha önceden haber vermeden bu bilgiye erişme hakkına sahiptir.
- Perform Portföy Yönetimi A.Ş. çalışanları, iş gereği ulaşmaları gereken Perform Portföy Yönetimi A.Ş.'ye ait patent, telif hakkı, buluş ve diğer fikri haklara erişim hakkına sahiptir.

5.3.2 Fikri Mülkiyet Haklarının Korunması

Perform Portföy Yönetimi A.Ş., kullanıcıların işlerini verimli ve etkin bir biçimde yapması için yeterli sayıda yazılım lisansı sağlamaktadır. İş aktiviteleri gereği ek lisans ihtiyacı doğması durumunda gerekli çalışmalar yapılır.

Kullanıcıların telif hakkı olan yazılımı yetkisiz olarak kopyalamaları yasaktır. Fikri mülkiyet haklarının korunması konusunda kullanıcıların uyması gereken kural ve sınırlamalar aşağıdadır.

- Kullanıcılar Perform Portföy Yönetimi A.Ş.'ye ait hiçbir yazılımı depolama cihazlarına kaydetmemeli, başka bilgisayarlara taşımamalıdır.
- Kullanıcılar sistem güvenliğini tehlikeye atacak veya test edilmekte olan yazılım araçlarını edinmemeli, kullanmamalı ve iletmemelidir.
- Yazılım lisans şartnamelerine sıkıca uyulmalıdır. Lisans şartnamesinde özellikle belirtilmediği sürece yazılım çoğaltılamaz, değiştirlemez veya birden çok bilgisayarda kullanılamaz.

5.3.3 İş Sürekliliği Acil ve Beklenmedik Durum Planı

- Perform Portföy Yönetimi A.Ş. acil ve beklenmedik durumlarda kritik görevleri etkin ve doğru şekilde yerine getirebilmek için yazılı, detaylı, kapsamlı ve uygun maliyetli bir plan hazırlar.
- Plan, acil ve beklenmedik durumlarda uyulması gereken dahili politikaları ve prosedürleri, kurtarma hazırlığını ve kısmi veya tam kurtarma başlatmak için gerekli olan asgari şartları kapsar.
- Plan, hayati öneme sahip işlemlerin ve kritik uygulamaların devamının sağlanması için gerekli tüm prosedürleri içerir. Acil ve beklenmedik durumlarda kritik uygulamalar önem sırasına göre sürdürülür. Uygulamalar ve hizmetler kritikliklerine göre İş Sürekliliği Komitesi tarafından onaylanmış önceliklere sahiptir. Bir acil ve beklenmedik durum anında bu önceliklere göre sistemler yeniden yüklenir.
- Kritik sistemleri belirlemek amacı ile iş etki analizi yapılır ve İş Sürekliliği Planına eklenir.

5.3.4 Yedekleme ve Kurtarma

Perform Portföy Yönetimi A.Ş. sisteminde bulunan kritik verilerin bulunduğu İnfleks sisteminin yedeklenmesi İnfina Yazılım A.Ş. ile yapılan sözleşme kapsamında İnfina Yazılım A.Ş. sorumluluğundadır.
Gerekli hallerde yedekten dönme testlerine Perform Portföy Yönetimi A.Ş. de dahil olur.
Yedekten dönme testlerine ait sonuçlar Perform Portföy Yönetimi A.Ş.'ye sunulur.

Tüm kurum çalışanları aşağıdaki konulara özen göstermelidir.

- Perform Portföy Yönetimi A.Ş.'ye ait veriler şirket tarafından sağlanan ve yine şirkete ait ortamlarda yedeklenmelidir. Perform Portföy Yönetimi A.Ş. 'ye ait veri, kişisel ve taşınalabilir cihazlara yedekleme amacı ile kopyalanamaz. Yedekleme ve veri saklama konusunda bir sözleşmeye istinaden başka bir resmi kurumdan hizmet alınması durumunda veri güvenliğinden ve yedeklerin alınmasından bu kurum sorumludur. Yapılacak anlaşmanın SPK dış hizmet alım şartlarını sağlaması gerekmektedir.
- Kamu kurum ve kuruluşları, portföy yönetim şirketinin işleyişi gereği sürekli yada isteğe bağlı veri sağlanması gereken Borsa İstanbul, Takasbank, MKK gibi kurumlar SPK tarafından yada BDDK tarafından yetkilendirilen kurumlar, dış denetçiler, sorun araştırması için müşteri bilgisi paylaşılmak durumunda olan yazılım ve destek firmaları, mahkemeler ve mahkeme emri ile yetkilendirilen kurum ve kuruluşlar onaya gerek duyulmaksızın bu bilgilerin paylaşılabileceği kurumlardır.
- Perform Portföy Yönetimi A.Ş. merkez ofisinde yedekleme amacı ile depolama cihazı kullanılamaz.
- Perform Portföy Yönetimi A.Ş. bilgisayarlarında ve iletişim sistemlerinde tutulan çok gizli ve gizli bilgi düzenli aralıklarla yedeklenir.
- Yedekleme sıklığı kullanılan uygulamanın kritikliği ve doğasına uygun olarak belirlenir.

5.3.5 Varlıkların Elden Çıkarılması

Perform Portföy Yönetimi A.Ş. Bilgi Sistemleri varlıklarının satılması, kullanımdan çekilmesi veya atılması öncesinde cihazlarda hiçbir Kurum verisinin kalmadığından ve geri döndürülebilir olmadığından emin olmalıdır.
Bu konuda alınacak tedbirler şunlardır.

- Son kullanıcı disketleri, cd ve diğer bilgi depolama aygıtları, içlerindeki verinin geri döndürülebilir olmadığından emin olunacak şekilde yok edilir.
- Kişisel bilgisayarlardaki veri aşağıdaki şekillerde silinir.
    - Veriyi temizleyerek(purging)
    - Alt düzey formatlama (low level formatting)
- Perform Portföy Yönetimi A.Ş. bilgisayarlarına lisanslanmış yazılım cihazdan silinir.
- Perform Portföy Yönetimi A.Ş. ileride referans olması için yok edilen varlıklarda bulunan önemli bilgilerin yedeklendiğinden ve depolandığından emin olunmalıdır.

5.3.6 İnternete Açık Sunucular

5.3.6.1 Sürece İlişkin Hususlar

- İnternet sayfaları aracılığıyla toplanan bilgiler, başka bir bilgi gerekmeden kullanıcıyı tanımlamaya, Kurum işlemleri yapmaya yetecek miktarda olmayacak şekilde düzenlenir.
- İş birimleri bir bilginin İnternet vasıtasıyla alınması gerektiği durumlarda proje/kampanya başlamadan ve İnternet sayfası hazırlanmadan önce Perform Portföy Yönetimi A.Ş. sistem yöneticisini bilgilendirmekle yükümlüdür.
- İnternet sayfaları aracılığıyla toplanan bilgiler 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında Perform Portföy Yönetimi A.Ş.'nin uymakla yükümlü olduğu kanun ve kendi prosedürlerine uygun saklanır, imha edilir ve olası ifşalara karşı güvenlik önlemleri alınır. İnternet sayfaları aracılığıyla toplanan verilere yönelik açık rıza ve aydınlatma metni Perform Portföy Yönetimi A.Ş. kurumsal internet sitesinde yer almaktadır.

5.3.6.2 Teknik Hususlar

- Perform Portföy Yönetimi A.Ş. İnternet sayfaları aracılığıyla bilgi toplanması durumunda iletişim
  mutlaka kriptolu yapılır.
- Kullanıcıya ait bilgiler (kimlik , iletişim , finansal, kredi kartı vb. bilgilerin) İnternete açık sunucular üzerinde yer alan veri tabanlarında saklanmaz.
- Kullanıcıya ait bilgiler (kimlik, iletişim , finansaL, kredi kartı vb. bilgiler) test ortamlarında bulundurulmaz.
- Sunucu DMZ'de (Demilitarized Zone) yer almalıdır.
- İnternet vasıtasıyla gelebilecek saldırılara karşı önlem olarak uygulama kontrolleri İnternet sayfaları üzerinde oluşturulur.

5.3.7 Depolama Cihazlarının Kullanımı

Perform Portföy Yönetimi A.Ş. 'de kullanılan bilgisayarlarda veri kaydetmeye yarayan cihazların (USB flash bellek, harici disk, CD/DVD Writer) kullanımına, yapılacak işlerin aksamaması amacıyla talebe istinaden sürekli veya acil durumlarda geçici olarak kullanıma açılması için Genel Müdür'den yazılı veya e-posta ortamında onay alınmalı ve BT' ye

iletilmelidir.

Görevi değişen ya da işten ayrılan personelin bilgisayarlarındaki veri kaydetmeye yarayan cihazların kullanım yetkisi kaldırılır.

- USB depolama cihazları haricindeki cihazlar (CD/DVD okuyucu - yazıcı cihazlar vb.) okuma özelliği ile kullanılabilir. USB depolama cihazları okuma veya yazma özelliğiyle kullanılamaz.
- Fare, klavye, tarayıcı , yazıcı vb. USB girişli cihazların kullanımı konusunda kısıtlama getirilmemiştir.
- Birim değişimi veya taşınma sebebiyle dosya aktarımı veya e-postaların transferi depolama cihazı vasıtasıyla yapılamaz. Çalışanlar saklamak istedikleri dokümanları veya e-postaları e- posta sistemi üzerinde birime transfer tamamlanana kadar saklayabilir.
- Çok gizli ve gizli bilgiler taşınabilir ortamlara kaydedilemez. Çok gizli ve gizli bilgiler sadece görevin etkin bir şekilde gerçekleştirilmesi için gerekli olunan hallerde veya yetkili kanuni mercilerden ve görevlilerinden talep edilmesi halinde taşınabilir ortamlara kaydedilebilir.
- Bilgisayarlarında depolama cihazı kullanma yetkisine sahip çalışanlar ;
    - Depolama cihazlarının sadece iş amaçlı kullanılması,
    - Bilgi güvenliği,
    - Veri kopyalama işleminin sadece Perform Portföy Yönetimi A.Ş. tarafından tahsis edilen cihazlara yapılması ,
    - Kullanılan depolama cihazlarının virüs açısından temiz olması konularından sorumludur . Bu sorumlulukları yerine getirmeyen çalışanların depolama cihazı kullanım hakları iptal edilir.

5.3.8 Veri Paylaşımı ve Transferleri Güvenliği

Çalışanlar, Perform Portföy Yönetimi A.Ş. birimleri arasındaki veri paylaşımları konusunda aşağıdaki konulara özen göstermelidir:

- Paylaşım, Perform Portföy Yönetimi A.Ş. sistemlerinde bulunan dosya sunucuları üzerinden veya Perform Portföy Yönetimi A.Ş. e-posta adresleri üzerinden yapılmalıdır.
- Dosya sunucularının kullanılacak olması durumunda, ortak yaratılacak bir klasöre kurumsal e- posta aracılığıyla ya da varsa şirket portalı aracılığı ile sistem sorumlusundan yetki istenmelidir. Bir birimdeki çalışanın farklı birimdeki klasöre erişebilmesi için erişilmek istenen klasör sahibi birime talepte bulunulmalıdır.
- Yetkiler, sistem yöneticisi tarafından mümkün olduğu sürece grup/rol bazında verilir . Böylece, görev veya birim değişikliği sonrası gruptan çıkarılan kişinin yetkilerinin güncellenmesi sağlanır.
- Paylaşımın süreklilik arz etmeyecek olması durumunda, dosyalar işlem sonrası ilgili

ortamlardan silinmelidir.
- Klasöre paylaşım sonrası ihtiyaç duyulmayacak olması durumunda, klasör kullanıcı tarafından silinmelidir.

Müşteri ve Perform Portföy Yönetimi A.Ş. 'ye ait veriler yönetmelikler ve kanunlar yoluyla bu bilgiye erişim hakkı olanlar hariç olmak üzere veri sahibi tarafından uygunluk verilmesi sonrasında dış firmalarla paylaşılabilir.

5.3.8.1 Veri Sınıflaması

Perform Portföy Yönetimi A.Ş.'ye ait veriler dört grupta sınıflanır:

- **Çok Gizli Bilgi:** Çok gizli bilgiler dış firmalarla paylaşılamaz.
- **Gizli Bilgi:** Gizli bilgi paylaşım sınırları açıkça ifade edildiği takdirde ve işin yapılması için şartsa paylaşılabilir.
- **Kuruma Özel Bilgi:** Kuruma özel bilgi paylaşım sınırları açıkça ifade edildiği takdirde ve işin yapılması için şartsa paylaşılabilir.
- **Kamuya Açık Bilgi:** Yönetim Kurulu tarafından halka açıklığı onaylanmış veya kanunlar tarafından açıklanması zorunlu tutulmuş bilgiler Kamuya Açık Bilgi olarak nitelendirilir.

5.3.8.2 Güvenlik Standartları

Paylaşılmak istenen veri hakkında yasal veya idari olarak Perform Portföy Yönetimi A.Ş.'yi bağlayıcı düzenlemelere uyulması zorunludur.

5.3.8.3 Kriptolama Standartları

Kurum çalışanlarının kriptolama konusunda aşağıdaki konulara özen göstermeleri beklenmektedir.

- Çok gizli olarak belirtilen veri iletişim ağı boyunca veya Perform Portföy ağları dışında bir ağa gönderilecekse (örneğine-posta) veya dış ağlardan Kurum sistemlerine gelecekse bu bilgi kriptolanmış olarak iletilmelidir.
- Gizli veya kuruma özel bilgi olarak belirtilen veri Perform Portföy Yönetimi A.Ş. ağları dışında bir ağa gönderilecekse (örneğin e-posta) veya dış ağlardan Kurum sistemlerine gelecekse bu bilgi kriptolanmış olarak iletilmelidir.
- CD, DVD, flash bellek, disket, harici hard disk gibi taşınabilir cihazlara atılan tüm gizli bilgi kriptolanmış olmalıdır. Çok gizli bilgiler taşınabilir cihazlara kaydedilemez.
- Son kullanıcılar kriptolama fonksiyonu için Microsoft Office yazılım özelliklerini kullanabilirler.

5.3.8.4 Veri Yolu Standartları

- Dış firmalarla bilgi paylaşımı güvenli kanallarla yapılır. Güvenli kanallar aşağıda belirtilenlerle sınırlı olmamak üzere şunlardır:
  - Leased line
  - Secure hyper text transfer protocol (https)
  - Secure FTP (sftp)
- Dış firmalarla yapılan tüm bağlantılardaki trafik güvenlik duvarı, IPS, IDS vb. cihazlarla korunur ve trafik izlenir.
- E-posta vb. yollarla veri paylaşılma ihtiyacı olması durumunda yukarıda belirtilen kriptolama standartlarında kriptolama yapılır.

5.3.8.5 Dış Firmaların Uyması Gereken Standartlar

Firmalar müşteri ve Perform Portföy Yönetimi A.Ş. 'ye ait verinin korunması amacıyla aşağıdaki şartları sağlamalıdır :

- Perform Portföy Yönetimi A.Ş. verileri hizmet sözleşmesi olmaksızın üçüncü tarafların ortamlarında saklanamaz.
- Veriye erişebilen tüm kişilerin denetim izleri değiştirilemez bir şekilde saklanır.
- Veriye sadece işi gereği bu bilgiyi görmesi gereken kişiler erişebilir.
- Veriye erişimde görev ve sorumluluklar göz önüne alınarak en düşük yetki verilir.
- Verinin dış firma sistemlerinden çıkışını engelleyebilecek her tür önlem alınır. Bu dokümanda yazılanlarla sınırlı olmamak üzere alınması gereken asgari önlemler aşağıda belirtilmiştir.
- Bilgisayarların USB girişleri kapalı olmalı ve son kullanıcı tarafından bu özellik iptal edilememelidir.
- Veriler dış firma sisteminden e-posta yoluyla dışarı çıkarılmamalıdır.
- Veri sızıntısını engelleyebilecek araçlar kullanılmalıdır.
- Perform Portföy Yönetimi A.Ş. ağlarına dahil edilecek üçüncü taraf uygulama ve sistemleri kod gözden geçirme ve penetrasyon testlerine tabi tutulur. (Zaafiyet Testleri)
- Perform Portföy Yönetimi A.Ş. ağlarına dahil edilecek üçüncü taraf uygulama ve sistemlerinin raporları ilgili üçüncü taraftan talep edilir. Yapılan güvenlik testlerinin aşağıdaki şartları sağlaması gerekmektedir:
- Yapılan testler sonrasında ortaya çıkan açıklar giderilmeli ve tekrar test edilmelidir.
- Testler network katmanını kapsamalıdır. Ayrıca testler ağ fonksiyonlarını destekleyen bileşenlerle işletim sistemlerini içermelidir.
- Test, uygulama katmanını kapsamalı ve asgari olarak injection saldırıları, buffer overflow ve kriptografik zayıflıkları, güvenli olmayan iletişimi, uygunsuz hata ayıklamayı , cross-site scripting, uygunsuz erişim kontrolü ve cross-site request forgery zayıflıklarını ve yeni oluşan riskleri test etmelidir.
- Dış firmalardan satın alınan hazır paket program/ uygulamalar veya geliştirilecek olan uygulamaların OWASP (The Open Web Application Security Project)

standartlarını karşılayacak nitelikte olması beklenmektedir.

5.3.9 Veri Gizliliği

Tüm çalışanlar , danışmanlar, yükleniciler ve geçici çalışanlar Perform Portföy Yönetimi A.Ş. 'ye katıldığı veya Perform Portföy Yönetimi A.Ş. ile çalışmaya başladığı zaman Bilgi işlem Güvenlik Prensipleri dokümanını imzalarlar.

Uyulması gereken diğer kurallara aşağıda yer verilmiştir :

- Perform Portföy Yönetimi A.Ş.'nin Kuruma Özel sınıfına dahil olan bilgiler üçüncü taraflara verilmez. Üçüncü taraflara Perform Portföy Yönetimi A.Ş. dahili bilgisine erişim sadece ispat edilebilir ihtiyaçlarının olması durumunda ve bilgi paylaşımı veri sahibi tarafından onaylanmışsa verilebilir.
- Kullanıcılar Perform Portföy Yönetimi A.Ş. dışındaki şahıslara bilgi sistemleri kontrolleri veya nasıl kuruldukları konusunda bilgi vermemelidir .
- Bilmesi gereken kişiler haricinde bilgi sistemlerinde yaşanan kesintiler vb. hiç kimseye iletilmez.

Bunlara ilave olarak ürün ve uygulama geliştirme faaliyetlerinde aşağıdaki güvenlik önlemleri alınır:

- Müşterilerin İnternet üzerinden giriş yaptıkları şifreleri SMS ile açık olarak gitmemelidir.
- Cep telefonu bilgisi, bilgilendirme ve teyit amaçlı kullanımı nedeniyle düşük güvenlik seviyesiyle kaydedilmemelidir.
- Perform Portföy Yönetimi A.Ş. içi/ Perform Portföy Yönetimi A.Ş. dışı istihbarat kayıtlarında dolandırıcı/şüpheli dolandırıcı olarak yer alan şahıs/firmalarla çalışmaya son verilmelidir.
- Perform Portföy Yönetimi A.Ş. ve müşteri arasında geçen telefon görüşmelerinde hassas bilgiler paylaşılmamalıdır.(Hassas bilgi tanımı için bkz. 6698 sayılı Kişisel Verilerin Korunması Kanunu)
- Telefon, adres , erişim bilgisi güncellemeleri telefon güncelleme telefon/faks ile yapılmamalıdır.
- Müşterilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Müşterinin "bildiği" unsur olarak parola/değişken parola bilgisi gibi bileşenler, "sahip olduğu" unsur olarak tek kullanımlık parola üretim cihazı, kısa mesaj servisi ile sağlanan tek kullanımlık parola gibi bileşenler kullanılabilir. Bileşenler tamamen müşterinin şahsına özgü olmalı ve bunlar sunulmadan kimlik doğrulama gerçekleştirilememeli, hizmetlere erişim sağlanamamalıdır.
- Müşteriye ait hassas bilgiler yukarıdaki doğrulama yapılmaksızın müşteriye herhangi

bir ekranda gösterilmemelidir.

- Herhangi bir Perform Portföy Yönetimi A.Ş. ürününün kullanımı/edinimi sırasında müşteriye gösterilen bir bilgi, bir başka ürünün kullanımı/edinimi sırasında doğrulama kriteri olarak kullanılmamalıdır.
- Müşterinin cep telefonu/PC'sine link/program indirmesini gerektiren yöntemlerin kullanılması, müşteri algısını etkilediğinden risklidir. Ürün kullanım akışı ve güvenlik uyarıları müşteriye iletişim kanalları ile net olarak iletilmelidir. .

5.3.9.1 Bilgi Türleri

Bilgi türleri, gizlilik derecesine göre aşağıdaki sınıflara ayrılır:

- Çok gizli bilgi
- Gizli bilgi
- Kuruma özel bilgi
- Kamuya açık bilgi

Bir bilginin yukarıdaki sınıflardan hangisine dahil olduğu, veri sahibi tarafından belirtilir. Veri sahibi, veri ile ilgili iş biriminin bağlı olduğu bölüm yöneticisidir(Müdür, Bölüm Başkanı, Genel Müdür Yardımcısı).

Yukarıda belirtilen kategorilerden herhangi birinin içine alınmamış, veri sahibi tarafından herhangi bir sınıf belirtilmemiş bilgi Kuruma Özel Bilgi sınıfında değerlendirilir. Yeni bir bilgi ya da verinin oluşturulma süreci başladığı anda sınıflandırılmasının yapılması gereklidir.

Çalışanlar, danışmanlar ve yükleniciler tarafından Perform Portföy Yönetimi A.Ş. yararına üretilen, sağlanan her tür bilgi, yazılı istisnalar haricinde Perform Portföy Yönetimi A.Ş.'nin malıdır. Perform Portföy Yönetimi A.Ş., bilgisayarlarında ve kendi ağ sistemlerinde saklanan dosyaların içeriğinin veya bu sistemler aracılığıyla iletilen tüm mesajların yasal sahibidir.İş ihtiyaçları gereği Perform Portföy Yönetimi A.Ş. daha önceden haber vermeden bu bilgiye erişme hakkına sahiptir.

5.3.10 Veri İşleme Prosedürü

- Çok gizli/gizli bilgi veri sahibinin onayı alınmadan Perform Portföy Yönetimi A.Ş. sınırları dışına çıkarılamaz. Bu politika burada belirtilenlerle sınırlı olmamakla birlikte üçüncü taraflarla paylaşımı, taşınabilir bilgisayarları, flash bellekleri, harici hard-diskleri, basılı çıktıları vb. kapsamaktadır. Off-site yedekleme işlemleri bu kapsam dışındadır.

- Perform Portföy Yönetimi A.Ş. verisi, bilgisi, yazılı , basılı ya da sosyal ortamda Perform Portföy Yönetimi A.Ş.'ye ait olmayan bir bilgisayara; veri depolama aracına, bilgi işlem sistemine ya da sosyal ortama taşınmaz; kopyalanmaz. E-posta, ftp, dosya paylaşım , aklama, aktarım sitesi ya da programı ya da protokolü ezcümle her hangi bir imkanla Perform Portföy Yönetimi A.Ş. dışına çıkarılamaz. İstisnai durumlar aşağıdaki maddede izah edilmiştir.

- Kamu Kurum ve Kuruluşları, Portföy Yönetim Şirketi'nin işleyişi gereği sürekli ya da isteğe bağlı veri sağlanması gereken Borsa İstanbul, Takasbank, MKK gibi kurumlar, SPK tarafından ya da BDDK tarafından yetkilendirilen kurumlar , dış denetçiler, sorun araştırması için müşteri bilgisi paylaşılmak durumunda olunan yazılım ve destek firmaları, mahkemeler ve mahkeme emri ile yetkilendirilen kurum ve kuruluşlar , mevzuat gereği bilgi sahibi olması gereken veri yayın kuruluşları ya da veri yayın kuruluşlarından alınan ve verilen içerikler, kurumsal iletişim ve reklam kampanyaları kapsamında çalışılan firmalar bu onaya gerek duyulmadan çalışılabilecek kurum ve kuruluşlardır. Bununla beraber müşteri ve Perform Portföy Yönetimi A.Ş. 'nin ticari sır niteliğindeki bilgilerinin üçüncü taraflar ile paylaşılmaması yönünde gizlilik anlaşması yapılmadan bu tür kurum, kuruluş ve kişiler ile bilgi paylaşımına kesinlikle girilmemelidir. SPK'nın ve Türk Ticaret Kanunu 'nun müşteri ve Perform Portföy Yönetimi A.Ş.'nin ticari sır niteliğindeki bilgilerini paylaşımını düzenleyen maddelere uygun hareket etme şartı, her veri alış verişinden ve anlaşmada dikkate alınmalıdır.
- Çok gizli ve gizli bilgi veri sahibinin açık yetkilendirmesi alındıktan sonra açıklanabilir. Bir kişinin çok gizli ve gizli bilgiye erişim izninin olması bu bilgiyi başkalarına dağıtabileceği, açıklayabileceği anlamına gelmez.
- Çok gizli ve gizli veya Perform Portföy Yönetimi A.Ş.'ye özel bilgi uçaklarda, restoranlarda , toplu taşıma araçlarında ve diğer halka açık alanlarda okunmamalı, tartışılmamalı veya açıklanmamalıdır.
- Çok gizli/gizli bilgiye erişen veya depolayan, burada belirtilenlerle sınırlı olmamakla birlikte tüm taşınabilir bilgisayarlar, cep telefonları, vb. tüm dosyaları kriptolu olarak saklamalı ve farklı işletim sistemleriyle USB bellek, CD, DVD, network vb. üzerinden çalıştırılamayacak şekilde önyükleme korumasına sahip olmalıdır.
- İçeriğinde çok gizli/gizli Perform Portföy Yönetimi A.Ş. bilgisi bulunan basılı tüm dokümanlar Perform Portföy Yönetimi A.Ş.binalarından çıkartılmaları durumunda ve kullanılmadıkları sürece kilitli bir çantada muhafaza edilir. Bu tür bilgi kilitli olsa dahi araba , otel odası, ofis veya benzeri diğer mekanlarda gözetimsiz bırakılmaz.
- Verilerin işlenmesi sırasında "Kişisel Veri Saklama ve imha Politikası", "Kişisel Verilerin Korunması ve Gizlilik Politikası" ve "Özel Nitelikli Kişisel Veri Yönetimi Politikası" na uygun şekilde davranılır.

5.3.10.1 Bilginin Depolanması ve Elden Çıkarılması

- Tüm çalışanlar bilgiyi uygun bir şekilde koruma altına almak için çalışma masalarını ve çalışma alanlarını temiz tutmalıdır.
- Bilgi her zaman yetkisiz kişilerin erişiminden korunmalıdır. Çok gizli ve gizli bilgi gözetimsiz bir odada bırakılması durumunda kilitli çekmece veya dolapta tutulmalıdır.
- Gizli bilginin bir hard diskte veya kişisel bir bilgisayarda saklanması durumunda bilgi, erişim kontrol paketleriyle veya kriptolama yoluyla korunmalıdır. Bu türde bilginin taşınabilir ortamlara (harici hard disk, flash bellek, CD, DVD vb.) kaydedilmesi

durumunda bu ortamlar gizli şekilde işaretlenmelidir. Bu türde bilgiler sadece görevin etkin bir şekilde gerçekleştirilmesi için gerekli olunan hallerde veya yetkili kanuni mercilerin ve görevlilerinin talep etmesi halinde taşınabilir ortamlara kaydedilmelidir.

- Manyetik depolama aygıtları üzerindeki gizli bilginin yok edilmesi gerektiğinde "zeroization" programları kullanılır. Bu ortamlardan veriyi "silmek" yeterli değildir. Çok gizli Perform Portföy Yönetimi A.Ş. bilgisinin disket, tape veya diğer manyetik depolama ortamlarından silinmesi durumunda tekrarlanmış üstüne yazma işlemi uygulanır. Böylece verinin daha sonra geri alınması engellenecektir.
- Basılı tutulan gizli bilgi elden çıkarılacağı zaman tüm Perform Portföy Yönetimi A.Ş. ortamlarına konumlandırılan CD/ DVD ve kağıt öğütme özelliklerine sahip makinalarda okunmayacak şekilde parçalanır veya yakılır.
- Kullanıcılar yöneticilerinin onayını almadan önemli olabilecek Perform Portföy Yönetimi A.Ş. kayıtlarını ve bilgisini yok etmemeli veya elden çıkarmamalıdır. Perform Portföy Yönetimi A.Ş. kayıtlarının veya bilgisinin yetkisiz olarak yok edilmesi veya elden çıkarılması durumunda disiplin yönetmeliği ve kanunlara göre işlem yapılacaktır . Kayıtlar ve bilgi aşağıdaki durumlarda saklanmalıdır :
  Gelecekte ihtiyaç duyulabilecekse,
  Kanunlar veya düzenlemeler saklamayı gerektiriyorsa,
  Yetkisiz , yasadışı, kötü niyetli davranışları araştırmak için kullanılacaksa

5.3.10.2 Çok Gizli ve Gizli Bilginin Çıktısının Alınması

Müşteri numarası, Türkiye Cumhuriyeti Kimlik Numarası, sözleşme numarası, telefon numarası gibi müşteriye özel bilgilerin yer aldığı elektronik ortamda bulundurulan dokümanların çıktılarının alınması sınırlandırılmıştır.
Çok gizli ve gizli bilginin çıktısı alınırken veya kısa bir zaman içinde çıktısı alınacaksa yazıcılar gözetimsiz bırakılmamalıdır. Yazıcının çalışmasına iştirak eden kişiler basılan bilgiyi inceleme yetkisine sahip olmalıdır.

5.4 YÖNETİMSEL GÜVENLİK

İdarecilerin genel güvenlik sorumlulukları aşağıda belirtilmektedir:

5.4.1 Eğitim ve Farkındalık

Bilgi Güvenliği Eğitimi tüm çalışanlar için zorunludur.

- Perform Portföy Yönetimi A.Ş. ; düzenli olarak çalışanlara , yüklenicilere, danışmanlara ve diğer çalışanlara bilgi güvenliğiyle ilgili eğitim ve eğitici materyal sağlamakla yükümlüdür.
- Yönetim, çalışanların Perform Portföy Yönetimi A.Ş. güvenlik politikalarına, prosedürlerine, iş yapış biçimlerine alışması için iş başında yeterli süreyi ayırır.
- Perform Portföy Yönetimi A.Ş. 'nin iş ortakları, tedarikçileri, müşterileri ve diğer iş

bağlantıları bilgi güvenliği sorumlulukları hakkında bilgilendirilir.
- Perform Portföy Yönetimi A.Ş. bilgi güvenliği sorumlusu, bilgi güvenliğine yönelik farkındalık ve hassasiyetine dikkat çekmek amacıyla güvenlik mesajları yayınlar.

5.4.2 Proje Yönetiminde Bilgi Güvenliği

Perform Portföy Yönetimi A.Ş. Proje Yönetimi süreçlerinde Bilgi Güvenliği açısından risk değerlendirmeleri yapılır. Perform Portföy Yönetimi A.Ş. Sistem Yöneticisi ve Bilgi Güvenliği Sorumlusu tarafından riskli görülen durumların olması halinde; riskli hallerin ortadan kaldırılması, iş birimi ve proje için görevlendirilmiş Proje Yönetimine atanan personelin sorumluluğundadır.

5.4.3 Güvenlik Sorunlarının Raporlanması

- Çalışanlar güvenlik olaylarını ele alma/raporlama prosedürlerine göre hareket eder.
- Tüm Perform Portföy Yönetimi A.Ş.çalışanları bilgi güvenliği ihlallerini ve sorunlarını en kısa sürede önlemlerin alınabilmesi amacıyla Perform Portföy Yönetimi A.Ş. Sistem Yöneticisi ve Bilgi Güvenliği Sorumlusu'na bildirmekle yükümlüdür.
- Bilgisayar virüsleri çok çabuk yayılabilirler ve bilgisayarlara ve veriye ciddi zarar vermelerini engellemek için en kısa sürede temizlenmelidirler. Bir kullanıcı bilgisayarında virüs olduğundan şüpheleniyorsa veya ekranda virüs olduğuna dair uyarı mesajı almışsa bu durumu Sistem Yöneticisine bildirir.
- Tüm çalışanlar donanımlarında ve yazılımlarında meydana gelen ciddi hasarları, kayıpları (örneğin, bir dizüstü bilgisayarın çalınması) Perform Portföy Sistem Yöneticisine bildirmekle yükümlüdür.

5.4.4 Diğer Güvenlik Konuları

- Bilgi güvenliği politikalarına, standartlarına veya prosedürlerine uyumsuzluk disiplin yönetmeliği ve ilgili kanunlar uyarınca işlem yapılmasını gerektirir.
- Bilgi Teknolojileri Bölümü çalışanlarının işten çıkartılması durumunda ilgili çalışanlar tüm görevlerden el çektirilir , Perform Portföy Yönetimi A.Ş. 'ye ait tüm materyal ve bilgi geri alınır.
- Tüm yükleniciler, danışmanlar ve geçici çalışanlar sözleşmenin sona erdirilmesi veya sona ermesi durumunda proje süresince aldıkları ve/veya üretilen Perform Portföy'e ait tüm bilgiyi teslim ederler.
- Önemli bilgisayar veya iletişim sistemleriyle ilgili çalışmalar en az iki kişi tarafından yürütülür. Bu sayede hizmet seviyesinde aksama azalacak ve yetkisiz işlemlerin tespit edilme ihtimali artacaktır.
- Bilgisayar sistemleriyle ilgili işlerde çalışacak çalışanların işe alımı öncesi referans araştırması yapılmalıdır.
- Çalışanlar, Perform Portföy Yönetimi A.Ş. dijital ve fiziksel ortamlarında oluşan bilgi

güvenliği ihlal olayları Perform Portföy Sistem Yöneticisi ve Bilgi Güvenliği Sorumlusu 'na bildirmelidirler.

5.5 FİZİKSEL GÜVENLİK

Bilginin saklandığı ortamlara yapılan fiziksel erişimlerin güvenliğinin sağlanmasına yönelik alınacak tedbirler aşağıda belirtilmiştir:

5.5.1 Bina Erişim Güvenliği

- Tüm çok kullanıcılı bilgisayarlar ve iletişim cihazları değiştirilmeyi ve yetkisiz kullanımı engellemek için kilitli odalarda bulundurulmalıdır.
- Çok gizli ve gizli bilgi içeren tüm ofis, bilgisayar odası ve çalışma alanlarına erişim fiziksel olarak kısıtlanır.
- Tüm çalışanlar ve ziyaretçiler Perform Portföy Yönetimi A.Ş. sınırları dahilinde giriş kartlarını görünebilir ve okunabilir şekilde taşımalıdır.
- Giriş kartları kaybolan - çalınan veya kaybolduğundan - çalındığından şüphelenen kişiler durumu en kısa sürede güvenliğe iletmelidirler.
- Çalışanlar yetkili oldukları alanlara kartlarıyla giriş yaparken tanımadıkları kişilerin onlarla beraber bu alanlara girmesine izin vermemelidir.
- Çok gizli veya gizli bilginin görüntülendiği bilgi sistemlerinin ekranları yetkisiz kişilerin göremeyeceği şekilde konumlandırılır.

5.5.2 Ekipman Güvenliği

- Tüm bilgisayar sistemleri güvenli ortamlar içinde konumlandırılır veya yetkisiz erişimi engellemek için çalışan gözetiminde tutulur.
- Dizüstü bilgisayar, taşınabilir cihazları kullanan çalışanlar cihazı yanından ayırmamalı ve uygun güvenlik önlemlerini almadan gözetimsiz bırakmamalıdır.
- Veriyi güvence altına almak için taşınabilir cihazlarda şifreleme veya eşit seviyede güçlü önlemler kullanılır.
- Tüm Perform Portföy Yönetimi A.Ş. cihazlarında yaşanacak donanım/yazılım problemleri ile ilgili olarak sadece Perform Portföy Yönetimi A.Ş. 'nin ilgili birimlerinden destek alınmalıdır.
- Çalıntı cihazlar için Perform Portföy Yönetimi A.Ş. sistem yöneticisine haber verilir.

5.5.3 Ziyaretçi Güvenliği

Perform Portföy Yönetimi A.Ş. tarafından kontrol edilen alanlara erişmek isteyen çalışanlar resimli kimlik ibraz etmek zorundadır.
İş amaçlı olarak Perform Portföy lokasyonlarına gelen ziyaretçiler bina girişinde resimli kimlik ibraz etmek zorundadır. Bu görev bina yönetimi güvenlik personelinin sorumluluğundadır.

Perform Portföy lokasyonlarına gelen ziyaretçiler, ilgili Perform Portföy Yönetimi A.Ş.çalışanı tarafından ana kapıda karşılanır ve ziyaret süresince ziyaretçiye eşlik eder.

5.5.4 Bilgisayar Tesislerine Erişim

- Bilgisayar odaları (server farm) veya iletişim sistemleri yetkisiz kişilerin erişimini engellemek için fiziksel güvenlik önlemleriyle korunur.
- Uygulama geliştiricilerin/programcıların bilgi işlem merkezlerine erişimine gözetim altında izin verilir.
- Bilgi işlem merkezlerine erişim için yazılı olarak giriş - çıkış kayıtlarının tutulmasından İnfina Yazılım A.Ş. sorumludur.

5.6 DİĞER HUSUSLAR

5.6.1 Kabul Edilebilir Bilgisayar Kullanımı

- Kişisel bilgisayarlar yetkisiz erişimlerden korunmalı ve gözetimsiz açık olarak bırakılmamalıdır.
- Kullanıcılar bilgisayarlarında kurulu olan sistem ve yazılım ayarlarını Perform Portföy Yönetimi A.Ş. sistem yöneticisinden izin almadan değiştirmemelidir.
- Çalışanlar bilgisayarlarında çalışması gereken anti virüs, uzaktan yönetim konsolu gibi programların çalışmadığını fark etmeleri durumunda olay bildiriminde bulunmalıdır.
- Çalışanlar işle ilgisi olmayan film, müzik ve görsel dokümanları bilgisayarlarına yüklememeli ve e-posta ile dağıtmamalıdır. Kişisel resimler disk kapasitelerini zorlaması sebebiyle ortak alanlarda saklanmamalıdır.

Bilgisayar virüsü kendisini çoğaltan ve çeşitli kayıt ortamlarına (hard disk, flash disk, manyetik teyp vb.} ve/veya ağa yayılan yetkisiz programdır. Virüs girmiş bilgisayarlarda aşırı yavaşlama , dosya kaybolması ve sistemin çalışmaması gibi olaylara rastlanabilir. Günümüzde virüsler komplike bir duruma gelmiştir. Kullanıcılar bilgisayarlarına virüs girdiğinden şüpheleniyorsa çalışmayı kesmeli ve sistem yöneticisini aramalıdırlar. Kullanıcıların, sistem yöneticilerinin yönlendirmeleri olmadan bilgisayarlarındaki virüsleri silmeleri, temizlemeleri yasaktır.

- Kullanıcılar Perform Portföy Yönetimi A.Ş. ağları dışındaki ortamlardan (Internet vb.) yazılım indirmemelidir. İndirilen yazılımların virüs, truva atı, solucan ve diğer zararlı yazılımlar içerme ve Perform Portföy Yönetimi A.Ş. sistemlerine zarar verme riski bulunmaktadır.
- Şüpheli veya bilinmeyen kaynaklardan gelen e-postaların içindeki eklentiler açılmamalıdır. Bu tür e-postalar sistemden ve çöp kutusundan silinmelidir. Kullanıcılar virüs içerdiğinden şüphelendikleri hiçbir e-postayı başka kullanıcılara iletmemeli , sistem yöneticisini haberdar etmelidirler.

- Kullanıcıların kendini kopyalayan, bilgisayara veya bilgisayarınyazılımlarına, işletim sisteminin performansına zarar veren bilgisayar kodlarını yazmaları, dağıtmaları, kopyalamaları ve çalıştırmaları kesinlikle yasaktır.

5.6.2 E-Posta Sistemleri Güvenliği

- Perform Portföy Yönetimi A.Ş. e-posta sistemi ; ırk, cinsiyet, saç rengi, engellilik, yaş, cinsel tercih, pornografi, dini inançlar ve ibadet, siyasi görüşler veya köken ile ilgili rencide edici yorumlar da dahil olmak üzere hiçbir yıkıcı veya rencide edici mesajın oluşturulması veya dağıtılması için kullanılamaz. Herhangi bir Perform Portföy Yönetimi A.Ş. çalışanından böyle mesajlar alan çalışanlar durumu üstlerine bildirmelidirler .
- Perform Portföy Yönetimi A.Ş. e-posta sistemleri iş amaçlı olarak kullanılır. Perform Portföy sistemleri kullanılarak iletilen tüm mesajlar Perform Portföy Yönetimi A.Ş.'nin mülkiyetindedir. Perform PortföyYönetimi A.Ş., kendi elektronik sisteminden iletilen mesajlara erişme ve bunları gerekirse açıklama hakkına sahiptir . Perform Portföy Yönetimi A.Ş. denetim birimi çalışanların yaptığı mesajlaşmaları güvenlik ihlali, şirket politikalarının ihlali veya diğer yetkisiz işlemleri belirlemek için izleyebilir.
- Kullanıcılar başka bir kişiye ait e-posta hesabını mesaj göndermek ve almak için kullanamaz. Kullanıcı kendi e-postalarına iş sebebiyle başka bir kullanıcının erişmesini istiyorsa Perform Portföy Yönetimi A.Ş. kurum içi otomatik mesaj veya ofis dışında mesajlarıyla yönlendirme sağlamalıdır.
- E-postaların Perform Portföy Yönetimi A.Ş. dışındaki bir adrese otomatik olarak yönlendirilmesi/iletilmesi yasaktır.
- E-posta kutularına gelen zincir postalar ve spam mesajlar (istenmeyen e-posta) bu mesajların bilgi toplama ve/veya sahtekarlık amaçlı kullanılması sebebiyle başka çalışanlara veya Perform Portföy Yönetimi A.Ş. dışına gönderilmemelidir.
- Virüs tehlikesine karşı, tanınmayan kişilerden gelen belge ve dokümanlar açılmadan silinmelidir .
- Kullanıcılar düzenli olarak önemli bilgilerini elektronik postalarından arşiv klasörlerine taşımalı veya kendi bilgisayarlarında yedeklemelidir. Elektronik posta sistemleri önemli bilgilerin arşivlenmesi ve depolanması için tasarlanmamıştır. Kayıtlı posta mesajları kullanıcılar tarafından veya sistemsel hatalardan dolayı silinebilir.
- E-posta üzerinden iletilen bilgilerin hassasiyeti konusunda dikkatli olunmalıdır. Müşteriye/ Perform Portföy Yönetimi A.Ş. 'ye ait, bu uygulama esaslarında belirtilenlerle sınırlı olmamak üzere çok gizli ve gizli bilgilerin e-postalarda açık olarak belirtilmesi , maskelenmeden/şifrelenmeden dolaşıma çıkarılması yasaktır. Bu tür bilgiyi e-posta yoluyla iletme ihtiyacı olan birimler ilgili üst yöneticisinin onayını almalıdır. Bu uygulama esasları kapsamında hassas olan bilgilerin bir kısmı aşağıda belirtilmiştir:

    - Müşteri özlük bilgileri
    - Müşteri iletişim bilgileri

- Her tür şifre bilgisi
- Müşteri Portföy Durumu ve işlemleri (Müşterinin kayıtlı e-mail'ine gönderilebilir.)
- Stratejik Planlar

Bu bilgilerin dışında kalan ve gizliliği konusunda emin olunmayan veri için Perform Portföy Yönetimi A.Ş. iç kontrol ve bilgi güvenliği uzmanına danışılmalıdır.

- Perform Portföy 'deki işlerin sürekliliğini sağlamak üzere önemli yazışmalarda mutlaka bir üst yönetici, duruma göre alt unvan bilgide (CC) tutulmalıdır.
- Gelen ve giden e-postalar virüsler için taranmalıdır.
- Dahili e-posta listelerinin bakımı düzenli olarak yapılmalı ve yetkisiz erişim ve değişiklikten korunmalıdır.

Perform Portföy Yönetimi A.Ş. sistem yöneticisi tüm e-posta iletişiminin bir kopyasını kanunlar gereği saklamakla yükümlüdür .

5.6.2.1 Uzaktan E-Posta Erişimi

- Perform Portföy e-posta sistemlerine uzaktan erişim; iş ihtiyacı için erişmesi gereken çalışanlara tanımlanabilir.
- Uzaktan e-posta erişimi, yabancı/bilinmeyen bilgisayarlardan, internet kafe, açık ağlar vb. güvenli olmayan alanlardan yapılmamalıdır. Bu alanlarda bulunabilecek virüsler sisteme zarar verebilir , bilgisayar korsanları tarafından bilgiler ele geçirilebilir, dolayısıyla bilgi güvenliği açısından risk oluşturabilir. Perform Portföy Yönetimi A.Ş. sistem yöneticisi bu madde kapsamında teknik açıdan getirilebilecek kısıtlamaları uygulamakla yükümlüdür.

5.6.2.2 Web Üzerinden E-Posta Erişimi Prensipleri

- E-postalarına bilgisayar aracılığıyla İnternet üzerinden erişmek isteyen çalışanların Microsoft Windows İşletim Sistemi kullanmaları zorunludur. Bilgisayarlarda en az Microsoft Windows 10 ve üstü işletim sistemi kurulu olmalıdır.
- Bilgisayarlarda Perform Portföy Yönetimi A.Ş. BT tarafından uygunluğu belirtilen güncel bir anti virüs programı kurulu, arka planda koruma sağlıyor ve bağlantı süresince çalışıyor olmalıdır.
- Kablosuz ağ vasıtasıyla bağlanılması durumunda kablosuz ağın WPA, WPA-2 , WPA-Enterprise veya WPA-2 Enterprise güvenlik seviyesinde kriptolu olması sağlanmalıdır.
- Sisteme erişim sağlanmadan önce Bluetooth ve kızıl ötesi kapatılır.

5.6.2.3 RPC Over Https E-Posta Erişimi Prensipleri

RPC Over https (remote procedure call over https), Microsoft Outlook veya başka bir e-posta uygulamasıyla Perform Portföy Yönetimi A.Ş. sistemleri dışından e-posta erişimidir. Bu türde erişimlerle ilgili çalışanların uyması gereken prensipler aşağıda belirtilmiştir. Yetki aşağıdaki çalışanlara tanımlanabiliir

- Üst Yönetim (Yönetim Kurulu , Genel Müdür, Genel Müdür Vekilleri, Genel Müdür Yardımcıları)
- Görev tanımı gereği düzenli olarak Perform Portföy Yönetimi A.Ş. binaları dışında görevli çalışanlar

Erişimde Microsoft Outlook 2010 ve üzeri kullanılmalıdır. Diğere-posta uygulamalarının kullanılmaması gereklidir.

5.6.2.4 Mobil Cihazlar Erişim Prensipleri

Perform Portföy Yönetimi A.Ş. tarafından kendisine cihaz tahsis edilen kullanıcılar e-postalarına mobil olarak bu cihazlarla bağlanmalıdır.
Perform Portföy Yönetimi A.Ş. tarafından tahsis edilmeyen cihazlarla erişim yapılmasına bilgi güvenliği riskleri sebebiyle izin verilmemektedir

5.6.2.5 İşten Ayrılma

Kurumumuz çalışanlarının Perform Portföy Yönetimi A.Ş. 'den ayrılması durumunda e-posta hesabı ve e-postaları için aşağıdaki prosedür uygulanır:

- Hukuki sorumluluğu olan, unvanı hangi ad altında olursa olsun GMY ve/veya üstü konumdaki tüm yöneticiler için 3 ay süre ile e-posta hesaplarına mesaj geldiğinde, orijinal mesaj yönlendirilmeden, göndericiye bilgilendirme yapılacaktır . Bilgilendirme metninde ayrılan kişinin Perform Portföy Yönetimi A.Ş.'ye yazılı olarak beyan ettiği yeni adresi sadece Gmail, Yahoo gibi kişisel mail adresleri olması durumunda kullanılacak, başka kurumların adresleri bilgilendirme mesajında kullanılamayacaktır. Ayrılan personelin e-posta göndermesi engellenecek, uzaktan e-postalarına erişimi kaldırılacak ve e-posta gruplarından çıkartılacaktır.
  Bilgilendirme Metni:

  Sayın ilgili,

  Bu mesaj, sistem tarafından gönderilen otomatik bir yanıttır. Gönderdiğiniz e-posta adreslediğiniz kişiye ulaşmamıştır.
  Sn. Xxxx Yyyyy'a gönderdiğiniz elektronik postalar sistem tarafından iletilememektedir.
  Kendisine <xxxx.yyyyy@zzzzz.com> adresinden
  ulaşabilirsiniz . Perform Portföy Yönetimi A.Ş.

  Dear Sir/Madam,

This is an auta reply message, your email was not delivered to the person you addressed.
All emails sent to Xxxx Yyyyy are rejected by the system and will not be forwarded.
You can contact him/her via <xxxx.yyyyy@zzzzz.com>
Perform Portföy Yönetimi A.Ş.

- 3 ay süre ile açık tutulacak e-posta hesaplarına gelen e-postaların bir kopyası, Perform Portföy iç kontrol tarafından belirlenen e-posta adresine yönlendirilecektir.

Unvanı hangi ad altında olursa olsun e-posta arşivi ayrılan kişiye teslim edilmeyecektir. Ayrılmış olan GMY ve/veya üstü pozisyonundaki kişiler, özel bir e-postasını talep etmeleri durumunda, iç kontrol yöneticisine yönlendirileceklerdir. Yapılan değerlendirme sonucunda e-postanın iş ile ilgili olmadığına emin olunması durumunda, e-posta ayrılan çalışana iletilebilir.

5.6.3 Kişisel İletişim Cihazları ve Sesli Posta

5.6.3.1 Sesli Posta

Sesli posta kutuları bir PİN vasıtasıyla korunur. PİN kodu hiçbir zaman sesli posta kutusunun bağlı olduğu telefonun son dört hanesi olmamalıdır.

5.6.3.2 Kayıp ve Çalıntı

Çok gizli veya gizli olan bilgiler kişisel iletişim cihazlarında tutulamaz. Kayıp veya çalıntı ekipman acilen BT bölümüne bildirilir.

5.6.3.3 Kişisel Kullanım

İletişim cihazları ve sesli posta çalışanlara Perform Portföy Yönetimi A.Ş. 'nin iş faaliyetleri için sağlanan hizmetlerdir. Kişisel kullanım asgari seviyede tutulmalı ve zorunlu olmadıkça bu tür cihazlar kişisel işler için kullanılmamalıdır.

5.6.4 Dizüstü Bilgisayar Güvenliği

5.6.4.1 Genel Prensipler

Perform Portföy BT dizüstü bilgisayarların güvenliğini sağlamaya yönelik olarak aşağıda belirtilen önlemleri alır.

- İşletim sistemlerinde ön tanımlı olarak gelen "Guest" hesabı ve "Administrator " hesabı "disable" edilmelidir.
- Bilgisayarlarda kullanıcılara "Administrator " rolü verilmemelidir . Administrator

rolüne ihtiyaç duyulan bilgisayarlar Perform Portföy Yönetimi A.Ş. sistem yöneticisi tarafından dokümante edilir ve takip edilir.

- Perform Portföy Yönetimi A.Ş. sistem yöneticisi tarafından üst yönetime teslim edilen veya servis işlemine tabi olan cihazlar haricindeki cihazlarda USB depolama aygıtlarının, kızıl ötesi cihazların ve Bluetooth kullanımı engellenir, CD/DVD cihazlarının "write" özelliğinin kapalı, "read" özelliğinin açık olması sağlanır.
- Bilgisayarlarda gerçek zamanlı virüs koruma (real-time protection) her zaman açık tutulmalı, son kullanıcı tarafından müdahalelere izin verilmemelidir.
- Bilgisayarlarda güvenlikle ilgili loglar (Security, Firewall vb.) çalışır olmalıdır.
- İş birimlerinin veya çalışanların yetki, birim vb. farklı ihtiyaçları gereği farklı konfigürasyonlar yapılması durumunda dokümante edilmeli ve uygulama konfigürasyon şablonu oluşturulmalıdır.
- Bilgisayarlarda en fazla 15 dakika içerisinde devreye giren, şifre korumalı ekran koruyucu kullanılır. Son kullanıcı tarafından şifreli ekran koruyucuya müdahale edilmesi sistem tarafından engellenmelidir. Bunun mümkün olmadığı durumlarda sorumluluk son kullanıcıdadır.
- Bilgisayarlar üzerinde yetkisiz donanımsal erişimlerin tespitine yönelik olarak güvenlik etiketleri bulunur.
- Perform Portföy Yönetimi A.Ş. sistem yöneticisi tarafından kablolu ve üretim ortamlarında yer alan kablosuz ağlarda Network Access Protection (NAP) devreye alınır.

Tüm çalışanlar dizüstü bilgisayar güvenliğini sağlamak amacıyla aşağıdaki konulara özen göstermelidir.

- Çalışanlara tahsis edilen dizüstü bilgisayarların iş amaçlı kullanımı esastır.
- Dizüstü bilgisayarlar , mesai saatleri içinde ve dışında, sadece yetkili Perform Portföy Yönetimi A.Ş. çalışanları ve yetkili outsource/geçici/firma çalışanları tarafından kullanılmalıdır.
- Bilgisayarlar üzerinde tutulan ve iş bitiminde saklanmasına gerek olmayan müşterilere veya Perform Portföy Yönetimi A.Ş. 'ye ait çok gizli ve gizli bilgiler uzun süre bilgisayarda biriktirilmemeli, 30 gün içinde bilgisayardan silinmelidir. Bilgisayardaki çöp kutusu boşaltılmalıdır.
- Bilgisayar üzerindeki verilerin , e-posta, depolama cihazlarına kopyalama, CD/DVD yazma, çıktı alma , vb. yöntemlerle yetkisiz şahıslarla paylaşılması veya bu şahıslarca görüntülenmesine izin verilmesi yasaktır.
- Bilgisayarda bulunan önemli bilgiler Perform Portföy Yönetimi A.Ş. networkünde yer alan, birimlere ayrılmış güvenli alanlara kopyalanarak periyodik olarak yedeklenir. USB depolama cihazı, CD/DVD gibi ortamlar yedekleme için uygun ortamlar değildir.
- Bilgisayarlar üzerinde kullanılan, güvenlikle ilgili programların çalışmasını engelleyici herhangi bir müdahalenin yapılması yasaktır.
- Bilgisayarlar üzerinde kullanılan güvenlik programları (güvenlik duvarı, anti virüs programı vb.) güncel tutulmalıdır. Programlar tarafından verilen uyarı mesajları

dikkate alınmalı, gerektiğinde BT aranmalıdır .

- Dizüstü bilgisayarlar Perform Portföy Yönetimi A.Ş. networküne takılı durumdayken Bluetooth özelliği kapalı tutulmalıdır.
- Dizüstü bilgisayarlarda yaşanacak donanım /yazılım seviyesindeki problemlerle ilgili olarak sadece Perform Portföy Yönetimi A.Ş. 'nin ilgili birimlerinden destek alınmalıdır.
- Perform Portföy Yönetimi A.Ş. tarafından çalışanlarına iş amaçlı tahsis edilen dizüstü bilgisayarların (laptop) her ayın üçüncü haftası Perform Portföy Yönetimi A.Ş. lokasyonlarına getirilerek ağ üzerinden dağıtılan güncel paketlerin bilgisayarlara yüklenmesi sağlanmalıdır.
- Perform Portföy Yönetimi A.Ş. çalışanlarının Perform Portföy Yönetimi A.Ş. 'ye ait olmayan dizüstü bilgisayarlarını Perform Portföy Yönetimi A.Ş. networküne bağlamaları yasaktır.
- Danışmanlık hizmetleri dış kaynak kullanımı vb. sebeplerle Perform Portföy Yönetimi A.Ş. 'ye ait olmayan dizüstü bilgisayarların Perform Portföy Yönetimi A.Ş. networküne erişmesine ihtiyaç duyulması halinde aşağıdaki şartların sağlanması gereklidir. Bağımsız denetim ve kamu denetimi faaliyetleri kapsamında yapılacak çalışmalar bu maddenin kapsamı dışındadır.
  - 1 aydan uzun süreyle Perform Portföy Yönetimi A.Ş. 'de çalışılacak durumlarda networke erişim verilebilir.Talepte bulunan Perform Portföy Yönetimi A.Ş. çalışanları bu şartın sağlandığından emin olacaktır.
  - Firmayla, çalışanlarını da bağlayacak şekilde, Perform Portföy Yönetimi A.Ş. güvenlik kriterlerine uygun çalışılacağına dair madde(ler)in ve yaptırımın bulunduğu sözleşme imzalanmış olmalıdır.
  - Erişimde kullanılacak bilgisayarların öncelikle Perform Portföy Yönetimi A.Ş. sistem yöneticisine bildirilerek gerekli güvenlik kontrollerinden geçmesi zorunludur. Sistem yöneticisi bilgisayarlarda güncel anti virüs programı olduğunu, gerçek zamanlı koruma sağlandığını kontrol eder.
  - Yukarıda belirtilen şartların yerine getirildiğini Perform Portföy Yönetimi A.Ş. sistem yöneticisi kontrol eder. Yukarıdaki şartların bir veya daha fazlasının sağlanamaması durumunda talepte bulunan iş birimi Perform Portföy Yönetimi A.Ş. sistem yöneticisine ithafen, sisteme bağlı olan kişilerin sadece iş amaçlı olarak çalışacaklarını ve anti virüs programının sürekli çalışmasının kendi kontrolünde ve gözetiminde olduğunu, bu bağlamda ortaya çıkabilecek, tespit edilen tüm bilgi güvenliği zafiyetlerinin sorumluluğunu aldığını peşinen kabul ve beyan ettiğini belirten resmi iç yazı gönderir.

5.6.4.2 Cihazın Kaybolmasını ve Çalınmasını Engelleyecek Önlemler

- Bilgisayar hiçbir zaman havaalanı, restoran gibi kamuya açık yerlerde göz önünden ayrılmamalıdır.
- Bilgisayar araba içinde veya arabanın bagajında bırakılmamalıdır.

- Özellikle seyahat esnasında dizüstü bilgisayar mutlaka çalışanın yanında bulundurulmalı, bagaja teslim edilmemelidir.
- Havaalanı, alışveriş merkezleri, x-ray cihazları gibi güvenlik denetim noktalarında tedbirli olunmalıdır.
- Cihazın çantası ve cihaz üzerinde Perform Portföy Yönetimi A.Ş. şirket adresinin ve kaybolduğu zaman aranması gereken bir telefon numarasının yazılı olduğu bir etiketin bulunduğundan emin olunmalıdır.

5.6.4.3 Verinin Çalınmasını Engelleyecek Önlemler

- Tüm dizüstü bilgisayarların hard diskleri, bilgisayarı kullanmaya yetkisi olmayan kişilerin veriye erişimini engellemeye ve veriyi gerekli yetkilendirme işlemlerinden geçilmediği sürece okunamaz şekilde saklamaya yarayan, genel kabul görmüş kriptolama teknolojilerinden biriyle şifrelenir.
- Bilgisayar açık olduğu sürece işletim sistemine ait ve/veya Perform Portföy Yönetimi A.Ş. tarafından onaylanmış güvenlik duvarı yazılımı açık tutulur.
- Güvenli olmayan veya halka açık alanlarda kablosuz ağlar kullanılmamalıdır.
- Güvenli olmayan Internet sitelerine girilmemelidir.
- Kullanılmadığı durumlarda cihazlardaki kızıl ötesi ve bluetooth özellikleri kapatılmalıdır.
- Bilgisayarlara Perform Portföy Yönetimi A.Ş. 'nin onayladığı/yüklediği programlar haricinde program yüklenmesi veya çalıştırılması yasaktır. Bir program kurulmak istendiğinde veya bilgi almak için Perform Portföy Yönetimi A.Ş. sistem yöneticisi ile temasa geçilmelidir.

5.6.4.4 Cihazın Kaybolması/Çalınması Durumunda İzlenecek Prosedür

- Dizüstü bilgisayarın kaybolması/çalınması durumunda aşağıdaki birimlerin bilgilendirilmesi gereklidir:
  - Muhasebe ve idari işler Müdürlüğü
  - Perform Portföy Yönetimi A.Ş. Sistem Yöneticisi(BT Ekipmanları için)
- Emniyet birimince tutulmuş zaptın aslının veya noter onaylı "Aslı Gibidir" mühürlü örneğinin elektronik kopyası ve dizüstü bilgisayar içinde yer alan verilerin içeriği en kısa sürede Muhasebe ve idari işler Müdürlüğü'ne iletilir .
- Emniyet Birimi'nce tutulmuş zaptın aslı veya noter onaylı "Aslı Gibidir" mühürlü örneği ve cihaz demirbaş numarası Perform Portföy Yönetimi A.Ş. BT'ye iletilir.
- Perform Portföy Yönetimi A.Ş. BT, cihazın envanterden düşülmesi için Muhasebe ve idari işler Müdürlüğü'ne bilgilendirme yazısı iletir.

5.6.5 Üçüncü Taraflar

Üçüncü tarafların bilgi varlıklarına erişimine, açıkça tanımlanmış iş ihtiyacı sonrası izin verilir .

- Üçüncü taraflarla ilgili riskler tanımlanır ve bu risklere uygun önlemler alınır.
- Üçüncü taraflardan alınan hizmetler için standart Perform Portföy Yönetimi A.Ş. Gizlilik Sözleşmesi, Kişisel Verilerin Korunmasına İlişkin Ek Protokol sözleşmeleri imzalanır. Üçüncü taraf çalışanlarına, Perform Portföy Yönetimi A.Ş. ortamlarına erişim haklarının verilmesi hallerinde, üçüncü taraf çalışanı Dış Kaynak Kullanıcıları Bilgi işlem Güvenlik Prensipleri'ni imzalar.
- Destek hizmeti kapsamındaki üçüncü tarafların görev ve sorumlulukları ile aşağıdaki hususlar sözleşmelerde açık bir şekilde tanımlanır:
- Hizmet seviyesine ilişkin tanımlamalar
- Hizmetin sonlanma koşulları
- Perform Portföy Yönetimi A.Ş. 'ye ait İş Süreklilik ve Acil Durum Planı'nın sekteye uğramasını engelleyecek şekilde üçüncü tarafın alması gereken önlemlere ilişkin hükümler
- Perform Portföy Yönetimi A.Ş. 'nin güvenlik politikası dahilinde hassasiyet arz eden konulara ilişkin gereklilikler
- Sözleşme kapsamında üretilecek olan ürünün sahipliğini, fikri mülkiyet haklarını da göz önünde bulundurulmasını düzenleyen hükümler
- Sözleşmede üçüncü taraflar için yükümlülük teşkil eden hükümlerin, alt yüklenici kuruluşlar ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler
- Üçüncü taraflardan hizmeti alımının, planlananın dışında sonlanmasından veya kesintiye uğramasından kaynaklanacak risklerin yönetilmesine ilişkin hükümler
- Perform Portföy Yönetimi A.Ş. 'nin tabi olduğu mevzuat hükümlerinin alınan hizmet çerçevesinde üçüncü taraflar için de uygulanmasını sağlayacak hükümler
- Üçüncü taraflara yetki "en az erişim ayrıcalığı" ve "bilgi ihtiyacı" prensiplerine göre verilir. Buna göre, üçüncü taraflara tanımlanan yetkiler ilgili kişilerin istenilen işi yapmasına yetecek kadar bilgiye erişim hakkını sağlamalıdır.
- Üçüncü taraflara erişim önceden belirlenen bir süreyle verilir. Verilen süre sonunda yetkinin kaldırılmasından, yetki talebinde bulunan ve yetkiyi tanımlayan birim sorumludur . Süre sonunda bağımsız olarak yetkiyi tanımlayan birim 3 ayda bir sistem üzerindeki tanımları kontrol etmekle yükümlüdür.
- Aşağıdaki durumlarda risk değerlendirmesinin yeniden yapılması gerekir:
- Kanun, tebliğ ve yönetmeliklerin süreci etkileyecek şekilde değişmesi durumunda
- İş süreçlerinde değişiklik olması durumunda
- İşi yapan , veriye erişen üçüncü tarafın değişmesi durumunda
- Erişilen verinin içeriğinin ve veri sınıfının değişmesi durumunda
- Teknolojide yaşanan önemli değişiklikler sonrasında

Bu koşulların oluşması durumunda ilgili birimler veri sahibini ve Perform Portföy Yönetimi A.Ş. sistem yöneticisini bilgilendirmekle sorumludur. Veri sahibi, Perform Portföy Yönetimi A.Ş. sistem yöneticisi desteğiyle yukarıda belirtilen durumlarda risk değerlendirmesini tekrarlar.

Gerekiyorsa yeni kontroller, önlemler Perform Portföy Yönetimi A.Ş. sistem yöneticisi ve işin sahibi birim tarafından uygulamaya alınır, üçüncü taraf ile yapılan sözleşmeler güncellenir.

5.6.6 Denetim İzleri

- Üretim ortamlarına erişen veya üretim ortamlarına ait veriyle test yapan tüm Perform Portföy Yönetimi A.Ş. kullanıcılarının ve üçüncü taraf faaliyetlerinin makul içeriğe sahip, anlaşılır , yönlendirici ve uyarıcı denetim izi tutulur. Denetim izlerinin aşağıdaki bilgileri sağlaması esastır:
- Kullanıcı oturumu aktivitesi - kullanıcı adı, oturum açma, işlem gerçekleşme , oturum kapatma tarih ve zamanı ve çalıştırılan uygulamalar
- İstemci bilgisayarın kendine has kimliği (IP No, bilgisayar adı, MAC-1D vb.)
- İşlem tipi, fonksiyonu
- Başarısız erişim denemelerine ait uyarı mekanizmaları
- Uygulama bazında riskli olarak belirlenen işlemlere , bilgilere ait uyarı mekanizmaları
- Kritik uygulamalardaki sistem dosyalarında yapılan değişiklikler
- Kullanıcıların ayrıcalıklarında yapılan eklemeler ve değişiklikler
- Sistem başlangıçları ve kapanmaları
- Hassas hareketler/işlemler (transaction)
- Tüm başarılı ve başarısız oturum açma denemeleri
- Kaydedilen denetim izleri SPK Mevzuatı uyarınca saklanır. Buna göre kaydedilen denetim izlerinin;
- Yetkisiz erişimlerden korunması,
- Bütünlüğünün sağlanması,
- Yedeklerinin alınması ,
- İlgili kanun ve tebliğlerin uygulanabilir olmadığı durumlarda asgari olarak 5 sene saklanması gereklidir.
- İç kontrol ve denetim faaliyetlerinden sorumlu birimler ihtiyaç durumunda denetim izlerini kontrol eder.

5.6.7 Temiz Masa

- Müşterilerin Perform Portföy Yönetimi A.Ş. hakkında olumlu imaj oluşturmasına yardımcı olmak için masalar temiz tutulmalıdır.
- Çok gizli ve gizli bilginin kullanılmadığı sürece erişimi kontrol edilecek şekilde saklanması güvenlik risklerini azalttığı için gereklidir.
- Çok gizli ve gizli bilgi içeren dokümanlar çalışma masasından uzak bulunulan durumlarda kilitli çekmecelerde saklanmalıdır.
- Gün sonunda masalar düzenlenmeli, tüm ofis kağıtları kilitli çekmeceler ve dolaplar içine konulmalıdır. Tüm çalışanların masaların temizlenmesi için zaman ayırması beklenmektedir.
- Çok gizli ve gizli bilgi içeren bir dokümanın kopyasının saklanması konusunda emin olunamazsa doküman kağıt imha makinesinde parçalanmalı veya parçalanmış olarak

çöpe atılmalıdır.

- Kağıda basılı dokümanların taranarak elektronik olarak saklanması mümkündür.
- Çok gizli ve gizli bilgi içeren dokümanlara belirli bir tarihten sonra ihtiyaç duyulmaması durumunda dokümanlar imha edilmelidir.
- Gün sonunda çekmece ve dolaplar kilitlenmelidir.
- Dizüstü bilgisayar veya cep telefonu gibi taşınabilir bilgi işleme cihazları kilitli dolaplarda saklanmalıdır.
- CD, DVD, USB bellek gibi depolama cihazlar çok gizli ve gizli bilgi içeriyor olarak değerlendirilmeli ve kilitli çekmece veya dolaplarda saklanmalıdır.

5.6.8 Ortak Dosya Alanları Kullanım Prensipleri

Perform Portföy Yönetimi A.Ş. BT'nin ortak dosya alanlarıyla ilgili sorumlulukları aşağıda belirtilmiştir.

- Perform Portföy , çalışanlarının iş amaçlı bilgi, belge saklamak ve 10 mb'dan büyük dosyaların şirket içerisinde paylaşımlarını güvenli bir ortam üzerinden sağlayabilmeleri için ortak dosya alan hizmeti sunmaktadır. Ortak alan, sadece ilgili departman üyelerinin erişebileceği şekilde yetkilendirilerek departman özelinde klasörler yaratılmıştır. Bilgiler ortak alanda veya aynı görev tanımına sahip başka bir kullanıcının bilgisayarında saklanabilir. Bu durumda dosyalara sadece ilgililerince erişilebilmesine yönelik gerekli paylaşım yetkileri düzenlenir.
- Her bir iş birimi, bölüm ve alt grup için klasör yaratılır.
- Dosya alanının ihtiyaçları karşılaması için iş birimlerinin talepleri doğrultusunda gerekli kaynak ve artırım planlanır.
- Yetkilendirme prensipleri aşağıdaki gibi sağlanır :
- İş Birimi seviyesindeki klasöre Genel Müdür Yardımcısı ve Genel Müdür Yardımcısı 'na doğrudan bağlı bulunan çalışanlar erişir. Genel Müdür Yardımcısı ayrıca iş birimi altındaki tüm klasörlere erişim için yetkilidir.
- Her bölüm çalışanı kendi bölüm klasörüne erişir. Bölüm Genel Müdür Yardımcısı , Başkanı ve Müdürü bölüm klasörü altındaki tüm klasörlere erişim için yetkilidir.
- Her bir alt grup çalışanı kendi alt grup klasörüne erişir. Her alt grup çalışanı grup altındaki tüm klasörlere erişim için yetkilidir.
- Klasör adı, birim kodu ve birim adının birleşiminden oluşur.
- Ortak dosya alanlarında 10 yıl boyunca erişilmeyen dosyalar silinmek üzere arşivlenir. Arşivlendikten sonra 1 yıl içinde talep edilmeyen dosyalar silinir.

Çalışanların aşağıdaki konulara dikkat etmesi gerekir:

- Tüm veri yedeklemeleri Perform Portföy Yönetimi A.Ş. ortak dosya alanlarına yapılmalıdır. Bu alanlar haricinde yedekleme yapılamaz.
- Ortak dosya alanlarında kişisel müzik, resim ve video dosyaları saklanamaz.
- Veri alışverişlerinin ilgili dosya alanları üzerinden yapılmasına özen gösterilir.
- Ortak dosya alanında kısıtlı sayıda kişinin erişilmesi istenen dosyalara açılış şifresi

konulmalıdır.
Ortak dosya alanları, departman klasörleri ve özel talebe istinaden açılan sınırlı yetkili klasörler dışında, 4 haftalık periyotlarla geri dönülemeyecek şekilde BT tarafından silinir.

5.6.9 Politika Uyum Denetimi

Perform Portföy Yönetimi A.Ş. Bilgi Güvenliği Sorumlusu bilgi güvenliği politikasının uyumunu denetler ve denetim sonuçlarını Yönetim Kurulu 'na en az yılda bir kez raporlar.

VERSIYON KONTROLU

Bu Prosedür, 02/01/2022 tarih itibari ile yürürlüge girmistir.

Versiyon	Tarih	Düzenleyen	Degisiklik Ozeti
1	02.01.2022		Doküman olusturulmustur.
2	02.01.2024		Değişiklik yapılmamaıştır.