ARZ PORTFÖY

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ PROSEDÜRÜ

İÇİNDEKİLER

I. AMAÇ

ISO 27001 standardının ve Bilgi Güvenliği Yönetim Sistemi Prosedürü'nün amacı, bilgilerin, gizliliğini, bütünlüğünü ve erişilebilirliğini korumak, sürdürmek, riskleri değerlendirerek uygun önlemleri almak ve yönetmektir.

II. KAPSAM

Gayrimenkul ve girişim sermayesi portföylerinin yönetimi, fon şirketlerinin yönetimi, yatırımcı ilişkileri, şirket içi mali ve idari tüm süreçler kapsam dahilindedir. ISO 27001:2017 standardına göre EK.A'da hariç tuttuğumuz maddelerimiz A.9.4.5, A.10.1.1, A.10.1.2, A.11.1.6, A.12.1.4, A.14.1.2, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1, A.18.1.5'dir.

TANIMLAR

Kullanıcı: Yönetim Kurulu Üyeleri, tüm tam/yarı zamanlı, süreli/süresiz sözleşmeli çalışanlar, danışmanlar, stajyerler ve üçüncü taraf hizmet sağlayıcılarını kapsar.

Üst Yönetim: Yönetim Kurulu ve Genel Müdür'den ibarettir.

Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve erişilebilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar.

Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da süreçlere erişilebilirliğini kısıtlama ya da açıklanmama özelliğidir. Önem taşıyan bilgilere yetkisiz erişimlerin önlenmesidir.

Bütünlük: Bilginin doğruluk ve bütünlüğünün sağlandığının gösterilmesidir.

Erişilebilirlik: Yetkisi olanların gerektiği hallerde bilgiye ulaşabilirliğinin gösterilmesi ilgili sistem standartları, sadece elektronik ortamda tutulan verilerin değil, yazılı, basılı, sözlü ve benzeri ortamda bulunan tüm verilerin güvenliğini kapsar. Standart, firma ölçeği, sektör, iş süreçlerinin farklılığı gibi konulara bakılmaksızın bütün kuruluşlar için uygulanabilir özelliktedir.

Gizli Bilgi: Yukarıda bahsedilen tanımlarla sınırlı kalmamakla birlikte aşağıda sunulan bilgiler "Gizli Bilgi" kapsamında değerlendirilir:

- Halka henüz açıklanmamış mali performans ve sonuçlar,
- Şirketin stratejik ve taktik planları,
- Geleceğe dönük yatırım planları,
- Üst Yönetim kararlarıyla ilgili bilgiler,
- Fon ve yatırım süreçleri ile ilgili bilgiler,
- Kullanıcı adı ve parolalar,

- Tercih edilen veya özel fiyatlandırma / tarifeler,
- Bilgi sistemleri / ağ mimarisi ve ilgili dokümantasyon,
- Medyada manşet haberi haline gelebilecek bilgiler,
- Mevcut, potansiyel ve aday konumundakiler dâhil yatırımcılara ait her türlü bilgi,
- Şirketin çözüm ortakları ve hissedarları ile ilgili her türlü işbirliği bilgisi ve çözüm ortaklarına ait bilgiler,
- Muhasebe birimi sorumluluğundaki mevcut çalışan ve / veya işten ayrılan kişilerin bilgileri (şahsi bilgiler, ücret, bordro, sözleşme vb.),
- Organizasyonel yapı (organizasyon şeması, terfi, kademe, kazanç grubu vb.),
- Şirket içi personel ile ilgili tutulan bilgiler (performans yönetimi, ücret yönetimi vb.)

BGYS Temsilcisi: Bilgi Güvenliği Yönetim Sistemi Temsilcisi, Üst Yönetim'in atadığı, bilgi güvenliği sisteminin yönetimi için Bilgi Güvenliği Komitesi çalışmalarını koordine etmekten sorumlu kişidir.

Bilgi Sistemleri Firması: Arz Portföy'ün bilgi sistemlerinin yönetimi için dışarıdan sözleşmeli destek aldığı firmadır.

Bilgi Güvenliği Komitesi: Bilgi Güvenliği ile ilgili kritik kararlarının görüşülmesi, değerlendirilmesi ve onaylanması amacıyla kurulmuş olan ve üyelerinin Üst Yönetim tarafından belirlendiği komitedir.

Çalışan: Arz Portföy bu politika hükümlerine tabi çalışanı ile kurum sistemlerine bağlanan danışman, stajyer, çözüm ortağı, dış kaynak statüsündeki kullanıcılar.

Varlık: Bir kurum için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır (İnsan, bilgi, yazılım, donanım, bina, iş araçları ve iş gereçleri gibi kurum için değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir).

III. SORUMLULAR

Tüm Arz Portföy çalışanları bu prosedür ve diğer ISO 27001 prosedürlerinde belirlenen kurallara uygun davranmaktan sorumludur. Ayrıca tüm yöneticiler, yönetici oldukları bölüm/birimlerde bu politikanın uygulanmasını sağlanmaktan sorumludur.

Bilgi sistemlerini kullanarak veya doğrudan bilgiye erişen tüm çalışanlar, danışmanlar ve hizmet alınan iş ortaklarımız gizlilik sözleşmesinde yer alan sorumlulukları kabul eder ve imzalarlar.

Bilgi Güvenliği Komitesi

Arz Portföy üst yönetimi tarafından, bilgi güvenliğinin iç organizasyonunun sağlanması için teknik, idari ve hukuki süreçlerde çalışmalarda bulunmak ve BGYS'nin kurum içinde uygulanmasını sağlamak ve denetlemek üzere "Bilgi Güvenliği Komitesi" oluşturulmuştur.

Komite üyeleri;

- BGYS Temsilcisi,
- Mali ve İdari İşler Müdürü,
- Muhasebe Müdürü

Komitenin görevleri;

- Bilgi güvenliği politika ve stratejilerini belirler,
- Bilgi güvenliği ile ilgili gerekli dokümanların hazırlanması için çalışmalar yürütür, BGYS kapsamında hazırlanan dokümanlarla ilgili revizyon kararlarını verir,
- Bilgi güvenliği politikalarının uygulamasının etkinliğini gözden geçirir,
- Bilgi güvenliği faaliyetlerinin yürütülmesini yönlendirir,
- Bilgi güvenliği ile ilgili eğitim ihtiyaçlarını belirler, gerekli eğitim programı hazırlar ve farkındalığını sağlamak için gerekli faaliyetleri yürütür,
- Bilgi güvenliği faaliyetleri ve kontrollerinin tüm kurum ve kuruluşlarda koordine edilmesini sağlar.

Bu prosedürün işlevsel sahipliği BGYS Temsilcisi'nde olup her yıl en az bir defa düzenli olarak Bilgi Güvenliği Komitesinin ve diğer ilgili kişilerin katılımıyla gözden geçirilir.

IV. GENEL HÜKÜMLER

A. BİLGİ GÜVENLİĞİ POLİTİKALARI

1. GENEL POLİTİKALAR

Arz Portföy, kurumsal bilgiyi son derece değerli bir varlık olarak kabul eder. Bu nedenle bilgi ve bilgiyi barındıran iş destek sistemleri ile süreçleri önemlidir ve uygun şekilde korunmaları gerekir. Bilgilerin kaybolması, bozulması, iş için gerekli olmadığı halde 3. kişilere ifşası veya çalınması, şirket iş faaliyetlerinin bütünlüğü ve itibarı üzerinde ciddi bir etkiye sahip olabilir. Bu nedenle tüm Arz Portföy çalışanlarının, bilgi güvenliği ve yönetimi politikalarının bilincinde olmaları bir gerekliliktir.

- Arz Portföy'ün teknolojik ihtiyaçlarının, gelişen ve değişen dünya teknolojilerine uyumunu sağlamak amacıyla, değişim ve yenilikler sürekli takip edilir. Bilgi teknolojileri ve sistem altyapısı, iş süreçlerini destekleyecek ve iyileştirecek şekilde güncellenir.
- Bilgi güvenliği, tüm ilgili mevzuatlara (öncelikli olarak 30292 sayılı SPK Bilgi Sistemleri Yönetimi Tebliği), kanunlara ve ISO 27001 standardına uyumlu olarak tasarlanır, kurulur ve işletilir.
- Bilgi teknolojileri hizmet ve ürün alımlarında, kişisel / kısa vadeli çözümlerin yerine, sürdürülebilirliği yüksek ve kurumsal çözümler tercih edilir.
- Bilgi yönetimi yetkilendirme altyapısı ile çalışanların ihtiyaç duydukları bilgiye hızlı, düzenli ve kontrollü bir şekilde ulaşmaları sağlanır. Çalışanların ihtiyaç duymadıkları, erişmelerinin uygun olmayacağı bilgilere erişimleri ise engellenir.
- Kurumsal bilginin, bilinçli / bilinçsiz taşınması, çalınması, kaybedilmesi, bütünlüğünün bozulmasını önleyecek mekanizmalar oluşturulur ve siber tehditlerden korunması sağlanır. Oluşturulan sistemler, belirli dönemlerde güvenilir şirketler tarafından sızma testine tabi tutularak, güvenlik açıkları tespit edilir ve gerekli tedbirler alınır.

- Tüm çalışanların, bilgi sistemlerinde, ağ sistemlerinde ve internet üzerinde gerçekleştirdikleri işlemlerin kayıtları gerektiğinde erişilebilecek şekilde tutulur.
- Yatırımcılar, fon şirketleri, çözüm ortakları ve tedarikçilerle ilgili sahip olunan bilgiler, ticari sır kapsamında görülür ve bu bilgilerin gizliliğine özen gösterilir. Çözüm ortakları ve tedarikçilerden de Arz Portföy ile ilgili sahip oldukları bilgileri gizli tutmaları istenir. Ticari sır kapsamındaki bilgi paylaşımının olduğu müşteri ve tedarikçiler ile yapılan sözleşmelerde, bilgi güvenliğine ilişkin müeyyide ihtiva eden maddelere yer verilir.
- Tüm çalışanlar, tanımlı yetkileri dahilinde Arz Portföy bilişim teknolojileri kaynaklarını kullanma hakkına sahiptir. Tüm çalışanlar gizlilik ve güvenlik ile ilgili kurallara uymak sorumluluğundadırlar.
- Arz Portföy'de kullanılan tüm yazılımlar, telif hakkı kanunlarına uymak durumundadır. Lisanssız yazılım kullanılmaz. Şirket tarafından lisanslanmış ya da şirkete ait yazılımlar izinsiz çoğaltılamaz, kopyalanamaz, iletilemez ve barındırılamaz.
- Arz Portföy bilgilerini ve bilgi sistemlerini kullanan çalışanlar, kişisel ve elektronik iletişimlerinde, şirkete ait bilgilerin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanmasından; kullanıcı hesaplarının ve şifrelerinin güvenliği ve gizliliğinden; ayrıca sahibi oldukları kullanıcı hesapları üzerinden gerçekleştirdikleri tüm işlemlerden sorumludurlar.
- Çalışanların bilgi güvenliği farkındalığını arttırmak, görev ve sorumluluklarını tanımlamak amacıyla, gerekli dokümantasyon ve sistemler oluşturulur. Oryantasyon ve bilgilendirme programlarıyla çalışanların eğitimi gerçekleştirilir. Çalışanlarda bilgi güvenliğinin korunması bilincinin oluşması açısından kendilerine bilgi güvenliği taahhüt formları imzalatılır.
- Arz Portföy Yönetimi, Bilgi Güvenliği Politikası doğrultusunda, çalışanlarının Bilgi Güvenliği konularıyla ilgili farkındalık eğitimleri almalarını temin eder ve politikayla uyumu sağlar.
- Gizli Bilgi'ye yönelik ihlallerde Üst Yönetim, Bilgi Güvenliği Komitesi'nin de görüşünü alarak mevzuata uygun olarak konuyu ele alır ve değerlendirir.
- Mevzuat ve/veya bilgi güvenliği süreç/gereksinimlerinde değişiklikler olması durumları da politikanın gözden geçirilmesini gerektirir.
- Ayrıca uygun sistem ve araçlar kullanılarak, bu ve diğer Bilgi Güvenliği politikalarına uyum izlenir; uyulmaması durumunda üst yönetime bilgi verilerek, bu politikalara uyulması için gerekli önlemler alınır.

Arz Portföy bilgilerini ve/veya Arz Portföy bilgi sistemleri altyapılarını kullananlar;

- Bu prosedür ile birlikte Arz Portföy'e ait diğer Bilgi Güvenliği politika ve prosedürlerini öğrenmek ve bunlara uymak,
- Kişisel ve elektronik iletişimde şirkete ait bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak, kullanıcı hesaplarının, şifrelerin, erişimlerin ve yetkilerin kullanımına, güvenliğine ve gizliliğine özen göstermek,
- Risk düzeylerine göre belirlenen güvenlik önlemlerini almak,
- Bilgi güvenliği ihlal olaylarını raporlamak ve bu ihlalleri engelleyecek önlemleri almak,
- Şirket içi bilgi kaynaklarını (duyuru, doküman vb.) yetkisiz olarak 3. kişilere iletmemek,
- Şirket bilgi sistemleri altyapılarını, mevzuata aykırı faaliyetler amacıyla kullanmamak,
- Arz Portföy yatırımcıları, iş ortakları, tedarikçiler veya diğer üçüncü kişilere ait bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak

sorumluluğundadır.

2. TEMİZ EKRAN - TEMİZ MASA POLİTİKASI

Her Arz Portföy kullanıcısı hassas bilgi içeren varlıklarla çalışması bittiğinde ya da çalışmaya ara verdiğinde bir başkasının yetkisiz olarak bu varlığa erişmesini engellemek için aşağıdaki konulara dikkat eder;

- Çok Gizli / Gizli olarak tanımlanmış tüm dokümanlar ve hassas elektronik bilgi barındıran depolama ortamları (harici disk, USB disk, hafıza kartı vb.) kullanılmadığı zamanlarda, özellikle de çalışma saatleri dışında açıkta bırakılmaz, bırakılması zorunlu olan durumlarda da uygun kilitli dolapta veya çekmecede saklanır.
- Şirkette veya diğer paydaşlarımızda gerçekleştirilen çalışmalar sonrasında, çalışma ortamından (toplantı odası, ofis vb.) ayrılırken, geride hiçbir hassas bilgi bırakılmadığından emin olunur (beyaz tahtanın silinmesi, ortamdaki yazılı kâğıtların toplanması vb.).
- Kişisel bilgisayarların başından ayrılırken ekran koruyucuların devreye girmesi için gereken zaman beklenmeden her defasında mevcut oturum kilitlenir (Windows Tuşu + L). Bu amaçla bilgisayar kullanılmadığında kısa süre içerisinde tekrar parola isteyecek şekilde ayarlamalar yapılmıştır.
- Hassas bilgi içeren bir varlığın teslim edilmesi gerektiğinde, kişinin kendisine teslim edilir, ilgili kişinin yerinde olmaması durumunda bırakılan varlığın güvenli olarak ulaştırılmasına dikkat edilir.
- Basılı doküman üzerinde ya da bilgisayarda çalışılırken, hassas bilginin başkaları tarafından görülmemesi için "bilgileri masa veya herkesin erişebileceği masaüstü raflar üzerinde bırakmamak, kapaklı dosyada taşımak, ekranı – sürekli olarak – kimsenin rahatça göremeyeceği şekilde konumlandırmak" gibi önlemler alınır.
- Bilgisayar masaüstü de çalışma masası gibi temiz tutulur, sunucudaki ilgili klasörüne yerleştirilmemiş dosyalar geçici veya taslak dosyalar dışında bulunmaz.

3. İLETİŞİM VE GİZLİLİK POLİTİKASI

Arz Portföy kendi içinde işlerini sürdürmeye ve geliştirmeye yönelik bir iletişim sistemini muhafaza eder. Arz Portföy'de örgütsel iletişimin başarısının çalışan başarısını, çalışan başarısının da kurumun başarısını beraberinde getireceği bilinir. İletişimin yazılı olması esastır. Yazışma ve konuşmalarda üslûbun açık, net, kesin ve yanlış anlamalara fırsat vermeyecek biçimde olmasına dikkat edilir.

Arz Portföy dışına yönelik haberleşmede, Arz Portföy çalışmaları ve ilişkileri hakkındaki bilgiler, tüm paydaşlar, aile ve arkadaşlar da dâhil olmak üzere ilgisiz kişilere hiçbir zaman verilmez. Kanunî veya hiyerarşik olarak haberi olması gereken kişilere de, gerekenin dışında bilgi aktarılmamasına özen gösterilir. Özellikle Arz Portföy mensupları rakiplerle iletişim kurarken hiyerarşik olarak bir üst âmiriyle konuyu paylaşmalıdır.

Arz Portföy'e ait kanunî defterlerin, diğer tüm bilgilerin ve belgelerin dışarıya karşı kesinlikle kapalı ancak yetki verilen (yetki sınırları Yönetim Kurulu tarafından çizilmek kaydı ile) denetçi, danışman vb. kimselere açık olmasına her bir Arz Portföy çalışanı özellikle dikkat etmelidir.

Her bir Arz Portföy çalışanı kurum dışarısıyla iletişimi kurumun kendisine sağladığı imkânlar doğrultusunda sağlar. Kişisel telefon ve e-posta adreslerinden kurumla ilgili görüşme ve yazışmaların yürütülmemesi esastır.

Kullanıcı bilgisi ve parolası girilerek erişim sağlanabilen program ve yazılımlara her çalışan kendi bilgileriyle giriş sağlamalı, çalışmalarını kendi hesabı üzerinden yürütmelidir.

Arz Portföy mensuplarının, Arz Portföy ile ilgili vereceği bilgi ve görüş, yalnızca kurum itibarına hizmet edecek olumlu, saygılı, nazik, dikkatli, yardımcı, iyi niyetli ve disiplinli yaklaşım ve mesajları içermelidir.

4. KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

Arz Portföy'de kişisel verilerin işlenmesi, mahremiyeti ve güvenliği ile ilişkili tüm hususlarda gerekli hassasiyeti göstermek temel prensiplerimizdendir. Bu anlamda her türlü kişisel verilerin, Kişisel Verilerin Korunması Kanunu'na uygun olarak işlenmesine, kaydedilmesine, aktarılmasına, paylaşılmasına ve saklanmasına önem verilmektedir ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi kalite standartlarında çalışmalar yürütülmektedir.

Arz Portföy faaliyet alanı içerisinde gayrimenkul ve girişim sermayesi yatırım fonlarının muhtemel ve mevcut yatırımcılarının yatırımcı profillerinin değerlendirilebilmesi, yatırım süreçlerinin gerçekleştirilebilmesi, ilgili resmi ve özel kuruluşlara gerekli bilgilendirmelerin yapılabilmesi ve hizmet sunum aşamasında etkin iletişim kurulabilmesi amaçları ile aşağıdaki kişisel veriler;

- Yatırımcıların kimlik, iletişim, varlıklarının/borçlarının bilgisi,
- Kullanılan finansal ürünlere ve yatırım alışkanlığına ilişkin bilgiler,
- Finansal ürünlere erişimde kullanılan yöntemlere ilişkin bilgiler

Arz Portföy tarafından temin edilmekte ve işlenmektedir, işlenen bilgiler hizmet sürecinde işbirliği yapılan çözüm ortakları ve resmi kurumlar ile paylaşılabilmektedir.

Ayrıca çalışanlar ile ilgili bilgiler personel bilgi sistemine aşağıdaki kategorilerde kayıt edilir;

- Çalışanların özlük (sabıka kaydı, sağlık raporu, ikametgâh, aile, kimlik vb.) bilgileri,
- Çalışanların özgeçmiş (eğitim, önceki tecrübe bilgileri, referans vb.) bilgileri,
- Çalışanların iletişim bilgileri,

Çalışanın kişisel verileri, kişisel veri işleme şartları ve amaçları çerçevesinde işveren – çalışan ilişkisinin düzenli bir şekilde işletilmesi ve işverenin sözleşme ve yasadan doğan mesuliyetlerini eksiksiz ve doğru bir şekilde yerine getirebilmesi amacı ile işlenebilecek, arşivlenebilecek ve gerekli durumlarda kamu kurumlarına veya mali müşavirlik, sağlık kurumları vb. özel kurumlara aktarılabilecektir.

Bu kapsamda alınan kişisel ve özel nitelikli kişisel veriler, Arz Portföy'ün sahip olduğu yasal yükümlülükleri yerine getirmesi ve iş ilişkisinin sağlıklı şekilde yürütülmesi amacıyla 6698 sayılı Kişisel Verilerin Koruma Kanunu'nda belirtilen kişisel veri işleme şartları ve amaçları dahilinde işlenmektedir.

Kişisel veriler, yukarıda belirtilen mevzuatlar veya işlendikleri amaç için gerekli olan ve herhalde kanuni zaman aşımı süreleri kadar muhafaza edilecektir. Yukarıda belirtilen amaçlar için 3. kişi ve kurumlar ile veriler paylaşıldıktan sonra verilerin güvenliği Arz Portföy'ün kontrolünde değildir, Arz Portföy söz konusu kurumlar adına herhangi bir taahhütte bulunmaz ve sorumluluk kabul etmez.

Gerek yatırımcılardan gerekse de çalışanlardan bu kapsamda muvafakatleri alınarak yatırımcı ve personel özlük dosyalarına yerleştirilir. **(F.BY.17 KVKK Yatırımcı Muvafakatnamesi, F.BY.18 KVKK Çalışan Muvafakatnamesi)**

5. ŞİFRE POLİTİKASI

Bu politikanın amacı, bilişim sistemlerinde veya çözüm ortağı / tedarikçi / kamu / finans kurumları sistemlerinde kullanılan şifrelerin, seçim kriterlerinin, koruma ve değiştirme periyotlarının belirlenmesidir.

Bu politika, kurumun bilişim sistemlerinde kullanıcı hesabı olan veya kullanıcı hesaplarından sorumlu olan, kurum dâhilinde veya haricinde şifre gerektiren veya şifre ile çalışabilen herhangi bir sisteme erişimi olan, kurumun bilgisayar ağına veya kurum hakkında gizli/özel bilgilerin saklandığı birimlere erişimi olan bütün çalışanlara uygulanır.

Kullanıcı parolalarının gizliliği çalışanların kendi sorumluluğundadır. Parolalar kişisel kullanım amaçlı olup şirket içi veya dışı hiç kimse ile kesinlikle paylaşılmaz, bir şekilde parolanın açığa çıktığından şüphe duyan çalışan parolasını anında değiştirir. Kişisel hesabın başkaları tarafından kullanılmasına izin verilmez.

Arz Portföy'de onay veya yetki gerektiren şifreler **F.BY.14 Kurumsal Şifre Envanteri'nde** belirtilmiş olup, belirtilen şifreler ilgili çalışanlara **F.BY.15 Kullanıcı Şifre Zimmet ve Taahhüt Formu** ile zimmetlenir.

a) Şifre Seçimi

Şifre seçiminde aşağıdaki hususlara **dikkat edilir**;

- Kullanıcılar tahmin edilmesi güç şifreler seçmelidir.
- Şifreler kişinin işiyle veya kişisel yaşamıyla ilişkili olmamalıdır.
- Özel isimler, yer isimleri, teknik terimler, kullanılan bilgisayarın markası ve argo deyimler kullanılmamalıdır.
- Kullanıcılar şifre oluştururken, aşağıdaki 3 farklı gruptan en az birer adet karakter içeren ve en az 6 karakterli şifreler oluşturmalıdır:
  - Büyük Harfler {A..Z}
  - Küçük Harfler {a..z}
  - Karakter{*-.}

Aşağıda bu kapsamda uygulanabilecek **örnek** yöntemler verilmiştir;

- Birkaç sözcüğü bir araya getirerek (passphrases), (Örn: güzel bir gün yerine G^zel-1-g^n)
- Bir sözcüğü, klavyede bir üst veya bir alt satıra, sola veya sağa kaydırarak, (Örn: Fıratww! yerine T95w633!)
- Bir sözcükteki karakterlerin yerine, alfabede bunlardan belli bir sayı önce veya sonraki karakterleri koyarak, (Örn: Bülent11 yerine bir sonraki harfler olan Cvmfou22)
- Normal bir sözcüğü belli bir yönteme göre değiştirerek, örneğin, sözcük içindeki her iki harften biri yerine sözcük içindeki konumlarını yansıtan bir rakam koyarak, (Örn: s yerine $, i yerine 1 (bir), a yerine @ kullanarak)
- Normal bir sözcüğü noktalama işaretleri veya rakamlarla birleştirerek,
- Bir sözcüğü bilerek yanlış yazarak, (yaygın olarak yapılan bir hatalı yazım olmamak kaydıyla)

- Kolay hatırlayabileceğiniz cümlelerin baş harflerini büyük küçük harf kombinasyonu ile birleştirerek şifre oluşturabilirsiniz. (Örn:"Bizim sitede 1221 apartman var" cümlesinden "Bs1221Av)

Yukarıda kullanılan örnekler aynen kullanılmamalıdır.

Şifre oluşturulurken aşağıdakiler **yapılmamalıdır**:

- Alfabetik serilerden oluşmamalıdır. (Örn: ABCDEFGH ya da hgfedcba)
- Numerik serilerden oluşmamalıdır. (Örn: 12345678 veya 87654321)
- Tümü aynı karakterlerden oluşmamalıdır. (Örn: QQQQQQQ veya 11111111)
- Klavyede yer alan tuş dizilerinden oluşmamalıdır. (Örn: qwertyui ya da ASDFGUI)
- İsminiz, kullanıcı kodunuz ya da benzer kolay hatırlanabilir özelliklerden ya da bunların değişik kombinasyonlarından oluşmamalıdır. (Örn: admin, user gibi)
- Sözlüklerde yer alan herhangi bir kelime olmamalıdır. (Örn: armut, kolonya gibi)
- Türkçe karakter kullanılmamalıdır.

b) Şifrelerin Gizliliği

Seçilen şifrelerin gizliliği ve güvenliğinin sağlanması için aşağıdaki hususlara dikkat edilir:

- Şifre anonim olarak hiçbir yere yazılmamalı, hiç kimse ile paylaşılmamalıdır.
- Farklı sistemlerdeki kullanıcı hesapları için farklı şifreler kullanılmalı, dış sitelerde (internette üye olunan siteler) kullanılan şifrelerden farklı olmalıdır.
- Sunucu (domain) hesapları kişiye özel olduğu için çalışan kendisine ait kullanıcı adı ve şifre ile sistemlere giriş yapmalıdır. Başkasının kullanıcı adı ve şifresi kullanılmaz.
- Çalışan bazında kullanıcı oluşturulabilen tüm sistemlerde her yetkili çalışan için ayrı kullanıcı ve şifre oluşturulur.
- Kurumsal hesaplara ait şifrelerin e-posta yolu ile transferi tercih edilmemelidir. (Telefon konuşması, SMS içeriğinde iletilmelidir.) Eğer e-posta ile iletme zorunluluğu varsa şifre sadece alıcıya gönderilmelidir.
- Sunucu (domain) kullanıcı şifreleri ayarları aşağıdaki şekildedir;
  - En fazla 90 günde bir değiştirilmelidir. Şifre değiştirme uyarıları şifre süresinin dolmasına 12 gün kala sistem tarafından iletilir.
  - Şifre değişimlerinde son kullanılan 3 şifre yeniden kullanılmamalıdır.
  - Şifre geçerlilik tarihi dolduğunda sistem kullanıcıyı şifresini değiştirmesi için zorlamalıdır.
  - Yeni kullanıcılar kendisine tahsis edilen şifre ile sisteme ilk kez giriş yaptığında, sistem kullanıcıyı şifresini değiştirmesi için zorlamalıdır.
  - Kullanıcı şifre bilgilerini BGYS Temsilcisi veya Bilgi Sistemleri Firması bilmemelidir. Zaruri hallerde şifre sıfırlaması yapılması halinde ilk oturum açıldığında şifrenin değiştirilmesi istenmelidir.
- Tüm seviyedeki sunucu / domain yönetici şifreleri (Root, Domain Admin, Administrator vb.) yılda bir değiştirilmelidir. Sistem şifreleri ve değişen şifreler bir nüsha halinde kapalı zarf usulü Üst Yönetime teslim edilir.
- İşten ayrılan çalışanların şifreleri veya gizliliği ihlal edilen şifreler anında değiştirilir.

6. ÖZDENETİM VE İÇ DENETİM POLİTİKASI

- Her bir Arz Portföy çalışanı, genel prensiplerimize uyulmadığında hiyerarşik iletişim zincirine uygun olarak ilgilileri uyarmakla yükümlüdür. Bu husus, firmamızın sürekliliğinin sağlanması ve çalışanlarımızın mutluluğunun korunması için vazgeçilmezdir.
- Arz Portföy çalışanları olarak, hepimizin esas sorumluluklarından biri, öncelikle kendimizi bu prensipler doğrultusunda özdenetime tâbi tutarak düzeltmek ve geliştirmek, diğeri de yine dostluk, sevgi ve saygı ortamını muhafaza etmek kaydıyla, bu prensiplerin yaşamasını sağlamak ve uygulanmasını engelleyecek hareketlerin düzeltilmesi için gerekli desteği vermektir.
- Tüm çalışanlarımız şirket varlıklarını korumalı ve kaynakların ekonomik ve verimli kullanımını sağlamalıdır.
- "Değersiz / önemsiz iş yoktur" prensibiyle her kademede ve her görevin kendine özgü sorumluluğu ve önemi olduğunun bilinciyle Arz Portföy çalışanları yaptıkları çalışmaları Toplam Kalite anlayışıyla sürdürmelidir.
- Tüm uygulamalarımızın kanun ve kurallara, kurumsal anayasamıza, prosedürlerimize, yönetmeliklerimize, verimlilik ve performans kriterlerine uygun olması asıldır. Bunun denetlenmesi amacıyla iç ve dış denetim mekanizmaları uygulanır.
- Arz Portföy, kişisel ve kurumsal gelişime katkı ve zenginlik sağlayan, nitelikli hatalara önem ve değer veren bir kurumdur. Arz Portföy'de ihmal, suistimal, kötü niyet dışındaki hatalar, bu hatalara yol açan sistemsel ve eğitimsel engellerin ortadan kaldırılmasına ve gerekli noktaların düzeltilmesine olanak sağlar. Bu kapsamda, hatayı yapan kişiye eksiğini giderebilmesi için geribildirim ve gerekli destek kurumumuzca verilir. Verilen geribildirim ve desteğin, durumu olumlu yönde değiştirmemesi halinde kişi öncelikle uyarılır, daha sonra iç denetim mekanizması ve gerektiğinde de disiplin süreci başlatılır.

7. TEDARİKÇİ İLİŞKİLERİ POLİTİKASI

Arz Portföy için her türlü tedarikçi ve/veya (alt) yüklenici tarafından temin edilen mal ve yerine getirilen hizmetlerin sağlanmasında bilgi güvenliğini tehlikeye atabilecek alanlarda bilginin bütünlüğünün ve/veya gizliliğinin korunması, bilgi sistemleri altyapısının sağlıklı çalışması ve yürütülen her türlü iş ve işlemlerin sürekliliğinin sağlanması ön koşuldur.

- Tedarikçi ilişkilerini yönetmek için alınan mal ya da hizmetlerde her birim kendi risk eğilimini belirlemeli; bunu işletebilen, depolayabilen, iletebilen veya kurum bilgisi için bilgi teknolojileri altyapı bileşenlerine ulaşan her bir tedarikçi ile anlaşılmalı, her iki tarafın sorumlulukları kararlaştırılmalıdır.
- Tedarikçi sözleşmelerinde, tedarikçilerin bilgi ve iletişim teknolojileri hizmet ve ürün tedarik zincirleriyle ilgili bilgi güvenliği risklerine ilişkin gereksinimlerini ifade eden şartları içerecek şekilde yazılı halde dokümante edilmelidir. Tedarikçilerin alt yüklenici kullanması söz konusu olacağından kendi tedarikçi ilişkileri ile ilgili önlemleri almalı ve kontrolleri gerçekleştirmelidir.
- Tedarikçi ve/veya (alt) yüklenicinin kendisi ya da üçüncü kişiler (alt yükleniciler) tarafından bilgi güvenliği ihlali gerçekleştiğinde, ihlal durumunun Arz Portföy Yönetimine yazılı olarak bildirme yükümlülüğü teknik sözleşmeye eklenmelidir.

- Tedarikçi ve/veya (alt) yüklenici, mevzuatta (kanun, tüzük, tebliğ, genelge vb.) meydana gelebilecek yenilik ve değişikliklerin bilgi güvenliği uygulamalarında sebep olacağı farklılıklara uyum sağlaması zorunluluğunu teknik sözleşmeye eklemelidir.
- Yazılım tedarikçilerine verilen fiziksel ve mantıksal erişimlerin yönetim tarafından onaylanmış olması; periyodik olarak verilen erişim haklarının ve yetkilerinin kontrol edilmesi gerekir.
- Tedarikçi destek faaliyetlerinin ve tedarikçi personelinin sistem üzerinde çalıştırdığı komutların iz kayıtları tutulmalı, izlenmeli ve gözden geçirilmelidir.
- Tedarikçiler ile yapılan anlaşmalarda alınan hizmetle ilgili olarak güvenlik kontrol gereksinimleri, hizmet seviyeleri ve yönetim gereksinimleri belirtilmelidir.
- Tedarik edilen sistemlerin barındırdığı ihtiyaç duyulmayan fonksiyonlar değerlendirilmeli ve güvenlik riski oluşturacaklarına karar verildiğinde geçersiz hale getirilmelidir.
- Ürün ve hizmet tedarikçilerinin güvenli sistem mühendislik prensiplerini en az organizasyon seviyesinde uygulayıp uygulamadıkları denetlenmelidir.
- Yazılım geliştirme sırasında dış kaynak kullanımının gerekli olduğu durumlarda tedarikçi firmanın güvenli yazılım geliştirme kurallarının uyguladığından emin olunmalıdır.
- Tedarik edilen yazılımlar için yazılım geliştirme ve derleme ortamına ilişkin bilgilerin tedarikçi firma tarafından dokümante edilmesi ve tedarikçi firmadan teslim alınması sağlanmalıdır.
- Tedarikçi ilişkilerinde bilgilere erişecek tedarikçi personelin listesi veya erişim yetkilendirme ve yetki kaldırma maddeleri sözleşmede belirtilmelidir.
- Tedarikçi sözleşmelerinde tedarikçilerin periyodik olarak bağımsız iç kontrol denetim geçirmeleri ve raporlarını teslim etmeleri istenmelidir.
- Tedarikçi hizmetleri yönetim süreci, tedarikçilerin hizmet içerik ve kapasitesinin yeterliliğinden ve herhangi bir hizmet kesintisi veya felaket durumunda uygulanabilir iş sürekliliği planlarına sahip olduklarından emin olunmalıdır.
- Tedarikçi hizmetlerindeki değişiklikler, hizmet kapsamına giren sistem ve süreçlerin kritikliğine bağlı olarak, yeniden risk analizi yapılması suretiyle değişen bilgi güvenliği ihtiyaçları açısından yönetilmelidir.

B. BİLGİ YÖNETİMİ SÜREÇLERİ

1. BİLGİ VE İLETİŞİM SİSTEMLERİ KULLANIMI

Arz Portföy'e ait bilgi, haberleşme sistemleri ve donanımları (internet, e-posta, telefon, faks, bilgisayar, mobil cihaz, vb.) sadece şirketle ilgili işlerin yürütülmesi için kullanılır. Yasa dışı, rahatsız edici veya şirketin diğer politika, prosedür ve standartlarına aykırı olarak kullanılmaz.

Şirket dışında (restoran, kafeterya, park vb.) mobil cihaz (telefon, tablet, dizüstü bilgisayar vb.) kullanılırken, gizli bilgilerin paylaşılmasından ve kullanılmasından kaçınılır.

Mobil cihazlar gözetimsiz bir şekilde ortada bırakılmaz, taşıma ve kullanım sırasında ilgisiz kişiler tarafından gözleme ve / veya çalınmaya karşı güvenlik önlemleri alınır ve güvenli bir yerde bırakılması durumunda bilgilere ulaşılmasını engelleyecek tedbirlerin alınması sağlanır.

İletişim sistemleri kullanımı ile ilgili tanımlanmış teknik kurallar, aşağıda yer alan politika ve prensiplere uygun olarak hazırlanmış sistem kontrolleri **P.BY.03 Bilgi Teknolojileri Alt Yapı Yönetim Prosedürü'nde** yer almaktadır.

a) Bilgisayar Kullanımı

- Bilgisayarlar ve tüm elektronik cihazlar iş çıkışlarında kapatılmalıdır; yemek aralarında veya 10 dakikadan fazla boş kalacak olmaları durumunda kapatılmalı veya bekleme durumuna alınmalıdır. Bilgisayarlar ve çevre cihazları jeneratöre bağlı prizlere takılmalıdır. Kullanıcı bilgisayarlarında kesintisiz güç kaynağı bağlantısı bulunmadığından dolayı dizüstü bilgisayarlar tercih edilir. Masaüstü bilgisayar tercih edilmesi halinde ise küçük UPS cihazları ile bilgisayarın aniden kapanmasının önüne geçilir.
- Arz Portföy'de kullanılan tüm yazılımların lisanslı olarak yüklemesi Bilgi Sistemleri Firması tarafından gerçekleştirilir. Lisanssız yazılım kullanılmamasından aynı zamanda kullanıcılar da sorumludur.
- Arz Portföy'ün hizmet verdiği ve faaliyet gösterdiği alanlarda katma değer üretmeyecek program/kod/eklentiler bilgisayarlara yüklenemeyeceğinden dolayı yükleme isteğinde bulunulmamalıdır.
- Arz Portföy'deki bilgisayarların sistemlerine (yazılım ve donanım) ve birimlerine yetkili kurum dışında kimsenin müdahale hakkı yoktur. Şirket bilgisayarları Güvenlik Duvarı Donanımı ve Virüs Yazılımı tarafından korunmaktadır, USB flashdisk ve diğer dosya taşıma cihazları tanınmamaktadır, DVD/CD okuyucular bilgisayarlarda engellenmiştir, yazıcı bağlantıları sadece Arz Portföy yazıcılarına izin verecek şekilde kısıtlanmıştır ve internet kullanımına uygun olarak internet protokolleri düzenlenmiştir. Bu düzenlemeler tüm çalışanların bilgisayarları için geçerlidir ve ancak yetkili kişi tarafından değiştirilebilir, kişiye özel uygulama bulunmamaktadır ve iş için zaruri olmadığı durumlarda talep edilmemelidir.
- Çalışanlar şahsi bilgisayar, harddisk vb. dijital ekipmanları iş amaçlı kullanamaz, işyeri ağına veya bilgisayarlarına bağlayamaz, dosya aktarımı gerçekleştiremez. Şahsi cep telefonları kablosuz internet kullanımı için misafir ağına bağlanabilirler, kurumsal ağa bağlanmamalıdır. Bilgisayar / ekipman eksikliği bu maddenin uygulanmamasına neden olamaz, ekipman planlaması doğru bir şekilde gerçekleştirilir ve gerekirse önceden satınalma talebinde bulunulur.
- Sunucu bilgisayarı zaruri durumlar dışında kapatılmaz. Yetkili kişi veya yetkili kurum dışında diğer Arz Portföy çalışanları hiçbir şekilde Sunucu Bilgisayarı, Ağ Cihazları (Firewall, Switch, Hub, Modem) ile temas kuramaz ve bu bilgisayara müdahalede bulunamaz. Acil bir durumda müdahale edilmesi gerektiğinde, derhal Bilgi Sistemleri Firması'ndan yetkili kişi durumdan haberdar edilir.
- Sunucu ve temel ağ bileşenleri sistem odasında ayrı bir kabinette tutulur. Sistem odası ve kabinet kilitli tutulur. Sistem odası girişi kartlı sistem ile yetkilendirilmiş olarak yönetilir. Sistem odasına giriş yetkisine Bilgi Sistemleri Firması ve BGYS Temsilcisi sahiptir.
- Bir başka çalışanın herhangi bir konu ile ilgili şifresinin ya da sisteminin kullanılması veya rızaları alınmaksızın şahsi dosyalarına erişilmesi yasaktır.
- İş ile ilgili çalışmaların çalışanların özel bilgisayarlarında yürütülmesi yasaktır. Eğer kurum dışında çalışma yürütülecekse şirketin dizüstü bilgisayarları bu çalışmalar için kullanılabilir.
- Elektronik ortamda kullanılan dosyalar, dokümanlar, yazılımlar veya Arz Portföy'ün

kurumsal internet hesapları üzerinde yetkili kişinin bilgisi olmadan şifre değişikliği ve/veya şifreleme yapılamaz. Şirket içerisinde kullanılan tüm şifreler ve kullanıcı adları kullanıcı ve şifre sahibi departmanlar tarafından sunucuda erişimi yetkilendirilmiş klasörlerde kayıt altına alınır.

- Kullanıcılar başka çalışanların veya bilgisayarların çalışmasını, iş görmesini, veri işlemesini veya işlevselliğini engellemeyecek şekilde çalışırlar.
- Bilgisayarları kapatırken normal yolların kullanılmasına dikkat edilir.
- Sunucu bilgisayarı veya bilgi sistemi üzerindeki verilerin silinmesi, tahrip edilmesi veya uygun yere yerleştirilmemesinden dolayı ortaya çıkan zararlardan kullanıcılar sorumludur. Aynı şekilde söz konusu verilerin kişisel kullanım, kişisel yarar sağlama, bilgi kaçırma amaçlı veya zarar verme amaçlı olarak kullanılması yasaktır. Bu konu ile ilgili **5237 Sayılı Türk Ceza Kanunu'nun 243. ve 244. Maddeleri** ve işverenin güvenini kötüye kullanmaktan **4857 Sayılı İş Kanunu'nun 23. Maddelerinin** hükümleri geçerlidir.

b) İnternet Kullanımı

- İnternet genel olarak iş ile ilgili bilgi ihtiyacı duyulan araştırmalarda ve iletişim amacıyla kullanılır.
- İnternetten elde edilen bilgiler, geçerliliği, güvenilirliği, güncelliği ve doğruluğu kontrol edilerek kullanılır.
- Bilginin kullanımında, lisans anlaşmalarına ve fikri mülkiyet haklarını düzenleyen yasal zorunluluklarına uygun davranılır.
- Arz Portföy kullanıcıları, Arz Portföy'de kullanmakta oldukları mobil veya sabit bilgisayarlar ve diğer mobil cihazlar ile kendi kullanıcı adları ve şifreleri üzerinden interneti kullanarak iletişim sağlarlar. İnternet erişimi ve iletişim esnasında kullanıcıların ulaştıkları kaynaklar düzenli olarak kayıt altına alınır.
- Kullanıcıların internet erişimi, güvenlik duvarı yazılımı üzerinde tanımlı kurallar ve bilgi güvenliği politikaları çerçevesinde sınırlandırılır.
- Arz Portföy'e ait internete erişebilen cihazlar ile başka şirket ya da kişilere ait ağlara, o ağların yöneticilerinden izinsiz olarak, erişim yapılamaz.
- İnternet erişimi sağlayan kullanıcıların spam, virüs veya worm gibi zararlı programcıklar içerebilecek sitelere girmemesi ve e-posta kullanımlarında sahte e-postalar üzerinden gelebilecek bu tür tehditlere yönelik dikkatli ve şüpheci olmaları gerekmektedir.
- İnterneti kullanırken; her ne nedenle olursa olsun, karşı tarafa ait bilgileri ele geçirmek, şifre kırmak, virüs göndermek, kendi veya karşı tarafın ağı üzerindeki dosyaları tahrip etmek, değiştirmek, yok etmek gibi rahatsız edici, yıkıcı ve saldırgan davranışlarda bulunmak, internetteki bir web sitesini kırmak veya tahrip etmek, başkasına ait bir siteye yetkisi olmadığı halde girmek, e-posta ile başkalarını rahatsız etmek veya zarara uğratmak, interneti alıcı tarafından belirlenmiş kurallara ya da internet ortamında yerleşmiş genel dürüstlük kurallarına aykırı sayılacak şekilde kullanmak, bu nitelikte sayılacak e-posta ya da dosya iletmek yasaktır.
- Arz Portföy'ün faaliyet konusu, işi, tedarikçileri, çözüm ortakları, yatırımcıları ya da adayları ile ilgisi olmayan erişimler ve transferler ile genel ahlak ve adaba aykırı, kanunlar çerçevesinde terör ya da suç teşkil eden yasa dışı veya zararlı içerikli sitelere erişim yasaktır.
- Her ne suretle olursa olsun, etnik veya politik/siyasi mesajların iletilmesi, haber, sosyal

ağ, forum, eğlence ve cinsel içerikli sitelere girilmesi; internet ortamında gazete, dergi, yorum takip edilmesi, anketlere oy verilmesi, oyun oynanması, sohbet yapılması, Genel Müdür'ün onayı alınmaksızın herhangi bir siteye üye olunması yasaktır.

c) E-Posta Kullanımı

Arz Portföy'de e-posta kullanımına ilişkin esaslar ve standartlar **T.BY.03 Elektronik Yazışma Talimatı'nda** tanımlanmış olup, söz konusu talimatname tüm çalışanlara bu doküman ile birlikte okutulmalıdır.

d) Cep Telefonu / Tablet Kullanımı

Şirket tarafından personele tahsis edilen ve yönetim tarafından kullanılan cep telefonları, şirket içi yazışma, e-posta, fotoğraf vb. kurumsal bilgileri içerdiğinden dolayı, Bilgi İşlem birimi tarafından veya kullanıcı tarafından belirlenen şifre koruması aktif olarak tutulur. Cep telefonu ve tabletler için kullanıcılar tarafından şifre oluşturulur ve BGYS Temsilcisi'ne iletilir.

Toplantılarda gizli bilgi içeren fotoğraflar ve notlar şirket cep telefonları ile fotoğrafı çekilir veya not alınır. Şahsi telefonlar, gizli bilgilerin kayıt edilmesine yönelik kullanılamaz.

e) Giden ve Gelen Evrak

Arz Portföy dışına giden veya dışarıdan gelen basılı evrak (yazışma, mektup, dilekçe vb.), Arz Portföy Gelen Evrak Kayıt Defteri veya Giden Evrak Kayıt Defterine uygun olarak kodlanır ve basılı olarak dosyalanır.

Gelen ve giden faturalar, bu kayıt düzeninin dışında tutulur.

a. Giden Evrak

Hazırlık
Dosya sunucusu üzerinde ortak alanda dijital olarak tutulan **Giden Evrak Kayıt Defteri (F.BY.04B)** bulundurulur. Evrakı hazırlayan departman, kurum dışına göndereceği bütün basılı yazışmalara, eki bulunan veya kayıt altında olması gereken e-postalara giden evrak formundan sıradaki numarayı verir ve evrakın bilgilerini **Giden Evrak Kayıt Defteri'ne** kaydeder.

Dosyalama
Giden evrak numarası verilen tüm dokümanların basılı bir nüshası her departman dahilinde açılmış olan Giden Evrak klasörüne yerleştirilir.

Aynı zamanda bu dokümanlar taranarak (tararken çözünürlüğü düşük tutulur) departmanların giden evrakları için dosya sunucusu üzerine açılmış klasörlere yerleştirilir. Taranmış dosya sadece giden evrak numarası ile isimlendirerek yerleştirilir. Dosyanın ismine başka bir bilgi girilmez. Böylece ihtiyaç halinde giden evrak numarasından arama yapılarak ilgili dosyaya ulaşılır.

b. Gelen Yazılar

Teslim Alma / Kayıt / Dağıtım
Arz Portföy'e faks veya kurye/posta yoluyla ulaşan evraklar açılıp/kontrol edilip tasnif edildikten sonra basılı olarak tutulan **Gelen Evrak Kayıt Defteri (F.BY.04A)** kaydedilir. Evrak sıra numarası evrakın üzerine, **gelen evrak kaşesi** basılarak elle yazılır. Tüm evraklar Arz Portföy'e ulaştıktan en geç 1 saat içerisinde ilgili kişisine teslim edilir / kişi kurumda değil ise e-posta veya online mesaj ile kişi evrak hakkında bilgilendirilir, talep etmesi halinde taranarak kendisine iletilir.

İlgili çalışan resmi kurumlardan gelen evraklarda yetkili kişiyi (Örneğin Sosyal Güvenlik Kurumu'ndan gelen evraklar için Mali ve İdari İşler Müdürü'ne) bilgilendirir ve yetkili kişi, evrakı imza karşılığı bizzat teslim alır.

Dosyalama
Gelen evrak numarası verilen tüm dokümanlar her departman dahilinde açılmış olan Gelen Evrak klasörüne yerleştirilir. Evrakın konusuna ait özel bir klasörü bulunmakta ise aslı ilgili klasöre kopyası ise Gelen Evrak klasörüne yerleştirilir.

Aynı zamanda bu dokümanlar taranarak (tararken çözünürlüğü düşük tutulur) departmanların gelen evrakları için dosya sunucusu üzerine açılmış klasörlere yerleştirilir. Taranmış dosya sadece gelen evrak numarası ile isimlendirerek yerleştirilir. Dosyanın ismine başka bir bilgi girilmez. Böylece ihtiyaç halinde gelen evrak numarasından arama yapılarak ilgili dosyaya ulaşılır.

2. BİLGİ VARLIKLARI YÖNETİMİ

Bu bölümün amacı, bilgi varlıklarının sınıflandırılması, gizlilik, erişilebilirlik, bütünlük ve kritiklik değerlerinin belirlenmesi ve yönetilmesi prensiplerini tanımlamaktır.

Arz Portföy'de bilgiler, elektronik ortamda ve basılı ortamda depolanmaktadır. Bilgi güvenliği kapsamında fiziksel bilgi varlıkları ve bilgiler ayrı olarak sınıflandırılmıştır.

Fiziksel bilgi varlıklarının sınıflandırılması şu şekilde yapılmıştır:

Bilgi Depolama Ortamları	Diğer Bilgi Varlıkları
• Sunucu Bilgisayarı	• Yazıcılar
• Çalışan Bilgisayarları (Client)	• Kablolu Ağ (Switch, Hub)
• Mobil Cihazlar (Laptop, Cep Telefonu)	• İnternet Ağı ve Kablosuz Ağ (Modem, Access Point)
• Klasör ve Dolaplar	• Yazılımlar / Programlar
• Harici Diskler, USB Bellekler ve SD Kartlar	• İşletim Sistemleri
• Ağ Depolama Üniteleri (NAS)	• İletişim Sistemleri (Santral, Sabit Telefon vb.)
• Ajanda, Notluk vb. Ortamlar	• Güvenlik Duvarı (Firewall / UAT)

- Web ve E-posta Sunucusu

Fiziksel bilgi varlıkları, **F.BY.16 Bilgi Sistemleri Envanteri** ve **F.İİ.01A Demirbaş Listesi**'nde belirtilmiştir.

Çalışanlar, kendisine **F.İİ.01B Demirbaş Zimmet ve Taahhüt Formu** ile zimmetlenen veya ortak kullanım alanlarındaki, mekanik veya elektronik araç, gereç ve büro ekipmanlarının, bilgisayar programlarının, elektronik ortamda ve dışarıda oluşturulmuş sistemlerin, Arz Portföy dosyalama ve arşiv sisteminin, etkin ve usulüne uygun kullanımından, bakımından, temizliğinden ve korunmasından sorumludurlar. Bunların dışında klasörlerde, elektronik ve dijital ortamlarda saklanan evrak, bilgi ve belgelerin hem korunmasından, hem de mahremiyetinden Arz Portföy çalışanları zincirleme sorumludur.

Arz Portföy'e ait mekanik veya elektronik araç, gereç ve büro ekipmanlarının iş amaçlı olarak kurum dışına çıkarılması gerektiğinde kayıt altına alınır. Kayıt altına alınmadan demirbaşlar kurum dışına çıkarılamaz. Özellikle şahıslara zimmetli olan demirbaşlarda zimmetli çalışandan yazılı olarak izin alınır. Yazılı olarak kaydı bulunmayan tüm işlemlerden zimmetli çalışan sorumlu tutulur.

- Bilgilerin hangi bilgi varlığında depolandığı **F.BY.02 Bilgi Envanteri Tablosu**'nda belirtilmiştir.
- Elektronik ortamdaki klasör/dosya yetkilendirmesi **F.BY.02 Bilgi Envanteri Tablosu'na** göre yapılır.
- **Bilgi Envanteri Tablosu**, BGYS Temsilcisi'nin yönetiminde yılda bir tüm birim sorumluları tarafından gözden geçirilerek değişiklikler var ise güncellenir. Buna uygun olarak klasör / dosya yetkilendirmeleri de güncellenir.

Fiziksel Bilgi Varlıklarının İmhası:

- Donanımların imha olması, BGYS Temsilcisi tarafından kullanıcı bilgisayarlarının, sabit disklerine Hard Format atıldıktan sonra hurdaya satılır veya geri dönüşüme verilmesi ile gerçekleşir. Yazıcı, Access point, modem vb. tüm cihazların ayarları ve bellekleri kullanımdan kaldırılmadan önce Bilgi Sistemleri Firması tarafından sıfırlanır.
- Arz Portföy sunucusunun imhası ise, sabit disklerine Hard Format atılıp, sabit disklerinin arşivde süresiz saklanması ve geri kalan parçalarının hurdaya satılması veya geri dönüşüme verilmesi ile gerçekleşir.
- İmha işlemi gerçekleşecek materyalin kritikliğine göre imha metodu belirlenmeli, dokümanın sahibi kâğıt kıyma makinesinden geçirerek imha edilmesini sağlamalıdır.

Bilgi Envanterindeki sınıflandırma, şu kriterlere göre yapılmıştır:

- Arz Portföy'de ana süreçlerimiz, mali, idari, personel, bilgi işlem ve ortak olarak sınıflandırılmıştır.
- **Doküman Türü:** Süreçlerin işletilmesi esnasında üretilen ve kullanılan bilgi türleri
- **Depolama Yöntemi:** Bilginin nihai depolama yeridir. Elektronik ortamda saklananlar için sunucu veya ağ depolama üniteleri, basılı olarak saklananlar için listede belirtilen klasör ve dolaplardır.
- **Bilgi Tipi:**

- **Kayıt:** İş süreçlerinde oluşan / üretilen veri ve dokümanlardır.
- **Rapor:** Kayıtların kurum içi veya dışına belli bir formatta aktarılması için oluşturulan dokümanlardır.
- **Kalite:** Kurum içi mevzuatlardır (Yönetmelik, prosedür, form, talimat vb.)
- **Yazılım:** İş süreçlerinde kullanılan yazılım ve kodları ifade etmektedir.

- **Bilgi Sahibi:** Bilginin gizlilik, erişim ve bütünlüğünün sağlanmasından sorumlu olan kişidir.
- **Bilginin Kritiklik Seviyesi:** düşük/orta/yüksek derecesi ise o bilgiye erişim/okuma yetkisinin ne kadar sınırlandırıldığı ile açıklanmıştır.
- Bilgi sahibi, erişim yetkisinin sadece kendinde olmasını istiyorsa, yüksek; yetkilendirdiği çalışanda/birimde olmasını istiyorsa orta; herkese açık bir bilgi ise düşük olarak tanımlamıştır.
- **Basılı Dosyalama Süresi:** Bilginin hassasiyet seviyesine ne kadar sürede arşivde kalıp sonrasında imha edileceği bilgisidir.
- Her departman kendi bünyelerinde oluşturdukları dokümanların arşiv sürecinin takibinden sorumludur.
- Basılı evraklar öğütme / kırpma işlemi ile veya yakılarak imha edilirler.

Bilgi varlıkları listesi kritiklik değerleri aşağıda yer aldığı gibi tanımlanmıştır. Bu seviyeler, bilgi varlıkları listesinde yer alan her bir bilgi için erişim ve değişiklik yetkisi olarak ayrı ayrı tanımlanmıştır. Üst yönetimin tüm bilgilere erişim ve değişiklik yetkisi bulunmaktadır.

Erişim ya da Değişiklik Değeri	Erişim/Değişiklik Yetkisi	Bilgi niteliği
Yüksek	Bilgi sahibi	Yatırımcı bilgisi, finansal bilgiler gibi gizlilik, erişim ya da bütünlüğünün zarar görmesi durumunda kurum itibarının önemli derecede etkileneceği, kuruma maddi zarar getirebilecek ya da iş süreçlerinde önemli aksama yaratacak bilgiler.
Orta	Bilgi sahibinin yetkilendirdiği çalışan / danışman / birim	İç işleyişe yönelik kayıtlar gibi gizlilik, erişim ya da bütünlüğünün zarar görmesi durumunda kurumun maddi zarara uğraması ve süreçlerin aksaması riski olan, kurum içinde sınırlı paylaşılan bilgiler.
Düşük	Tüm Arz Portföy çalışanları	Arz Portföy işleyişine yönelik süreç dokümantasyonu ve prosedürler gibi gizlilik, erişim ya da bütünlüğünün zarar görmesi durumunda kurumun maddi zarara uğraması ve süreçlerin aksaması riski düşük olan, kurum içinde paylaşılabilen bilgiler.

Bilgi varlıkları listesinde yer alan Yüksek ve Orta kritiklik seviyesindeki bilgiler için listede belirtilen bilgi sahibi ve yetkilendirilen çalışan dışında erişim talebi olması durumunda erişim yetkisi **F.BY.07 Erişim Yetkisi İstek Formu** ile istenir. Yetki onayı, orta kritiklik seviyesi için ilgili bilgi sahibi, yüksek kritiklik seviyesi için üst yönetimdir. Form dijital ortamda doldurularak e-posta ile ilgili kişilerin onayına sunulur. E-posta bilgi olarak, BGYS Temsilcisine iletilir. Bu yetki yazışmaları formlarla beraber BGYS Temsilcisi tarafından elektronik olarak dosyalanır.

3. DİJİTAL DOSYALAMA VE BASILI ÇIKTI KULLANIMI

Bu bölümün amacı, Arz Portföy'e ait kâğıt tabanlı ve elektronik ortamlı bilgilerin korunması ve güvenliğinin sağlanmasına ilişkin kuralları düzenleyen, kullanılan basılı dokümanların; saklama, kullanma, çoğaltma ve imha koşullarını belirtir.

a) Şirket çalışanlarının dijital dosyalama ve dosya taşıma konularında dikkat etmesi gereken noktalar;

- Elektronik ortamda oluşturulan bilgiler sadece elektronik ortamda işlem görürler. Yasal veya temsili olarak ıslak imza gerektiren durumlar dışında basılı çıktısı alınmaz.
- Tüm elektronik dosyaların nihai depolama yeri, bilgi varlıkları listesinde belirtilen, kurumun sunucularıdır. Sunucularda yer alan bilgiler, zorunlu olmadıkça elektronik olarak çoğaltılmaz.
- Kişisel bilgisayar ve mobil cihazlar nihai bilgi depolama yeri olarak kullanılmaz. Dokümanlar oluşturulurken ya da üzerlerinde çalışma yapılırken kişisel bilgisayarlarda ya da mobil cihazlarda kopyası bulundurulabilir. Çalışma tamamlandıktan sonra doküman nihai depolama yerine (sunucuya) aktarılır ve kişisel bilgisayar / mobil cihazdaki kopyası silinir.
- Dosya silinirken ve oluşturulurken dikkat edilmesi, boşu boşuna dosya oluşturulmaması ve önemli dosyaların silinmemesi gerekir.
- Arz Portföy ve yatırımcılarının sınaî ve ticari sınırlarının korunması ana prensibinden hareketle; iş ile ilgili verilerin toplanması, işlenmesi ve kullanılması yöntemlerine, "doğru kişi-doğru adres-doğru zaman" üçgeninde özel bir hassasiyet gösterilmesi şarttır.
- Yetkilendirilmiş ve sorumlu çalışanlar dışında, Genel Müdür'ün izni olmaksızın, yatırımcılarımız ile ilgili bilgileri içeren dosyaları Arz Portföy bilgi sistemlerinin dışındaki bir depolama alanına (offline, online veya basılı) ve kurum dışına herhangi bir yöntemle çıkartamaz.
- Dosyaların transferi ancak ağa erişmek üzere yetkilendirilmiş bilgisayarlara yapılabilir. Kurum dışına çıkarılacak bilgisayarlara önceden bu dosyaların transfer edilmesi ve hazırlık yapılması gerekmektedir. Misafir veya çalışanların şahsi bilgisayarları kurum ağına bağlanamaz.
- Şirket bilgisayarlarının tamamı USB bellek / SD kart vb. cihazların bağlanamayacağı şekilde düzenlenmiştir. Bu konudaki aktarımlar Genel Müdür tarafından yazılı olarak yetkilendirilmiş çalışanların bilgisayarları / kullanıcıları üzerinden yapılır.
- Şirket bilgisayarlarının tamamının DVD/CD yazma fonksiyonları pasif hale getirilmiştir, sadece bu konuda yetkilendirilmiş çalışanlar (Genel Müdür, BGYS Temsilcisi) tarafından belirli bilgisayarlarda bu işlemler yapılabilir. DVD/CD yazma işlemi talep eden, içerik ve kaydeden olarak kayıt altına alınır.
- Sunucu bilgisayarının düzeni ve hızlı çalışması amacıyla klasör veya dosya oluştururken / kaydederken ayrıca aşağıdaki kurallara dikkat edilmelidir;

  ✓ Arz Portföy'e ait tüm çalışmaların sunucu üzerinde ilgili klasör veya geçici klasör içerisinde yürütülmesi, geçici klasöründe sürdürülen çalışmaların sonuçlandırılması halinde ilgili klasöre bekletmeden aktarılması, diğer şirket bilgisayarları üzerinde şirket çalışmalarının dosyalanmaması,

- ✓ Sunucuda paylaşılan klasörlerde dosya silmenin geri alınamayan bir işlem olmasından dolayı dosya silerken veya taşırken dikkat edilmesi, önemli dosyaların silinmemesi, dosya taşıma yerine öncelikle kopyalama işleminin yapılması, başarı ile tamamlanmasının ardından önceki yerinden silinmesi,
- ✓ Dosya / klasör adında noktalama işaretlerinin kullanılmaması ve kısa tutulması,
- ✓ Büyük-küçük harf uyumuna dikkat edilmesi,
- ✓ Ana klasörlerin dizinine hiçbir dosyanın kaydedilmemesi ve kaydederken dosyanın olması gereken yere kaydedilmesi,
- ✓ Şahsi isimler veya kodlar kullanılarak klasör oluşturulmaması (Nedim Çalışmalar gibi)
- ✓ Mevcut bir dosyanın üzerinde revizyon, düzenleme gerçekleştiriliyorsa farklı bir versiyon oluşturularak çalışılması, onayın ardından gereksizse silinmesi,
- ✓ Sunucu bilgisayarında yanlış veya aynısından birden fazla bulunan bir dosya görüldüğünde düzeltilmesi,

b) Şirket çalışanlarının basılı dosyalama ve kopyalama konularında dikkat etmesi gereken noktalar;

- Bilgi varlıkları envanterinde yüksek kritiklik seviyesinde belirtilen basılı dokümanlar kilitli dolaplarda saklanır.
- Yüksek kritiklik seviyesindeki basılı dokümanların lojistiği kapalı zarfta ve gizli bilgi kaşesi ile birlikte yapılır. Kaşe zarfın açılan yerine basılır ve zarfın açık olarak teslim edilmesi halinde Arz Portföy ile iletişime geçilmesi gerektiği zarfın üzerine kaşe ile not düşülür.
- Basılı çıktıların arka yüzü sadece kritiklik düzeyi düşük olan dokümanlarda kullanılır. Orta ve yüksek kritiklik düzeyine sahip dokümanların arkasına farklı bir yazı çıktı alınmaz, müsvedde olarak kullanılmaz. 3. kişiler ile yapılan toplantılarda bu hususa dikkat edilir.
- Her çalışan kendi dokümanının dosyalanması ve arşive kaldırılmasından sorumludur. Arşive kaldırılan dokümanlar, Arşiv Sorumlusu olarak yetkilendirilen çalışan ile birlikte kaldırılır. Dokümanlar, idari ve hukuki hükümlere göre belirlenmiş, **F.BY.02 Bilgi Envanteri Tablosu**'na uygun olarak muhafaza edilir.
- Kritikliği yüksek olan bilgiler üst yönetim izni olmadan (basılı ya da dijital) kopyalanarak çoğaltılmaz. İncelenmesi, başvurulması gereken durumlarda kaynağında (saklandığı) yerde bilgi varlıkları yönetim talimatnamesine göre erişim izinleri alınarak incelenir. Basılı kopyalar, işleri tamamlandıktan sonra kağıt kırpma makinesinden geçirilerek imha edilir.
- Arşiv süresini dolduran veya farklı nedenlerle imha edilmesi gereken basılı klasör ve içerikleri için **F.BY.10 Arşiv İmha Formu** düzenlenmesi ve imha edilen klasörlerin Dosyalama Fihristindeki kayıtlarının güncellenmesi gerekmektedir.

C. BİLGİ GÜVENLİĞİ DENETİMİ

Her Arz Portföy yöneticisi Bilgi Güvenliği Prosedürüne uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetmekten birinci derece sorumludur. Başta Bilgi Güvenliği Prosedürü olmak üzere yayınlanmış olan tüm politika ve prosedürler ile ilgili standartlara uyum esastır. Bu esasa uyumun gerekli teknik yetkinliklere ve İç Tetkikçi Sertifikasına sahip kişilerce periyodik olarak yılda bir denetimi ve ilgililere raporlanması gerekmektedir.

Bu gereklilik, planlama önceliklerine ve kaynak durumuna uygun olması halinde yönetimin belirlediği iç tetkikçi ekibi, aksi durumlarda bu konuda yetkin bağımsız kurumlar tarafından, yılda bir defa **F.BY.03 ISO 27001 Uygulanabilirlik Tablosu**'na uygun olarak yerine getirilir.

BGYS Temsilcisi, **F.BY.11 Bilgi Güvenliği İç Tetkik Programı**'nı hazırlayarak bir hafta öncesinden tetkik yapılacak birimlere gönderir. **F.BY.12 İç Tetkik Soru Kontrol Listesi**'ni 2 hafta öncesinden inceler, günceller. Denetimi tamamladıktan sonra İç Tetkik Raporu'nu hazırlar, tüm çalışanlarla paylaşır, yönetimin onayına sunar. İç Tetkik Rapor sunumu ile ilgili mutabakata varılan düzeltici-önleyici faaliyetler ile ilgili birimlere **F.KY.03 Düzeltici - Önleyici Faaliyet Düzeltme Talep Formu** iletilir. Birime verilen düzeltici-önleyici faaliyetler **F.KY.04 DÖF Takip Listesi** oluşturularak takip edilir, kapatılması sağlanır.

İç Denetim çalışmalarının ardından Yönetimin Gözden Geçirme Toplantıları yılda 1 defa ve gerekli durumlarda yapılır.

D. BİLGİ GÜVENLİĞİ İHLAL YÖNETİMİ

Tüm Arz Portföy çalışanlarının bu prosedür ve diğer bilgi güvenliği politika ve talimatlarında belirlenen kurallara uygun davranma sorumluluğu, bilgi güvenliği ihlali şüphesinde dahi BGYS Komitesi, BGYS Temsilcisi'ne bildirme sorumluluğunu da içermektedir. Gerek gözetim, gerek denetim, gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlallerinden ötürü yaşanabilecek olaylarda Arz Portföy Yönetimi prosedür, sözleşme ve kanunlara uygun olarak gerekli aksiyonları alır.

Herhangi bir bilgi güvenliği ihlalinin gerçekleşmesi halinde **F.BY.08 Bilgi Güvenliği İhlal Bildirim Formu** ile ihlali tespiti yapılır ve sonrasındaki süreçler Düzeltici / Önleyici faaliyet ve aşağıdaki süreçlere göre işletilir. Ayrıca bu olay ve ihlaller **F.BY.09 BT İhlal ve Olayları Takip Listesine** işlenir ve takip edilir.

Arz Portföy, bilgi güvenliğinin sağlanması adına çalışanlara **F.BY.05 Bilgi Güvenliği Çalışan Gizlilik Sözleşmesi** ve anlaşma yapılan kurum/kişi için **F.BY.06 Bilgi Güvenliği Kurum Gizlilik Sözleşmesi** imzalatılmaktadır. Bilgi güvenliği ihlalindeki yaptırımlar bu sözleşmelerde ve Arz Portföy ilgili prosedürlerinde tanımlanmıştır. Çalışanlar tarafından bilinçsiz bir şekilde gerçekleştirilen bilgi güvenliği ihlallerinde ihlalin kuruma verdiği zarar ölçüsünde yönetim tarafından kararı verilmek kaydı ile yazılı uyarı, kınama veya iş akdinin feshi cezaları uygulanır. Çalışanlar tarafından bilinçli bir şekilde gerçekleştirilen bilgi güvenliği ihlallerinde ise yönetimin onayı ile direkt olarak iş akdinin feshi cezası uygulanır.

Bu sözleşmeler dâhilinde çalışılmayan kurum / gerçek kişiler ile imzalanan özel sözleşmelere bu sözleşmelerde yer alan maddeler eklenir. Ayrıca yatırımcılar ile yaptığımız protokollerde bilgi güvenliği maddeleri yer almaktadır. Bilgi Güvenliği ihlali durumunda yetkili yasal otoriteler (Mahkemeler) bu sözleşmelerde ve yatırımcı protokolünde belirtilmiştir.

E. BİLGİ GÜVENLİĞİ OLAY YÖNETİMİ

Arz Portföy'ün acil ve beklenmedik durumlarda yatırımcılarına, aracı kurumlara, piyasa katılımcılarına ve üçüncü taraflara karşı olan yükümlülüklerini yerine getirme koşulları, yöntemleri ve prosedürleri ortaya koyulmuş ve bununla ilgili iş akış prosedürleri **T.BY.02 Acil ve Beklenmedik Durum Planı**'nda belirtilmiştir.

F. BİLGİ GÜVENLİĞİ BİLİNÇLENDİRME ÇALIŞMALARI VE EĞİTİMLERİ

Tüm Arz Portföy çalışanları ISO 27001 BGYS Bilinçlendirme Eğitimi'ni alırlar. Alınan eğitimlerin kayıtları ilgili Arz Portföy prosedürleri kapsamında tutulmaktadır. Ayrıca işe alınan her çalışana deneme süresi tamamlandıktan sonra söz konusu eğitim iç veya dış eğitmenlerce verilerek BGYS genel bilinçlendirmesi yapılır. Ayrıca her yeni başlayan çalışana Bilgi Güvenliği Yönetim Sistemi Prosedürü oryantasyon programı kapsamında okutulur ve okuduğuna dair imza alınır.

V. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ DOKÜMANLARI

1. F.BY.01 Bilgi Güvenliği Risk Envanteri
2. F.BY.02 Bilgi Envanteri Tablosu
3. F.BY.03 ISO 27001 Uygulanabilirlik Tablosu
4. F.BY.4A Gelen Evrak Kayıt Defteri
5. F.BY.4B Giden Evrak Kayıt Defteri
6. F.BY.05 Bilgi Güvenliği Çalışan Gizlilik Sözleşmesi
7. F.BY.06 Bilgi Güvenliği Kurum Gizlilik Sözleşmesi
8. F.BY.07 Erişim Yetkisi İstek Formu
9. F.BY.08 Bilgi Güvenliği İhlal Bildirim Formu
10. F.BY.09 BT İhlal ve Olayları Takip Listesi
11. F.BY.10 Arşiv İmha Formu
12. F.BY.11 Bilgi Güvenliği İç Tetkik Programı
13. F.BY.12 İç Tetkik Soru Kontrol Listesi
14. F.BY.13 Bilgi Sistemleri Bakım Takip Listesi
15. F.BY.14 Kurumsal Şifre Envanteri
16. F.BY.15 Kullanıcı Şifre Zimmet ve Taahhüt Formu
17. F.BY.16 Bilgi Sistemleri Envanteri
18. F.BY.17 KVKK Yatırımcı Muvafakatnamesi
19. F.BY.18 KVKK Çalışan Muvafakatnamesi
20. F.İİ.01A Demirbaş Listesi
21. F.İİ.01B Demirbaş Zimmet ve Taahhüt Formu
22. F.KY.03 Düzeltici – Önleyici Faaliyet Formu
23. F.KY.04 DÖF Takip Listesi
24. T.BY.02 Acil ve Beklenmedik Durum Planı
25. T.BY.03 Elektronik Yazışma Talimatnamesi
26. P.BY.01 Bilgi Güvenliği Risk Yönetimi Politikası
27. P.BY.03 Bilgi Teknolojileri Altyapı Yönetim Prosedürü