FONVENTURE KİTLE FONLAMA PLATFORMU A. Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

BİRİNCİ BÖLÜM

GENEL HÜKÜMLER

Amaç

Madde 1 - Bu bilgi güvenliği politikasının ("Politika") amacı, FonVenture Kitle Fonlama Platformu A.Ş.'nin ("Platform") bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak ve yedek olarak saklanmak üzere bulunan verilerin gizlilik, bütünlük ve ulaşılabilirliklerini sağlayacak önlemlere ilişkin kontrol altyapısını geliştirmek ve düzenli olarak güncellenmesine yönelik kural ve kontrolleri belirlemektir. Ayrıca, Platform faaliyetlerinde çalışanların ve ilgililerin uyması gereken bilgi güvenliği kıstaslarını belirlemek bu politikanın bir diğer amacını teşkil etmektedir.

Kapsam

Madde 2 - Bu Politika, Platform bilgi sistemleri ve üzerinde işlenen, iletilen, depolanan ve yedek olarak saklanan tüm varlıkları kapsamaktadır. Platform'un tüm organizasyon yapısı içerisinde bilgi sistemleri altyapısını kullanmakta olan tüm personeli, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

Hukuki Dayanak

Madde 3 - Bu Politika, Sermaye Piyasası Kurulu'nun 27.10.2021 tarihli 31641 sayılı Resmi Gazete'de yayınlanan Kitle Fonlaması Tebliği (III – 35/A.2) ve 05.01.2018 tarihli 30292 sayılı Resmi Gazete 'de yayınlanan 'Bilgi Sistemleri Yönetimi Tebliği (VII-128.9) esas alınarak hazırlanmıştır.

İKİNCİ BÖLÜM

TANIMLAR

Tanımlar

Madde 4 - Değerlendirme politikası kapsamında yer alan tanımlar aşağıda listelenmiştir:

• **Bilgi Teknolojileri Birimi (BT Birimi):** Bilgi güvenliğinden ve bilgi teknolojilerinden sorumlu Platform çalışanını/çalışanlarını,

• **Denetim İzi:** Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar takip edilmesinin sağlayacak kayıtlar,

• **Platform**: FONVENTURE KİTLE FONLAMA PLATFORMU Anonim Şirketi'ni,

• **SSL (Secure Socket Layer):** İnternet üzerinde bilginin gizliliğini ve bütünlüğünü korumak için oluşturulmuş bir protokol katmanıdır. Bu protokol bütün yaygın web sunucuları ve tarayıcıları tarafından desteklenmektedir. Bu protokolle çalışan web siteleri 'http' yerine 'https' ile başlar. SSL, gönderilen bilginin sadece doğru adreste deşifre edilmesinisağlar; bilgi gönderilmeden önce şifrelenir ve sadece doğru alıcı tarafından deşifre edilir. Bilginin bütünlüğü de bu süreçte kontrol edilir. İlgili protokol katmanını,

• **Taşınabilir Aygıtlar:** Dizüstü bilgisayarlar, akıllı telefonlar, tablet bilgisayarlar, CD, DVD, USB hafıza cihazları ve hard disk sürücüleri,

• **Tebliğ:** SPK Bilgi Sistemleri Yönetimi Tebliği (VII-128.9),

• **Üst Yönetim:** Yönetim Kurulu ve Genel Müdür'ü, ifade eder.

ÜÇÜNCÜ BÖLÜM

POLİTİKA UNSURLARI VE HEDEFLERİ

Bilgi Güvenliği

Madde 5 - Bilgi, diğer önemli ticari ve kurumsal varlıklar gibi, bir işletme ve kurum için değeri olan ve bu nedenle korunması gereken bir varlıktır. Bilgi güvenliği iş sürekliliğini sağlar, kayıpları en aza indirir, tehlike ve tehdit alanlarından korur. Bilgi güvenliği, bahsedilen politikada aşağıdaki bilgi niteliklerinin korunması olarak tanımlanır:

• **Gizlilik:** Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek,

• **Bütünlük:** Bilginin ve işleme yöntemlerinin doğruluğunu sağlamak ve yetkisiz değiştirilememesini temin etmek,

• **Erişilebilirlik:** Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.

Bilgi güvenliği politikası dokümanı, yukarıdaki korumaları ve gereksinimleri sağlayabilmek için oluşturulmuş denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtildiği dokümandır.

Bilgi Güvenliği Hedefleri ve Amaçları

Madde 6 - Bilgi Güvenliği Politikası, Platform'un;

• Çalışanlarına Platform güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermeyi,

• Bilinç ve farkındalık seviyelerini artırmayı ve bu şekilde Platform'da oluşabilecek riskleri minimuma indirmeyi,

• Platform'un güvenilirliğini ve imajını korumayı,

• Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamayı,

• Teknik güvenlik kontrollerini uygulamayı,

• Platform'un temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla Platform'un tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarını korumayı hedefler.

DÖRDÜNCÜ BÖLÜM

SORUMLULUKLAR

Bilgi Teknolojileri Birimi

Madde 7 - Bu Politika kapsamında bilgi teknolojileri biriminin sorumlulukları aşağıda listelenmiştir:

• Bilgi Güvenliği Politikasının oluşturulması, uygulanması ve güncelliğinin sağlanması,

• Veri Sınıflandırma çalışmasının gerçekleştirilmesi ve güncelliğinin sağlanması,

• Risk Envanteri kapsamında BT risklerinin belirlenmesi ve güncelliğinin sağlanması,

• İç güvenlik testleri ile bağımsız sızma testlerinin gerçekleştirilmesi sürecinin koordine edilmesi, aksiyonların planlaması, uygulanması, sonuçların raporlanması ve kontroller ile oluşturulan yapıların teknolojik gelişmelere göre güncellenmesi,

• Bilgi güvenliği olaylarına yönelik incelemenin yapılabilmesi için kritik sistem ve veri tabanları için denetim izlerini kaydederek yasal gerekliliklere uygun süreler içerisinde saklanması,

• Platform çalışanlarının bilgi güvenliğine ilişkin farkındalıklarının arttırılması amacıyla faaliyetlerde bulunulması ve periyodik olarak bilgi güvenliği farkındalık eğitimlerinin düzenlenmesi,

• Platform Bilgi Güvenliği Politikasının tüm çalışanlara duyurulması ve bilgi güvenliğine ilişkin taahhütnamelerin tüm çalışanlar tarafından imzalanması süreçlerinin tesis edilmesi,

• Bilgi güvenliğine ait ihlallerin izlenmesi, raporlanması ve aksiyon planlarının oluşturulması,

• Bilgi Güvenliği Planı'nın hazırlanması,

• Kullanıcı Kimlik ve Hesap Yönetimi standartlarının belirlenmesi.

Platform

Madde 8 - Bu Politika kapsamında Platform'un sorumlulukları aşağıda listelenmiştir:

• Bilgi Güvenliği Politikasının sağlanması amacıyla teknoloji altyapısı, süreçler ve insan kaynağı konusunda kaynak planlamasının yapılması,

• Bilgi sistemleri üzerinde etkin ve yeterli iç kontrollerin tesis edilmesi,

• Güvenlik kontrol sürecini değerlendirmeye tabi tutulması ve uygunluğunun onaylanması,

• Çalışanların bilgi güvenliğine ilişkin sorumluluklarının atanması; Bilgi Güvenliği Politikasına uymalarını ve politikaya aykırı davranışlar tespit edildiğinde gerekli disiplin işlemlerinin yürütülmesi,

• Bilgi Güvenlik Planı'nın onaylanması,

• Bilgi güvenliği hususunda farkındalığı artıracak çalışmaların desteklenmesi.

Platform Çalışanları

Madde 9 - Bu Politika kapsamında Platform çalışanlarının sorumlulukları aşağıda listelenmiştir:

• Bilgi Güvenliği Politikası ve politika ile ilgili tüm prosedürlere uyulması,

• Sahibi olduğu veriler için sınıflandırma çalışmasının gerçekleştirilmesi,

• Veri sınıflandırma çalışması sonucu belirlenen güvenlik kontrollerine uyulması,

• Bilgi güvenliğine yönelik tespit edilen olayların ivedilikle BT Birimi'ne bildirilmesi,

• Platform kaynaklarına erişim için kullanılan her türlü hesap/parola bilgisinin saklı tutulması ve BT Birimi personeli dahil hiç kimseyle paylaşılmaması.

Üst Yönetim

Madde 10 - Bu Politika kapsamında Üst Yönetim'in sorumlulukları aşağıda listelenmiştir:

• Bilgi güvenliği politikasının uygulanması üst yönetim tarafından gözetilir. Bilgi güvenliği politikası kapsamında bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesi yönetim kurulunun sorumluluğundadır.

• Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projeler üst yönetim tarafından gözden geçirilir ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanır. Kritik projelerin Kurum, Kuruluş ve Ortaklıkların iç kaynaklarıyla veya dış kaynak yoluyla alınan hizmetlerle gerçekleştirilmesine bakılmaksızın personel uzmanlığının, projelerin teknik gereksinimlerini karşılayabilecek nitelikte olması esastır. Bu yapıyı desteklemek üzere oluşturulacak yönetsel rol ve sorumluluklar açıkça belirlenir.

• Kurum, Kuruluş ve Ortaklıkların üst yönetimi, bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder. Üst yönetim, asgari olarak aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

• Bilgi güvenliği politikalarının ve tüm sorumlulukların her yıl gözden geçirilmesi ve onaylanması,

•. Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetiminin gerçekleştirilmesi,

•. Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi, o Tüm çalışanların bilgi güvenliği farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerin verilmesi.

• Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürler, Kurum, Kuruluş ve Ortaklıkların organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir ve işlerliğine ilişkin gözetim ve takipler gerçekleştirilir.

• Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda üst yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip bir bilgi sistemleri güvenliği sorumlusu belirlenir.

• Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için iş sürekliliği planı hazırlanır. Planda kritik iş süreçlerine ilişkin kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı belirlenir.

BEŞİNCİ BÖLÜM

UYGULAMA ESASLARI

İş Sürekliliği ve Bilgi Sistemleri Süreklilik Esasları

Madde 11 -

• Yürütülen faaliyetlerde bir kesinti olmaması için veri merkezi altyapısında tüm bileşenler yedekli olacak şekilde çift olarak kullanılır. Elektrik altyapısı ve bağlı olduğu UPS altyapısı, internet servis sağlayıcıları, firewall ve sunucu ekipmanları yedekli olacak şekilde çift olarak uygulanır.

• Yedekler taşınabilir medyalar üzerinde oluşturulur ve kilit altında saklanır. Yedekleme medyaları etiketlenir ve hangi medyada hangi yedeğin bulunduğuna dair kayıtlar tutulur. Yedekleme bilgisine uygun seviyede fiziksel ve çevresel koruma sağlanır. Gizliliğin önemli olduğu durumlarda yedeklemelerin kriptolu olarak alınması göz önünde bulundurulur. Yedekleme işlerine ait kayıtlar ayrıca tutulur, başarısız olan yedekleme işleri takip edilir ve yedeği alınamamış verinin yedeği alınır.

• Yedeklenmiş verinin düzenli aralıklarla geri döndürme testi yılda bir kere yapılır.

• Yedeklemenin türü (tam yedekleme/değişen kayıtların yedeklenmesi), yedeklemenin sıklığı iş gereklerine, güvenlik gereksinimlerine ve bilginin kritiklik derecesine göre belirlenir.

• Sunucu yedekleri günlük olarak alınır ve yedi gün geriye dönük saklanır.

• Veri tabanı yedekleri günlük olarak tam yedek alınır ve saatlik değişen kayıtların yedeği alınır.

• Kesinti durumunda sunucu bileşenlerinden dolayı bir problem oluşmuş ise günlük alınan sunucu yedeği yeni bir sunucuya yüklenir ve uygulamalar son versiyonları ile yeniden yayına alınır.

• Eğer veri tabanı sunucusunda problem yaşanırsa ek olarak veri tabanı tam yedekten yüklenerek üzerine değişen kayıt yedekleri yüklenir, en son bir saat önce alınan yedekler ile sistem ayağa kaldırılır.

E-posta Kullanım Esasları

Madde 12 -

• İşe yeni başlayan personel için, belirlenen şablon ile sistem yöneticisi tarafından e-posta adresi açılır.

• Kullanıcı e-posta adresini ve şifresini sistem yönetim ekibinden SMS ya da e-posta yoluyla alır, ilk kullanımda şifresini değiştirir.

• Kullanıcı kendisine verilen e-posta adresinden sorumludur. Şifresini başka bir kullanıcı ile paylaşamaz. Farklı bir kullanıcının e-posta hesabını kullanamaz.

• Kişisel kullanımlarda, internet ortamındaki listelere üye olunması durumunda Platform'a ait e-posta adresleri kullanılmamalıdır.

• Olası durumda spam, sahte e-posta vb. zararlı e-postalara cevap yazılmamalı, e-posta ekleri açılmamalıdır. Bu tür e-postalar virüs ya da truva atı amaçlı zararlı kodlar içerebilir.

• Çalışanlar e-posta hesaplarını düzenli olarak kontrol etmelidir.

• Başkasına ait bir cihazdan e-posta hesapları kontrol edilmemelidir.

• Uzun süre kullanılmayan e-posta hesapları (en az 6 ay giriş yapılmamış) BT Birimi tarafından kapatılır.

Kullanıcı Erişim Yetkilendirme ve Yönetim Esasları

Madde 13 -

• Hiçbir şekilde generic hesap (birden fazla kişinin kullandığı ortak hesap) oluşturulmaz, tüm kullanıcılar isme özeldir.

• Yönetici onaylı gelen talep doğrultusunda kullanıcı hesapları ve e-posta adresleri açılır.

• İhtiyaç halinde personele kullanacağı PC zimmet formu karşılığında teslim edilir.

• Kullanıcı çalışma süresi boyunca kendisine zimmetli olan eşyalardan sorumludur.

• Kullanıcının şahsi bilgilerini başkaları ile paylaşması ve bu durumda ortaya çıkacak olumsuz durumlardan kendisi sorumludur.

• Kullanıcıda herhangi bir admin / yönetici yetkisi bulunmaz.

• Sistem yönetimi, admin haklarını ve şifrelerini hiçbir kullanıcı ile paylaşamazlar.

• Kullanıcı hakları tanımlanırken en az ayrıcalık ilkesine uygun olarak, yalnızca gerekli işi gerçekleştirmek için yeterli erişime izin vermeye dikkat edilir.

Antivirüs Kullanım Esasları

Madde 14 -

• Kullanıcılar bilgisayarlarda yüklü olan Anti Virüs programının devamlı olarak açık olmasından sorumludur.

• Anti virüs programı güncellemeleri otomatik olarak kendisi yapar.

Şifre Oluşturma ve Kullanım Esasları

Madde 15 -

• Kullanıcı kendine ait olan hiçbir şifreyi, başka bir kullanıcı ile paylaşamaz. Kullanmakta olduğu panel, programlar, e-posta, web ortamları vb. sistemlerden kullanıcı sorumludur.

• Şifreler e-posta ve diğer yazışmalı veya sözlü programlarda paylaşılmamalıdır.

• Kullanıcı şifreleri herhangi bir kâğıda yazılıp saklanmamalıdır.

• Herhangi bir kişiye telefonda şifre verilmemelidir.

• Şifreler aile bireyleri veya yakın çevre ile paylaşılmamalıdır.

• Şifreler izin dönemlerinde veya herhangi bir sağlık sorununda raporlu olunması durumunda iş arkadaşları ile paylaşılmamalıdır.

• Şifreler “123456” veya “abcde” gibi basit şifreler olmamalıdır. Bunun gibi şifreler konulmak istendiğinde sistem otomatik olarak izin vermeyecektir.

• Şifre uzunlukları en az 7 karakter sıralı olmayan karmaşık şifreler olmalıdır. Bunun dışındaki şifreleri sistem kabul etmeyecektir.

• Kullanıcı şifresini unutmuş ise yöneticisi bilgisi ile BT Birimi’ne başvurur ve şifresinin sıfırlanmasını sağlar.

İnternet Kullanım Esasları

Madde 16 -

• Kullanıcılar peer-to-peer bağlantı yolu ile internetteki servisleri kullanmayacaktır.

• Bilgisayarlar üzerinden genel ahlak anlayışına aykırı sitelere girilmemeli ve herhangi bir dosya indirilmemelidir.

• Personel ortak kullanılan internet bağlantımızın yavaşlamaması adına yüksek bant genişliği kullanabilecek istekler konusunda dikkatli davranmalı, BT Birimi’nin aynı internet bağlantısını ofis dışındaki veri merkezine bağlanmak için de kullandığının bilincinde olmalıdır.

• Personel iş saatleri dahilinde bilgisayarını sadece iş amaçlı kullanmalıdır.

• Şüpheli herhangi bir durumda BT Birimi'ne bilgi verilmelidir.

• Tarayıcı adres bölümündeki adres bilgisi ve SSL sertifika durumu kontrol edildikten sonra işlem yapılmalıdır.

• Sık kullanılan adresler için kısa yol oluşturulmalı, arama yapılarak arama sonucundan link tıklanmamalı, arama ile girilecek ise arama sonucunda adres linkleri kontrol edilerek tıklanmalıdır.

Bilgisayar (Dizüstü&Masaüstü) Kullanım Esasları

Madde 17 -

• Bilgisayar başından kısa veya uzun süreli uzak kalınması durumunda bilgisayar kilitlenmelidir (Windows + L tuşu ile).

• Dizüstü bilgisayarların çalınması/kaybolması veya bozulması durumunda en kısa sürede BT Birimi'ne haber verilmelidir.

• Her kullanıcı kendi bilgisayarından sorumludur. Bu bilgisayarlardan kaynaklanabilecek, Platforma veya kişiye yönelik saldırılardan kullanıcı sorumludur.

• Kullanıcı bilgisayarından ağ güvenliğini ve ağ trafiğini etkileyecek eylemleri yapmamalıdır. (Örneğin bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi veya bir yere devamlı ping atması vb.)

• Port veya ağ taraması yapılmamalıdır.

• Cihazlar üzerindeki lisanslar gizli tutulmalıdır.

• Bilgisayarlar üzerinde bir problem oluştuğunda yetkisiz kişiler tarafından müdahale edilmemelidir.

• Bilgisayarlara herhangi bir lisanssız yazılım yüklenmemelidir. Aksi durumda sorumluluk kullanıcıya ait olacaktır.

• Dizüstü bilgisayarlar ve diğer taşınabilir aygıtlar ofis dışında güvenlik açısından daha dikkatli korunmalıdır. Herhangi bir bilginin 3. şahıslara geçmesi engellenmelidir.

Wireless (Kablosuz) Kullanım Esasları

Madde 18 -

• Personelin kullanacağı wireless ile misafir şahısların kullanacağı wireless sistemi ayrı tutulmuştur.

• Platform wireless şifresi, personel dışında kimse ile paylaşılamaz.

• BT Birimi gerekirse wireless kullanımında MAC filtreleme yapabilir.

• Mevcut wireless şifreleri 6 ayda bir değiştirilir.

• Misafirlere sadece "Guest" wireless bağlantısı bilgileri verilmelidir. Misafirler sınırlı erişim hakkına sahip olmalıdır. (Guest wireless bağlantısı sınırlandırılmıştır)

• Platform'a ait olmayan hiçbir cihaz Platform ağına kablo ile bağlanmamalı sadece misafir kablosuz ağ bağlantısı paylaşılmalıdır.

Bilgi Sistemleri Risk Yönetim Esasları

Madde 19 - Bilgi sistemlerine ilişkin risklerin yönetilmesinde asgari olarak değerlendirmeye alınacak hususlar aşağıda listelenmiştir:

• Bilgi teknolojilerindeki hızlı gelişmeler sebebiyle rekabetçi ortamda gelişmelere uymamanın olumsuz sonuçları, gelişmelere uyma konusundaki zorluklar ve yasal mevzuatın değişebilmesi,

• Bilgi sistemleri kullanımının öngörülemeyen hatalara ve hileli işlemlere zemin hazırlayabilmesi,

• Bilgi sistemlerinde dış kaynak kullanımından dolayı dış kaynak hizmeti veren kuruluşlara bağımlılığın oluşabilmesi,

• İş ve hizmetlerin önemli oranda bilgi sistemlerine bağlı hale gelmesi,

• Bilgi sistemleri üzerinden gerçekleştirilen işlemlerin, verilerin ve denetim izlerine ilişkin tutulan kayıtların güvenliğinin sağlanmasının zorlaşması.

• Bilgi sistemlerine ilişkin risk analizi yapılır. Bu analiz yılda en az bir defa veya bilgi sistemlerinde meydana gelebilecek önemli değişikliklerde tekrarlanır.

• Bilgi sistemlerinin teknik açıklarına ilişkin bilgi, zamanında elde edilir ve Platform'un bu tür açıklara karşı zafiyeti değerlendirilerek, riskin ele alınması için uygun tedbirler alınır.

Taşınabilir Aygıtlar ve Materyaller Kullanım Esasları

Madde 20 -

• Personel giriş kartı kayıp/çalıntı durumlarında BT Birimi'ne derhal bildirmek zorundadır.

• BT Birimi bina yönetimini bilgilendirir güvenlik açısından kaybolan veya çalınan kartı sistemden bloke eder ve giriş-çıkışlar engellemiş olur.

• Taşınacak veri eğer usb disk ile taşınacaksa bu usb diskin tehdit unsuru olan bir yazılım içermediğine emin olunmalıdır.

• Usb disk biçimlendirildikten sonra şifrelenerek veri kopyalanmalıdır.

• Usb diskleri bilgisayardan çıkartılırken önce “aygıtı düzenli şekilde çıkar” komutu verilerek bağlantısı kesilmelidir.

• Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan bu diskler darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir. Özellikle hard diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır.

• Kötü amaçlı kimselerin bilgilere ulaşmasını engellemek için taşınabilir materyaller güvenilir şekilde muhafaza edilmeli, gerekirse kilitli dolaplarda veya çelik kasalarda saklanmalıdır.

• Taşınır materyaller çalışma masasında veya bilgisayarda güvensiz şekilde bırakılmamalıdır. Gerekmediği sürece dışarıya çıkartılmamalı, kaybolma riskine karşı tedbirli olunmalıdır.

• Misafirlere ait USB, taşınır disk ya da hafıza kartları kesinlikle kullanılmamalı, dosya transferi gerektiği durumlarda eposta ile alınması gerekmektedir.

Fiziksel ve Çevresel Güvenlik Esasları

Madde 21 -

• Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.

• Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir. İmha edilmesi gereken yazılar bekletilmeden imha edilmelidir.

• Personel dışındaki kişilerin ofislere girişleri kontrol edilmeli ve bilgi kaynaklarının olduğu mekanlara personel eşliği haricinde girişlerine izin verilmemelidir.

• Dışarıdan hizmet alınan kuruluşların çalışanları için "ihtiyacı kadar bilme" prensibi uygulanmalıdır.

Ekipman Güvenliği ve Temiz Masa Esasları

Madde 22 -

• Hassas bilgiler içeren evraklar, bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir. Bu bilgi ve belgelerin kilitli yerlerde muhafaza edilmesi gerekmektedir.

• Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır.

• Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir.

• Faks makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmamalıdır.

• Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), PC'ler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

• Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmalıdır. Ekipman, gereksiz erişim asgari düzeye indirilecek şekilde yerleştirilmelidir.

• Kritik veri içeren araçlar yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilmelidir. Özel koruma gerektiren ekipman izole edilmiş olmalıdır.

• Bilgi işlem araçlarının yakınında yeme, içme ve sigara içilmesi engellenmelidir.

• Ekipmanın bakımı doğru şekilde yapılmalıdır. Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılmalıdır. Bakım sadece yetkili personel tarafından yapılıyor olmalıdır. Tüm şüpheli ve mevcut arızalar ve bakım çalışmaları için kayıt tutulmalıdır. Ekipman bakım için ofis dışına çıkarılırken kontrolden geçirilmelidir. İçindeki hassas bilgiler silinmelidir. Ekipman sigortalıysa, gerekli sigorta şartları sağlanıyor olmalıdır.

• Üretici garantisi kapsamındaki ürünler için garanti süreleri kayıt altına alınmalı ve takip edilmelidir.

• Tesis dışına çıkarılan ekipmanın başıboş bırakılmamasına, seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilmelidir.

• Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulmalıdır.

• Evden çalışma ile ilgili tedbirler alınmalıdır, ofiste uyduğumuz kurallar evde çalışma ortamımızda da geçerlidir.

• Cihazlar sigortalanır.

• Ekipman imha edilmeden önce gizli bilginin bulunduğu depolama cihazı fiziksel olarak imha edilmelidir.

• Depolama cihazının içerdiği bilginin bir daha okunamaması için klasik silme veya format işlemlerinin ötesinde yeterli düzeyde işlem yapılmalıdır.

İşten Ayrılma Durumunda Uygulanacak Esaslar

Madde 23 -

• İşten ayrılan personelin tüm hesapları kontrol edilir.

• Panel kullanıcısı pasif hale getirilir.

• E-posta ve varsa VPN hesapları kapatılır.

• Gerekli görülürse e-posta hesabı geçici bir süre için yönlendirilir.

• Zimmet formu ile personele tahsis edilen cihazlar/ekipmanlar geri alınır ve kontrolleri sağlanır.

• Bina/ofis yönetimine bilgi verilir ve kullanıcı giriş şifre ve giriş kartı iptal edilir.

ALTINCI BÖLÜM

DİĞER HUSUSLAR

Politika'da Yer Almayan Diğer Hususlar

Madde 24 - Bu Politika metninde düzenlenmemiş, Politika kapsamı ile ilgili diğer konularda Platform tarafından çıkarılan diğer Politika metninde, genelgeler ile sermaye piyasası işlemlerini düzenleyen yasalar ve diğer ilgili mevzuat hükümleri esas alınır.

Politika Hükümlerinde Değişiklikler

Madde 25 - Politika hükümlerini değiştirme yetkisi Platform Yönetim Kuruluna aittir.

Yürütme

Madde 26 - Bu Politika hükümleri FonVenture Kitle Fonlama Platformu Anonim Şirketi tarafından yürütülür.

Yürürlük

Madde 27 - İşbu Politika hükümleri FonVenture Kitle Fonlama Platformu Anonim Şirketi Yönetim Kurulu'nun 03.03.2025 kararı ile kabul edilmiş olup, karar tarihi itibarıyla yürürlüğe girer.

Hazırlayan	Kalite Sistem Onayı	Onaylayan
		Genel Müdür