T.C. GÜLTEPE 2. NOTERLİĞİ 1993

08 Şubat 2023

№07460

ECOFOLIO KİTLE FONLAMA PLATFORMU ANONİM ŞİRKETİ
YÖNETİM KURULU KARARI

KARAR NO : 2023/04
KARAR TARİHİ : 07/02/2023
GÜNDEM : Ecofolıo bilgi güvenliği politikası ve iş sürekliliği planı Hk.
TOPLANTIYA KATILANLAR: Hakan EK, Mehmet Tevfik Başkaya, Arif Ünver, Mustafa Duman, LETVEN CAPITAL GİRİŞİM SERMAYESİ PORTFÖY YÖNETİMİ ANONİM ŞİRKETİ (Temsilen Kamil KILIÇ)

Şirket merkezinde toplanan yönetim kurulu aşağıdaki hususları karar altına almışlardır.

Ecofolıo kitle fonlama platformu A.Ş. nin bilgi güvenliği politikasının ve iş sürekliliği planının ekteki şekilde kabulüne,
Oy birliği ile karar verilmiştir.

EK-1: Bilgi Güvenliği Politikası ve iş sürekliliği planı.

Hakan EK
Yönetim Kurulu Başkanı

Mehmet Tevfik BAŞKAYA
Yönetim Kurulu Başkan Vekili

Arif ÜNVER
Yönetim Kurulu Üyesi

Mustafa DUMAN
Yönetim Kurulu Üyesi

Yönetim Kurulu Üyesi
LETVEN CAPITAL GİRİŞİM SERMAYESİ
PORTFÖY YÖNETİMİ ANONİM ŞİRKETİ
(Temsilen Kamil KILIÇ)
(TC No: 41146527358)

ECOFOLIO KİTLE FONLAMA PLATFORMU A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

BİRİNCİ BÖLÜM
AMAÇ, KAPSAM ve HUKUKİ DAYANAK

Amaç

Madde 1 - Bu yönetmeliğin amacı, Ecofolio Kitle Fonlama Platformu A.Ş.'nin (bundan sonra Platform olarak anılacaktır) tüm faaliyetlerinde bünyesinde çalışanlar ve ilgili tarafların uyması gereken bilgi güvenliği şartlarının çerçevesini çizmek ve yazılı kurallara ilişkin ilke ve esasları düzenlemektir.

Kapsam

Madde 2 - Bu politika, Ecofolio Kitle Fonlama Platformu A.Ş.'nin bilgi sistemleri varlıklarını, bilgi sistemlerine erişim sağlayan personelleri, yazılım geliştirme, satış, kurulum, destek, entegrasyon, eğitim ve danışmanlık hizmetlerinin iş süreçleri ile bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik olarak bilgi güvenliği politikası üst yönetim tarafından hazırlanır ve yönetim kurulu tarafından onaylanır. Onaylanan bilgi güvenliği politikası personele duyurulur. Bu politika, bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanmasını, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulmasını, kontrollerin tesis edilmesini ve gözetimini kapsar.

Hukuki Dayanak

Madde 3 - Bu Politika, Sermaye Piyasası Kurulu'nun 27.10.2021 tarihli 31641 sayılı Resmi Gazete'de yayınlanan "Paya Dayalı Kitle Fonlaması Tebliği (lll – 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
TARAFLAR, SORUMLULUKLAR ve BİRİMLER

Sorumluluk ve Yetki

Madde 4 - Bilgi Güvenliği Politikasının sürekliliğinin sağlanmasından BGYS Yöneticisi sorumludur. Bilgi Güvenliği politikasında yapılacak güncellemeler yönetim gözden geçirme toplantılarında belirlenir ve BGYS yöneticisi tarafından "Üst Yönetimin" onayı alınarak dokümana yansıtılır.

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 göstermek,
- Bilinç ve farkındalık seviyelerini artırmak ve bu şekilde Platform'da oluşabilecek riskleri minimuma indirmek,
- Platform'un güvenilirliğini ve imajını korumak,
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak,
- Teknik güvenlik kontrollerini uygulamak,
- 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.

Bilgi Güvenliği Organizasyonu

Madde 7 - Platform'da Bilgi Güvenliği Yönetim Sistemi ile ilgili aşağıdaki şekilde bir organizasyon yapılmıştır.

- BGYS ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden BGYS Yönetim Temsilcisi
- Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesinden BGYS Yöneticisi sorumludur.
- BGYS Yönetim Temsilcisi ve BGYS Yöneticisi, Üst Yönetim tarafından atanır.
- Kapsam dâhilindeki birimlerde BGYS sorumluları belirlenmiştir. BGYS sorumluları kendi birimlerindeki Bilgi Güvenliği Yönetim Sistemi çalışmalarını takip etmek ve koordine etmekle yükümlüdürler.
- BGYS'nin işletilmesi, sürdürülmesi gözden geçirilmesi, eylem planı oluşturulması, karar alınması ve uygulanması faaliyetleri bir komite ile yürütülmektedir.
- Bu anlamda BGYS Yürütme ve Yönetim Komitesi oluşturulmuştur. BGYS Yürütme ve Yönetim Komitesi, BGYS Üst Yönetim Temsilcisi, BGYS Yöneticisi, ilgili birimlerden seçilen BGYS sorumlularından oluşur.
- BGYS Yürütme ve Yönetim Komitesi İş sürekliliği tatbikat raporlarının değerlendirmesi veya önemli bir güvenlik ihlal olayı olması durumunda da toplanabilir.

İş Sürekliliği Planı

Madde 8 - Platform, Kalite Yönetim Sistemi ve Bilgi Sistemleri Yönetimi Tebliği baz alınarak İş Sürekliliği Planı ve Acil Durum Eylem Planı hazırlanmıştır. Platform 'un değer yaratan faaliyetlerini, herhangi bir felaket, kriz ve afet durumunda önceden belirlenen seviyede yürütebilmesi için gerekli olan bu planlarda iş sürekliliği ve acil durum yönetim kapsamı, yapısı, temel unsurları, bilgi sistemleri sürekliliği planı, acil ve beklenmedik durum planı dokümante edilerek tanımlanmıştır. Olası durumlarda hazırlanan planlar ile Platform'un herhangi bir kesinti anında faaliyetlerinin sürdürülmesi veya zamanında kurtarılmasını sağlamak üzere operasyonel, finansal, yasal ve itibari olumsuz etkileri en aza indirmek, sorunları yönetebilmek, herhangi bir beklenmedik ve acil durumda öncelikli gerçekleştirilecek eylemleri, alınacak önlemleri belirleyerek, Şirket'in varlık ve itibarını korumak hedeflenmiştir.

Risk Yönetimi

Madde 9 - Platform'un Risk Yönetim Çerçevesi; Bilgi Güvenliği ve Hizmet Yönetimi risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Risk Analizi ve Risk İşleme Planı Bilgi Güvenliği ve Hizmet Yönetimi risklerinin nasıl kontrol edildiğini tanımlar. Risk İşleme Planının yönetiminden ve gerçekleştirilmesinden BGYS Yürütme ve Yönetim Komitesi sorumludur.

Bilgi sistemlerine ilişkin risklerin yönetilmesinde asgari olarak aşağıdaki hususlar değerlendirmeye katılır:

- 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.

Yukarıda verilen hususlar için aşağıda bulunan Risk Yönetim Planı hazırlanmıştır.

RİSK YÖNETİM PLANI

Cihaz Adı	Kritik Varlık Değeri	Tehdit	Açıklık	Olasılık	Etki	Risk üstlenme	Düzenleyici / risk azaltıcı faaliyetler
YAZILIMIN KOŞULDUĞU ANA SERVERLAR	5	Elektrik Kesintisi	Elektrikle çalışıyor	1	5	Risk kabul edilmiştir	Veri merkezinde bulunan sanal serverlar muhtemel kesintilere karşı UPS mevcuttur. UPS'ler ile ilgili herhangi bir arıza veya yetersizlik söz konusu olması halinde ise Jeneratör bulunmaktadır.
		Fiziksel Müdahale	İnsan faktörü	1	5	Risk kabul edilmiştir	Veri merkezinde bulunan fiziksel serverlara erişim yalnızca şirketin belirlediği yetkili kişiler tarafınca SSL VPN ile iki faktör doğrulama yöntemi kullanılarak yapılabilmektedir.
		İnternet bağlantısının kesilmesi	Servis Sağlayıcıları	1	5	Risk azaltılacaktır	Kullanılan veri merkezinin internet bağlantısı hâlihazırda iki servis sağlayıcı ile sağlanmaktadır. Her iki servis sağlayıcıda da problem yaşanması durumunda diğer lokasyonda bulunan serverlar devreye girecektir.
		Çalışma Ortamı, Nem, Sıcaklık	Ortamın fiziksel koşulları	2	4	Risk azaltılacaktır	Veri merkezinde bulunan, Sistem odası anlık olarak takip edilmektedir.
		Doğal Afetler, Yangın, Su Baskını	Bina ve mekânın özellikleri	1	5	Risk azaltılacaktır	Veriler yedeklenmektedir. Olası bir felaket senaryosunda, alınan yedeklerden dönüş sağlanacaktır.

		Hırsızlık	İnsan faktörü	2	5	Risk azaltılacaktır	Veri merkezi 7/24 güvenlik kamerası ve güvenlik görevlileri tarafından izlenmektedir. Binaya ve sunucunun bulunduğu bölgeye erişim sadece izni bulunan yetkili tarafından yapılır. Herhangi bir şekilde verilerin fiziksel olarak çalınması ihtimal dâhilinde dahi olsa hâlihazırda güvenlik gereksinimi yüksek olan veriler şifrelendiği için fiziksel olarak ele geçirilse bile 3. kişiler tarafından kullanılamayacaktır. Verinin çalınması ihtimaline karşı veri güvenlik uygulaması tüm dosya ve klasörleri anlık olarak takip etmekte ve yetkisiz erişim denemeleri karşısında ivedilikle müdahale ederek bağlantıyı kesmektedir. Sunucudaki verilerin ve donanımın fiziksel olarak çalınması senaryosunda ise alınan yedekler devreye alınabilecektir.
		Konfigürasyon Arızası	Yazılım yapısı	1	5	Risk azaltılacaktır	Teknik destek şirket içinde çözümlenmektedir. Yazılım koruması yeni antivirüs programı ve firewall ile desteklenmektedir. Konfigürasyon yedeği, her versiyona özel olarak alınmaktadır.
		Bant Genişliği Aşımı	Fazla trafik /cihaz kapasitesi	2	3	Risk azaltılacaktır	Anlık olarak izlenen veri trafiği kapasitesine göre server konfigürasyonları ilgili teknik personel tarafından ivedi bir şekilde artırılabilmektedir.
		Hacking, Fidye, Ddos ve Benzeri saldırılar	Dijital Saldırılar	3	4	Risk azaltılacaktır	Serverlar, yoğun istek almaları durumunda öncelikle istek atan IP'lere göre robot kontrolü yapmaktadır. İsteğin ısrarla sürdürülmesi durumunda Firewall konfigürasyonları devreye girerek ısrarcı IP'leri bloke etmektedir. Fidye ve benzeri virüslere

							karşı Log analiz ve data güvenliği uygulamaları sunucu bağlantılarını keserek ilgili ekibe sms ve mail ile bildirim göndermektedir. Sunucu ve client vlanları ayrılmıştır. Sunucular sadece VPN erişimine açıktır.
TÜM OFİS BİLGİSAYARLARI	3	Yazılım Arızası	Yazılım yapısı	1	5	Risk azaltılacaktır	Tüm yazılımların teknik destek altyapıları değerlendirilerek gerekli olması durumunda teknik destek personeli devreye girmektedir.
		Donanım Arızası	Donanım Yapısı	2	4	Risk azaltılacaktır	Teknik destek Şirket bünyesinde sağlanmaktadır. Gerekli görülmesi halinde donanım hizmet sağlayıcılar ile gerekli altyapı sağlanmıştır.
		Hacklenme ve korsan yazılımlar tarafından enfekte olma	Kullanıcı tarafında gerçekleşen risk	4	4		Yazılım koruması güncel antivirüs programı ve firewall ile desteklenmektedir. Konfigürasyon yedeği, her versiyona özel olarak alınmaktadır. Server ve client vlanları ayrıldı. Sunucular sadece VPN erişimine açık.
		Fiziksel Müdahale	İnsan faktörü	1	5	Risk kabul edilmiştir	Erişim yalnızca şirketin belirlediği yetkili kişiler tarafından yapılabilmektedir.
		İnternet bağlantısının kesilmesi	Servis Sağlayıcıları	1	5	Risk azaltılacaktır	İnternet bağlantısı hâlihazırda iki servis sağlayıcı ile sağlanmaktadır. Her iki servis sağlayıcıda da problem yaşanması durumunda mobil internet erişimi sağlanacaktır.
		Çalışma Ortamı, Nem, Sıcaklık	Ortamın fiziksel koşulları	2	5	Risk azaltılacaktır	Hali hazırda ofisin yer aldığı bina yönetimi tarafından gerekli önlemler alınmaktadır.
		Doğal Afetler,	Bina ve mekânın özellikleri	1	5	3.taraflar ile	Hali hazırda ofisin yer aldığı bina yönetimi

		Yangın, Su Baskını				paylaşılacak	tarafından gerekli önlemler alınmaktadır.
		Hırsızlık	İnsan faktörü	2	3	Risk azaltılacaktır	Şirket binası 7/24 güvenlik kamerası ve güvenlik görevlileri tarafından izlenmektedir. Binaya erişim izni bulunmayan kimse ulaşamamaktadır. Herhangi bir şekilde verilerin fiziksel olarak çalınması ihtimal dâhilinde dahi olsa hâlihazırda güvenlik gereksinimi yüksek olan veriler şifrelendiği için fiziksel olarak ele geçirilse de 3. kişiler tarafından kullanılamayacaktır. Donanımın fiziksel olarak çalınması senaryosunda alınan yedekler devreye alınabilecektir.
YAZICI, FAX, TELEFON VS.	5	Elektrik Kesintisi	Elektrikle çalışıyor	3	3	Risk azaltılacaktır	UPS mevcuttur.
		Fiziksel Müdahale	İnsan faktörü	2	3	Risk kabul edilmiştir	Erişim yalnızca şirketin belirlediği yetkili kişiler tarafından yapılabilmektedir.
		Doğal Afetler, Yangın, Su Baskını	Bina ve mekânın özellikleri	1	5	3.taraflar ile paylaşılacak	Hırsız alarmı mevcuttur. Ortam Kameralar yardımı ile izlenmektedir. İş yeri sigortası mevcuttur. Dış kapı kapalı tutulmaktadır.24 saat güvenlik mevcuttur.
		Çalışma Ortamı, Nem, Sıcaklık	Ortamın fiziksel koşulları	2	5	Risk kabul edilmiştir	Oda sıcaklığı, oda termostatı ve klimalar ile istenilen sıcaklığa ayarlanabilmektedir.
		Virüs Saldırısı	Teknik Açıklık	4	3	Risk azaltılacaktır	Antivirüs yazılımı var; lisanssız programlar kaldırıldı, sosyal ağlar ve uygunsuz içerikli sitelere erişim engellendi. Sunucu ve client vlanları ayrıldı. Sunucular sadece VPN erişimine açıktır.
		Hırsızlık	Taşınabilir varlık	1	5	Risk azaltılacaktır	Kameralar bina giriş-çıkış ve kat koridorlarında her ofis girişini görecek şekilde

							yerleştirilmiştir. Bina girişinde turnike sistemi ile otopark girişinde plaka tanıma sistemli bariyer sistemi bulunmaktadır.

Rol ve Sorumluluklar Tablosu

Madde 10 - Bu maddede Platform için her bir kontrol süreci için süreç sahibinin, rollerin, faaliyetlerin ve sorumlulukların açık bir şekilde tanımları bulunmaktadır. Ayrıca kontrol süreçleri periyodik olarak yapılmakla birlikte, dönemsel performans ölçümleri ile bilgi sistemleri kontrollerine ilişkin etkinlik, yeterlilik ve uygunluk ile öngörülen risk ya da risklerin etkisini azaltmaya yönelik faaliyetler devamlı bir şekilde takip edilmekte ve değerlendirilmektedir. Değerlendirme neticesinde tespit edilen önemli kontrol eksiklikleri üst yönetime raporlanır ve gerekli önlemlerin alınması derhal sağlanır.

BGYS YÖNETİM TEMSİLCİSİ	• Ecofolio Kitle Fonlama Platformu A.Ş.'nin BGYS altyapısını desteklemek ve işleyişini sürdürmesini sağlamak, • Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve güvenli şekilde işletilmesi için gerekli prosedür ve sorumlulukları belirleyerek ayrılmasını gerçekleştirmek ve ilgili tüm birimlere duyurulmasını sağlamak, • Çalışanların bilgi güvenliği kapsamında karşılaşabileceği riskleri anlaması, tanımlayabilmesi ve tanıması için eğitici metotların kullanımını sağlamak, • Güvenlik Politikasını tasdik etmek ve Platform içinde uygulanmasını sağlamak, • BGYS politikalarının ve ilgili tüm görevlerin takvim yılı başında gözden geçirerek revizyonunu sağlamak • Çalışanların BGYS hakkında bilgilenmelerini sağlayacak mekanizmaların işletilmesini sağlamak, • Bilgi güvenliğini tesis etmeye yönelik olarak tespit edilen ihtiyaçların karşılanmasını planlamak ve sağlamak, • BGYS kapsamlı dokümanları tasdik etmek, • Ecofolio Kitle Fonlama Platformu A.Ş. BGYS dair Risk analizini gerçekleştirmek sonucunda ortaya çıkan artık riskleri raporlayarak tasdik etmek. • Bilgi güvenliği politikasının, bilgi sistemleri süreklilik planının, bilgi sistemleri varlık envanteri ile iş sürekliliği ve güvenliği açısından önem teşkil eden diğer evrakların güncel sürümlerini ve bilgi sistemleri yönetimine ilişkin parolalarını güvenli ortamlarda saklamak.
BGYS YÖNETİCİSİ	• Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesini tesis etmek, • Yönetim Gözden Geçirme toplantılarını koordine etmek, • BGYS dokümanlarının revizyonunu ve kontrolünü belirli aralıklarla sağlamak, • Sistem plan etkinliğini ve güncelliğini temin etmek üzere testler yapmak, test sonuçlarını üst yönetime raporlamak. Ve daha önce belirlenmiş aralıklar kapsamında işlemi tekrarlamak • BGYS kapsamı içerisindeki tüm dokümanları tasdik etmek, • Çalışanların bilgi güvenliği farkındalık eğitimlerinin koordine edilmesi ve eğitim etkinliklerinin raporlarının değerlendirilmesi, • Risk analizi sonuçlarını değerlendirmek, kontrollerin belirlenmesi ve uygulanmasını gözden geçirmek ve koordine etmek, • Bilgi Güvenliği İhlal olaylarına ilişkin önleyici önlemleri planlamak, değerlendirmek ve takibini yapmak, • Bilgi Güvenliği 'ne ilişkin Düzeltici ve Önleyici faaliyetleri takip etmek, onaylamak ve değişikliklerin sonuçlarının kontrolünü sağlamak • Bilgi Güvenliği Politikası'nı takvim yılı başında revizyonunu ve BGYS Yönetim Temsilcisi'nin onaylamasını sağlamak

Varlık Yönetimi

Madde 11 - Bu maddede Varlık Yönetimi'ne dair hususlar yer almaktadır.

Bilgi varlıklarımız, sorumluları ve önem derecelerine göre sınıflandırılmasının yer aldığı envanter aşağıda olup, gerekli hallerde güncelleme yapılmaktadır. Taşınabilir ortamlar, içerdiği bilgilerin hassasiyet derecesine göre kaybolma veya hırsızlık risklerine karşı korunur ve önem derecesi yüksek bilgileri veya bu bilgilere erişim sağlayan yazılımları barındıran taşınabilir ortamlar yetkilendirme olmaksızın kurum dışına çıkarılmaz. Depolama ortamları elden çıkarılmadan önce üzerinde kuruluşa ait veri, bilgi ve lisanslı yazılımın bulunmamasına yönelik gerekli önlemler alınır. Temiz masa ve temiz ekran ilkeleri şirketimizce benimsenmiştir.

Platformumuzun 7 Şubat 2023 Tarihli Varlık Envanteri aşağıdaki belirtildiği gibidir:

Envanter No	Türü	Markası	Modeli	Alım Zamanı	Seri No / Detay
EKFP-001	LAPTOP	LENOVO	IDEAPAD 5 PRO	2022	S/N: YX03G9BMYXN0B1 C06007
EKFP-002	LAPTOP	HP	ELITEBOOK 650 G9	2022	S/N: SCD2356P48

Görevlerin Ayrılığı Prensibi

Madde 12 - Bu maddede Bilgi Sistemleri üzerinde hata, eksiklik veya kötüye kullanım risklerini azaltmak için görev ve sorumluluk alanlarının ayrılığı prensibine göre hareket edilir. Uygulanan örgüt yapısı içerisinde Bilgi Sistemleri ve Veri Güvenliği Birimi ile Yazılım Geliştirme Birimleri ayrı ayrı oluşturulmuş olup, gerekli testler testin niteliğine göre diğer birimler ile veya dış kaynaklardan sağlanmaktadır.

Şirketimizde;

- Bilgi sistemleri kapsamında süreçler tasarlanırken kritik işlem fonksiyonlarının tek bir personel veya dış kaynak hizmeti sunan kuruluş nezdine bağlı kalmamasına önem verilir.
- Sistem, veri tabanı ve uygulamaların geliştirilmesi/iyileştirilmesinde, test edilmesinde ve işletilmesinde görevler ayrılığı prensibi uygulanarak Görev ve sorumluluklar önceden belirlenmiş düzenli aralıklarla kontrol edilir ve güncelliği korunur.
- Sorumlulukların eksiksiz ve yerinde tasnif edilmesinin mümkün olmadığı durumlarda oluşması muhtemel hata, eksiklik veya kötüye kullanımı önleyici ve tespit etmeye yönelik telafi edici kontroller tesis edilir.

Fiziksel ve Çevresel Güvenlik

Madde 13 - Bu maddede Fiziksel ve Çevresel Güvenlik'e dair hükümler yer almaktadır. Platformumuz İdari İşler Birimi tarafından;

- Gizlilik gerektiren belgelerin fiziksel erişimi yalnızca yetkilendirilmiş kişiler tarafından yapılır.
- Personel dışındaki kişilerin ziyaretleri personel eşliğinde ofis giriş-çıkışları kontrol edilerek gerçekleştirilir.
- Dışarıdan hizmet alınan kuruluşların çalışanları için "ihtiyacı kadar bilme" prensibi uygulanır.
- Doğal afetler veya insan kaynaklı felaketlerden kaynaklanan hasarlara karşı fiziksel koruma önlemleri uygulanır ve personelin acil durum eğitimi alması sağlanır.

Ağ Güvenliği

Madde 14 - Bu maddede Ağ Güvenliğine dair hükümler yer almaktadır. Söz konu maddede yer alan tedbirlerden Bilgi Sistemleri ve Veri Güvenliği Birimi ve İdari İşler birimi sorumludur.

- Bilgi sistemleri altyapısına yönelik yetkisiz erişimleri engellemek için ağ izlenir ve yetkisiz erişim çabaları raporlanarak üst yönetime bildirilerek gerekli önlemler alınır.
- İç kaynak veya dış kaynak kullanımı yoluyla alınan her türlü ağ hizmetinin güvenlik kriterleri, hizmet düzeyleri ve yönetim gereksinimleri tanımlanır ve hizmet anlaşmalarına dâhil edilir.
- Ağların tehditlere karşı korunması ve ağları kullanan sistem, veri tabanı ve uygulamaların güvenliğinin sağlanması için kablolu ve kablosuz güvenli ağ protokolleri uygulanır.
- Ağ sistemine dâhil olan kullanıcılar için oluşturulan düzeylere göre yetkiler tanımlanır. Kullanıcı ağ giriş şifreleri belli periyotlarda değiştirilir.
- İletişim altyapılarının dinlemeye ve fiziksel hasarlara karşı korunması için gerekli tedbirler alınır.
- Uzaktan erişim sağlayan kullanıcıları kontrol etmek için gerekli yetkilendirme/görevlendirme yapılır. Bu kapsamda belirli konumlardan ve ekipmanlardan gelen bağlantıları yetkilendirmek için otomatik ekipman tanımlaması planlama içerisinde oluşturulur.
- Mobil cihazların ağ erişimine ilişkin risklere yönelik güvenlik tedbirleri gereği sistem unsuru olmayan mobil cihazlar 'Misafir Ağ Katılımcısı' olarak değerlendirilir ve sistem unsuru mobil cihazlar için gerekli güvenlik protokolleri uygulanır.
- Yüksek riskli uygulamaların güvenlik düzeyini artırmak için özel bağlantı prosesler uygulanır.
- Kurumsal ağ dışındaki ağlarla olan iletişimde, dış ağlardan gelebilecek tehditler için daimi gözlem kontrolünde tutulan güvenlik duvarı çözümleri kullanılır.
- İç ağın farklı güvenlik gereksinimlerine sahip alt bölümleri birbirinden ayrılarak, denetimli geçişi tesis eden kontroller yapılır.
- İç ve Uzaktan erişilebilen ağ sistemleri için fiziksel ve yazılımsal güvenlik duvarları aktive edilir.

Kimlik Doğrulama

Madde 15 - Bu maddede Sistem Kullanıcılarının Kimlik Doğrulamalarına dair hükümler yer almaktadır. Platform sisteminde kullanıcıların giriş bilgileri ve şifreleri kriptolu bir şekilde saklanır. Bu sayede sızmalar dahi olsa kullanıcı güvenliği sağlanır. Kullanıcıların şifrelerinin belirli bir güvenlik seviyesinde olması için uygulanan "Şifre Güvenliği Prosedürü" sistemde uygulanmaktadır. Bu prosedüre göre şifrelerin aşağıdaki özellikleri mevcuttur:

- Şifreler minimum 8 karakter, en az bir sayı, büyük harf, küçük harf veya alfa nümerik karakter içerecek şekilde girilmesi zaruridir.
- Şifreler ardışık tuş yöntemleri ile belirlenemez, tekrarlanan karakterlerden oluşturulamaz durumdadır.
- Şifreler ardışık tuş yöntemleri ile belirlenemez, tekrarlanan karakterlerden oluşturulamaz durumdadır.

Bu önlemlere ek olarak, kullanıcılar şifre değişimi yaptıklarında açık oturumları sonlandırılır. Hâlihazırda açık oturumlarını görebilen kullanıcılar, profil ayarları kısmından mevcut açık oturumları ve daha önce yapılan başarılı / başarısız giriş denemelerini görebilir.
Ayrıca kullanıcılar sisteme ilk kayıt esnasında sırasıyla e-posta hesaplarını, cep telefonu numaralarını, e-devlet üzerinden T.C. kimlik numaralarını ve varsa MKK sicil numaralarını doğrulamak zorundadırlar. Bu işlemleri gerçekleştirmeyen kullanıcılar Platform üzerinde herhangi bir işlem yapamazlar.

Veri Gizliliği

Madde 16 - Bu maddede KVKK hükümlerine göre Veri Gizliliğine dair hükümler yer almaktadır.

Ecofolio Kitle Fonlama Platformu A.Ş.. (Platform) olarak, kendisi adına, vekil olarak, bir şirket veya kuruluşun temsilcisi olarak Platform ile iletişime geçen girişimcilerin, yatırımcıların, hissedarların, iş ortaklarımızın, çalışanlarımızın, iş başvurusunda bulunmak veya internet sitemizi ziyaret etmek suretiyle veya diğer iletişim yöntemleri ile bizimle ilişki kuran diğer gerçek kişilerin, Platformumuzla paylaştığı kişisel verilerinin korunmasına ilişkin büyük önem vermektedir. Bu kapsamda 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) çerçevesinde veri sorumlusu olan Kurumumuz, aşağıda detayları yer alan "Kişisel Verilerin Korunması ve Gizlilik

Politikası" (Politika) ile kişisel verilerin işlenmesi, çerez ve benzeri teknolojilerin kullanımı konularında uygulamaya aldığı kural ve politikalarını kamuoyu ile paylaşmaktadır.

Kişisel Verilerin İşlenmesi

Kişisel Verinin İşlenmesi; kişisel verilerin tamamen veya kısmen otomatik olarak veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması veya kullanılmasının engellenmesi gibi kişisel veriler üzerinde gerçekleştirilebilecek her türlü işlem olarak tanımlanmaktadır. Platform, kişisel verilerin, "hukuka ve dürüstlük kurallarına uygun olarak", "doğru ve güncel olması" için elden gelen çabayı göstererek, kurum faaliyetlerine uygun "belirli, açık ve meşru" amaçlar için ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü" olacak şekilde, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilecek şekilde" işlemeyi hedeflemektedir.

Ecofolio Kitle Fonlama Platformu A.Ş. kişisel verileri, ilgili kişinin açık rızası olmadan işlememektedir. Ancak, "Kanunlarda açıkça öngörülmesi", "fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması", "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması", "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması", "ilgili kişinin kendisi tarafından alenileştirilmiş olması", "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hallerinden birisinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi KVKK hükümleri gereğince mümkün olabilecektir.

Platformumuz, Kanunun 12. maddesine uygun olarak, kişisel verilerin hukuka aykırı olarak açıklanmasını, erişimini, aktarılmasını veya başka şekillerde meydana gelebilecek güvenlik eksikliklerini önlemek için, korunacak verinin niteliğine göre gerekli tedbirleri almaktadır. Bu kapsamda; Şirketimiz Kişisel Verileri Koruma Kurulu ("Kurul") tarafından yayımlanmış olan rehberlere uygun olarak gerekli güvenlik düzeyini sağlamaya yönelik teknik ve idari tedbirleri almakta, denetimleri yapmakta veya yaptırmaktadır.

Dış Kaynak Kullanımı

Madde 17 - Bu maddede Dış Kaynak Kullanımına dair hükümler yer almaktadır. Bilgi güvenliği yönetim sistemi standardının gerektirdiği dış kaynaklı bilgiler aşağıdakileri temin etmek için kontrol edilir:

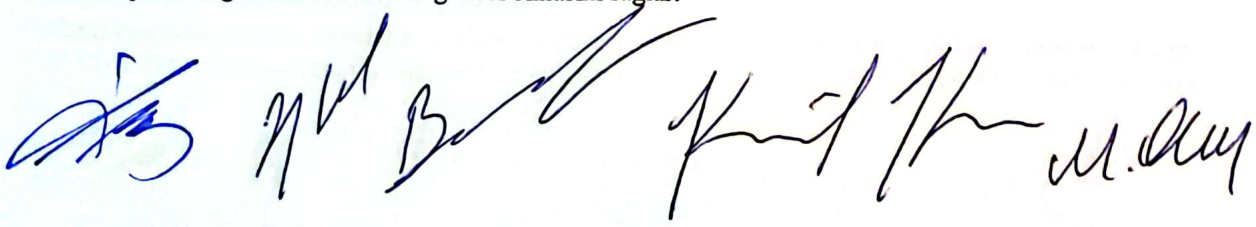
- Gereken yerde ve zamanda kullanım için erişilebilir ve uygun olması ve Doğru bir şekilde korunması (Örneğin, gizlilik kaybından, uygun olmayan kullanımdan veya bütünlük kaybından).

Yazılı bilgilerin kontrolü için, Platform uygunluğuna göre aşağıdaki faaliyetleri ele alınır:

- Dağıtım, erişim, getirme ve kullanım,
- Okunaklığın korunması da dâhil olmak üzere saklama ve koruma,
- Değişikliklerin kontrolü (Örneğin, sürüm kontrolü)
- Muhafaza etme ve yok etme.

Platform tarafından, "Doküman ve Kayıtların Kontrolü Prosedürü" ile düzenlenerek bilgi güvenliği yönetim sisteminin planlaması ve işletimi için gerekli olduğu tespit edilen dış kaynaklı yazılı bilgiler, kontrol edilir.

Platformda kullanılan, bilgi güvenliği sistemini etkileyen tüm evraklar çoğaltılarak kullanılır. Tutulan kayıtlar ilgili bölümlerinde ve iş bitimi sonrası merkezde olmak üzere toplam beş yıl muhafaza edilir. Destek dokümantasyonda sayılan bilgi güvenliği kayıtları ECOFOLIO KİTLE FONLAMA PLATFORMU ANONİM ŞİRKETİ'nde süresiz olarak saklanır. Yönetim Temsilcisi her takvim yılı altı ayda bir destek dokümanlarının güncel olup olmadığını kontrol eder ve güncel olmasını sağlar.



Gelen ve Giden evraklar kaydedilerek Genel Müdür'e iletilir. Genel Müdür gelen yazıları inceleyerek ilgili Bölüm/Birim Sorumlularını ve yapılacak işlemleri evrak üzerinde belirtir. Evrakların bir adet kopyasını Genel Müdürün belirlediği Bölüm/Birim Sorumlularına ulaştırır. Dışarıdan alınan ve verilen teklifleri ilgili firmanın dosyasına, diğer evrakların orijinalleri ise GELEN EVRAK klasörüne kaldırır. Gönderilecek yazılar Antetli Kâğıt kullanılarak gerçekleştirilir. Elle tutulan bilgi güvenliği kayıtlarının hepsi ilgili dosyasında ilgili birim sorumluları tarafından muhafaza edilir. Dokümanlar beş yıllık saklanma süresi sonunda Yönetim Temsilcisi ve ilgili Birim Sorumlusu tarafından bir daha kullanılamayacak şekilde imha edilir.

Elle tutulmayan kayıtlar ise, dijital ortamda ilgili klasörlerine kaldırılarak süresiz olarak kaydedilir ve server ya da CD/DVD ortamında ayda bir yedekleri alınır.
Bilgi güvenliği kayıtları, bilgi güvenliği yönetim sistemi prosedür, proses ve talimatlarında belirtilen saklama süresi sona ermeden, sözleşmelerde belirtildiği hallerde müşteri veya müşteri temsilcisinin değerlendirmelerine sunulur.

Bilgi güvenliği kayıtlarını saklamaktan sorumlu kişiler, bilgi güvenliği kayıtlarının saklanması sırasında çevre şartlarından dolayı hasar görmesini, bozulmasını engelleyecek önlemleri alırlar. Bu kayıtlara kolay ulaşılmasına imkân sağlayacak şekilde işaretleme ve sınıflandırma yöntemlerini geliştirilir. Geliştirdikleri uygulama önerilerinin Yönetim Temsilcisi'nden onayını aldıktan sonra uygulama başlatılır. Aynı zamanda uygulama şekli ilgili prosedür ve talimatlara eklenir.

Tüm prosedür ve talimatların ekler ve kayıtlar bölümünde yer alan ilgili bölümlerdeki saklanma süreleri sonunda bilgi güvenliği kayıtlarının toplanarak arşive kaldırılması Yönetim Temsilcisi tarafından sağlanır. Toplam saklanma süresi sona eren bilgi güvenliği kayıtları Yönetim Temsilcisi ve ilgili Birim Sorumlusu ile birlikte bir daha kullanılamayacak şekilde imha edilir.
İlave olarak dış kaynak yöntemi ile alınan sunucu hizmetlerinin sağlanmasında kullanılan sistemlere erişim yalnızca yetkili kişilerin kontrolünde sağlanır. Bu hizmetlerin sağlanmasında bilgi güvenliği prosedürleri uygulanır ve kişisel verilerin korunumuna azami önem gösterilir. Dış kaynak yöntemi ile karşılanan ihtiyaçlarda Platform ile hizmet sağlayıcı arasında gerekli önlemlerin alınmasını sağlayan sözleşmeler tesis edilir.

Kullanıcı Bilgilendirme

Madde 18 - Bu maddede sistem kullanıcılarının bilgilendirmelerine dair hükümler yer almaktadır. Platforma kayıt olan tüm kullanıcılar; Çıkar Çatışması Politikası, Değerlendirme Politikası, Bilgi Güvenliği Politikası, KVKK Bildirimi ve Genel Risk Bildirimi ile yapılan iş ve işlemlerle ilgili olarak şartlar, riskler ve istisnai durumlarla ilgili bilgilendirilir.
Platform, işlemler hakkında bilgi vermek veya güncel kampanyalar ile ilgili bilgilendirmek amacı ile zaman zaman kullanıcıları ile telefon, e-posta veya diğer iletişim yolları ile irtibata geçebilir. Kullanıcılar, Platforma üye olurken onayladıkları şart ve koşullarımız doğrultusunda kendileri ile bu tarz iletişimde bulunmasına razı olduklarını onaylamış olurlar. Kendileri ile bu tarz bir iletişimde bulunmasını istemeyen müşteriler, Ecofolio Kitle Fonlama Platformu A.Ş. ile 0216 759 88 48 numaralı telefonla veya ecofolio@hs01.kep.tr e-posta yoluyla irtibata geçerek bu taleplerini dile getirebilme hakkına sahiptirler.
Bunlara ek olarak platforma kayıtlı kullanıcılar; platform kullanımı esnasında karşılaştıkları sorunları mevcut feedback sistemi üzerinden ticket kaydı oluşturarak bildirme kolaylığına sahiptirler. Bu sistem üzerinden oluşturulan hata kayıtları ile bildirilen hata ve sorunların tarihçesi tutulacaktır. Tarihçesi tutulan kayıtlar üzerinden en çok sorun yaşanan alanlar ve en çok sorulan soruların istatistiksel verileri çıkarılabilecek ve böylece sorunlu alanların dinamiklerinde gerekli iyileştirmeler yapılabilecektir. Aynı zamanda kullanıcılar yaşadıkları sorunlar ile ilgili sorunları tekrar sormaya ihtiyaç duymadan sorunlarını çözebileceklerdir.
Ayrıca canlı yardım uygulaması ile mesai saatleri içerisinde kullanıcılar sistem ile ilgili yaşadıkları sorunları kolayca ilgililere iletebileceklerdir. Canlı yardım ile kullanıcıların sorunları tanımlamada yaşadıkları zorluklar ve uzaktan yardım alma kolaylığı sayesinde hızlı bir şekilde çözüme ulaşmaları sağlanacaktır.

İşlem Kayıtları

Madde 19 - Bu maddede sistem kullanıcılarının yaptıkları işlemler için sistem kayıtlarına dair hükümler yer almaktadır.

Platform üzerinden yapılan işlemlerde risklerin azaltılması amacıyla kullanıcıların yaptıkları işlemlerin denetim izleri kayıt altına alınmaktadır. Bu sisteme göre kullanıcının yaptığı her türlü işlem kayıt altına alınır ve gerekli

uyarı mekanizmaları kurularak hatalı ve fraud işlemlerin önlenmesi hedeflenmektedir. Örnek olarak art arda yapılan hatalı girişler sonrası kullanıcının sisteme girişi belirli bir süre boyunca engellenecektir. İlgili denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve olası bozulmaların tespiti için denetim izi kayıtları düzenli aralıklarla mutabakat yapılarak doğruluğundan emin olunur.
Denetim izleri aşağıdaki verileri içerir:

- Yapılan işlemin türü
- Yapılan işlemin statüsü
- Yapılan işlemin yetki ve izin doğruluk durumu
- Yapılan işlemin gerçekleştirildiği sistemin, uygulamanın detayları
- Yapılan işlemin zamanı

Denetim izleri geriye dönük olarak süresiz olarak saklanabilir, yedeklenir ve yüksek güvenlik düzeyine sahip ortamlarda korunur. Saklanan denetim izlerine çok kısa sürede ulaşmak mümkün olmaktadır. Denetim izlerinin işaretlenmesinde kullanılan işlem zamanlarının doğruluğunun sağlanması için NTP protokolü ile sistem, belirli aralıklarla zaman sunucusuna bağlanarak tarihi eşzamanlar. Böylelikle sistem saati, atomik saatlerle çalışan zaman sunucuları ile eşleşerek sürekli olarak tarihin güncel kalmasını sağlar.

Birincil ve İkincil Sistemler

Madde 20 - Bu maddede Veri ve Kayıtların birincil ve ikincil sistemlerde tutulasına dair hükümler yer almaktadır.

Sistemin sürekliliğinin sağlanması, yük dengesinin oluşturulması, herhangi bir saldırı durumunda zararlı bağlantıların engellenmesi ve olası risklerin azaltılması amacıyla; platformun verilerinin iletiminde ve yayınında birden fazla sunucu görev almaktadır.
Bu yapıya göre belirli periyotlarda yedek alan sunucular, ana sunucuda ya da ana sunucunun bulunduğu konumda herhangi bir sıkıntı olması durumunda kısa süre içerisinde yayına geçerek sistemin devamlılığını sağlar. Bu esnada servis dışı olan sunucu ile ilgili sorunların giderilmesinin ardından; servis dışı sunucu ile veri eşleme yapılarak verilerin normalizasyonu ve yeniden güvenliği sağlanır. Bu çalışma sistemi sayesinde sistemin sürekliliği ve verilerin güvenliği sağlanır.

Bilgi Sistemlerinin Sürekliliği

Madde 21 - Bu maddede Bilgi Sisteminin Sürekliliğine dair hükümler yer almaktadır.
İş ve Bilgi Sistemlerinin Sürekliliği Planları; Platform 'un faaliyetlerini etkileyen bir kesinti ya da olağanüstü bir durum yaşanması sonrasında, kritik iş birimlerinin ve aktivitelerin sürekliliğini sağlamak amacıyla hazırlanmış kurtarma stratejilerini ve aksiyonlarını kapsamaktadır. Kurtarma stratejileri ve aksiyonlar Kurum hizmetleri baz alınarak oluşturulmuştur. İş ve Bilgi Sistemleri Sürekliliği Planları olmayan kurumların, kritik süreçlerinde/aktivitelerinde yaşayacakları kesintiler sonucu itibar/saygınlık kaybı (imaj) yaşanma, finansal zarara uğrama, uyum açısından zor duruma düşme ve kendisine bağımlılığı olan üçüncü tarafları kötü yönde etkileme ihtimalleri daha yüksektir. İş ve Bilgi Sistemleri Sürekliliği Planlarının, Yönetim Kurulu'nun yetki verdiği Bilgi Güvenliği Yöneticisi tarafından yürütülmesi sağlanır. İş Sürekliliği Planları; İş Sürekliliği Planı, Bilgi Sistemleri Süreklilik Planı ve eklerinden oluşmaktadır. Plan dâhilinde görevli personelin hem İş Sürekliliği Planı'na hem de kendisi ile ilgili kurtarma planlarına (varsa ilgili ek dokümanlara) hâkim olması gerekir.
İş ve Bilgi Sistemleri Sürekliliği Planları; Platform çalışanları, müşterileri ve Platform kaynakları (teknoloji, ekipman) için güvenli bir çevre oluşturmak, olağanüstü durumlar için hazırlıklı olmak, olay anında ve sonrasında yapılacak işlemleri tanımlamak, Kurum süreçlerine/aktivitelerine minimum kesinti ve zararla devam etmesini sağlamak amacıyla hazırlanmıştır. Doküman dâhilinde; türü ve sebebi ne olursa olsun, herhangi bir kesinti ya da olağanüstü durumda, Kurumun kritik iş süreçlerinin/aktivitelerinin sürekliliğini sağlayan iş sürekliliği planlamasının alt başlıkları ifade edilmiştir.

ÜÇÜNCÜ BÖLÜM
ESASLAR ve PRENSİPLER

Genel Esaslar

Madde 22 - Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS prosedürleri ile düzenlenir. Platform çalışanları ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür. Bu kural ve prosedürlerin, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır. Bilgi Güvenliği Yönetim Sistemi, "Bilgi Teknolojisi Güvenlik Teknikleri ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimleri standartları temel alınarak ve SPK tarafından 05.01.2018 tarihli 30292 sayılı Resmi Gazete'de yayınlanarak yürürlüğe giren 'Bilgi Sistemleri Yönetimi Tebliği (VII-128.9) esas alınarak işletilir.

BGYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yöneticisi sorumluluğundadır. Ek, form, talimat gibi dokümanların güncellenmesi ise ilgili birimlerin sorumluluğundadır. Platform tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça Platform'a aittir. Kritik iş süreçlerini büyük felaketlerin ve işletim hatalarının etkilerinden korumak amacıyla iş sürekliliği yönetimi uygulanır. Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut Platform çalışanlarına ve yeni işe başlayan çalışanlara verilir. Bilgi güvenliğinin gerçek veya şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.

Temel BGYS Prensipleri

Madde 23 - Temel BGYS Prensipleri şu şekildedir;

- Gerekli durumlarda çalışanlar ve üçüncü taraflarla Platform'un gizlilik ihtiyaçlarını güvence altına almayı amaçlayan gizlilik anlaşmaları yapılır.
- Dış kaynak kullanım durumlarında oluşabilecek güvenlik gereksinimleri analiz edilerek güvenlik şart ve kontrolleri şartname ve sözleşmelerde ifade edilir.
- Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.
- Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.
- İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.
- Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.
- Platform'a ait bilgi varlıkları için Platform içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.
- Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.
- Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır.
- Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.
- Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
- Bilgi güvenliği ihlal olayları ve zayıflıklarının raporlanması için gerekli altyapı oluşturulur. İhlal olay kayıtları tutulur, gerekli düzeltici önleyici faaliyetler uygulanır ve düzenlenen farkındalık eğitimleri vasıtasıyla güvenlik olaylarından öğrenme sağlanır.
- Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.
- Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.

Uyulması Gereken BGYS Kuralları

Madde 24 - Uyulması Gereken Kabul Edilebilir Kullanım Kuralları, çalışanlar ve 3. taraflar için Platform iş süreçlerinde ve ilgili çalışmalarında bilgi depolama, iletim ve kullanım biçimleri ile ilgili uyulması gereken kuralları belirler. Aşağıda yer alan davranışlar; aksi yönde açık ve net bir iş tanımı, talimat veya prosedür bulunmadıkça Bilgi Güvenliği Politikasının ihlali olarak değerlendirilir.

- Platform tarafından sağlanan bilgi işlem sistemleri ve uygulamalar iş amaçlı olarak kullanılır. İş süreçlerini engellemeyecek düzeyde ve Bilgi Güvenliği Politikasını ve BGYS prosedürlerini ihlal etmeyen kişisel kullanımlar kabul edilebilir kapsamda değerlendirilir.
- Çalışma alanlarında, "Temiz Masa ve Temiz Ekran" prensiplerine uygun olarak, Genel özellikteki bilgiler dışında bilgilerin başkalarınca görülmesine imkân verilmeyecek şekilde önlemler alınmalıdır.
- Genel olmayan belgeler, masalarda bırakılmamalıdır.
- Genel olmayan dosyalar üzerinde çalışılırken bilgisayar ekranları herkesin görebileceği konumda bırakılmamalıdır.
- Genel olmayan dokümanlar diğer kişilerce görülmesini engellemek amacıyla, kullanılmadığı zamanlarda masa üstlerinden kaldırılıp gerekli korumaları alınmış çekmece ve dolaplarda saklanmalıdır.
- Genel olmayan belgeler dışında doğrudan işle ilgili olarak kendisine ulaştırılmayan ya da teslim edilmeyen Platform belgelerini incelememeli, değiştirmemeli, saklamamalı, kopyalamamalı, silmemeli ve paylaşmamalıdır.
- Platform tarafından açıkça belirtilen durum ve yöntemler dışında 3. taraflar ile Platform bilgilerini paylaşmamalı, satmamalı, aktarmamalı, yayınlamamalı ve internet ortamında paylaşmamalıdır.
- Birim çalışanları çalıştıkları ortamdaki masa ve dolap çekmecelerini kilitli tutmalı ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmamalıdır.
- Bilgisayarlar, aktif kullanım dışında iken şifreli ekran koruyucular devreye alınmalıdır.
- Mesai zamanları dışında bilgisayar sistemleri kapalı tutulmalıdır.
- Çalışanlar, kendilerine verilmiş olan kullanıcı adı ve şifreleri sadece kendileri kullanmalıdır.
- Çalışanlar, kendilerine verilmiş olan kullanıcı adı ve parola bilgilerini yetkilendirilmemiş kişilerin ele geçirmesine imkân verecek şekilde söylememeli, yazmamalı, kaydetmemeli ve elektronik ortamda depolamamalıdır.
- Platform'un, bilgi ve haberleşme sistemleri ve donanımları (İnternet, e-posta, telefon, çağrı cihazları, faks, bilgisayarlar, mobil cihazlar ve cep telefonları vb.) Platform işlerinin yürütülmesi için kullanılmalıdır. Bu sistemler yasadışı, Platform'un diğer politika, standart ve rehberlerine aykırı veya Platform'a zarar verecek herhangi bir şekilde kullanılmamalıdır.
- Platform'a ait bilgi sistemleri üzerindeki kaynaklara erişecek tüm bilgisayarlar etki alanına dâhil edilerek kullanılmalıdır.
- Gerekmedikçe bilgisayar kaynaklarını paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde sadece ilgili kişilere yetki verilmelidir.
- Gizli ve hassas bilgiler elektronik ortamda Platform içine ve özellikle Platform dışına gönderilmeden önce şifrelenmelidir.
- Gizlilik dereceli bilgiler içeren belgeleri, elektronik ortamları ve bilgi işlem sistemlerini korumak için gerekli fiziksel önlemleri "Fiziksel Güvenlik Prosedürü"ne uygun şekilde yerine getirmemelidir.
- Platform'a aya ait bilgi işlem sistemlerini, veri tabanlarını, dosyaları, ağ topolojilerini, cihaz konfigürasyonlarını ve benzeri kaynakları, Platform tarafından açıkça yetkilendirilmedikçe 3.taraflar ile paylaşmamalıdır.
- Platform çalışanları, çalıştıkları sürece veya Platform'dan ayrılmaları (emeklilik, istifa, vs.) durumunda Platform bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur.
- Taşınabilir sistemlerin kullanıcıları, bu sistemlerin güvenliğini sağlamak üzere "Taşınabilir Ortam Kullanımı Prosedürü"ne uymalıdırlar.
- Başta kullanıcı bilgisayarları ve sunucular olmak üzere mümkün olan tüm sistemler, zararlı yazılımlara karşı korunması için "Virüslü ve Zararlı Yazılımdan Korunma Prosedürü" ne uygun şekilde kullanılmalıdır.
- Gizlilik dereceli bilgiler elektronik ortamda işlenirken, depolanırken, aktarılırken "Bilgi İşleme Prosedürü"ne uygun şekilde davranılmalıdır.
- Gizlilik dereceli bilgilerin ve bilgi içeren ortamlarının imhasında "Teçhizatın Elden Çıkarma Prosedürü" ne uygun şekilde davranılmalıdır.

- Herkese açık sistemler (Örn; Genel internet sayfaları) hariç tüm bilişim sistemlerine erişim parola korumalı olmalıdır. Parolalar "Şifre Politikasına" uygun şekilde tanımlanmalı ve kullanılmalıdır.
- Gizlilik dereceli bilgilerin posta, faks, telefon, e-posta ve benzeri elektronik yöntemlerle iletiminde "Bilgi İşleme Prosedürü "ne uygun davranılmalıdır.
- Herkese açık bilgiler dışındaki bilgileri internet üzerinde, haber gruplarında, posta listelerinde ve forumlarda paylaşmamalıdır.
- Yeni bilgi sistemlerinin devreye alınması ve geliştirilmesi "Yeni Bilgi Sistemleri ve Yapılan Geliştirme Prosedürü "ne uygun yapılmalıdır.
- Çalışanlara ve gerekli görülen durumlarda 3. taraflara tahsis edilen e-posta hesapları, "E-posta Prosedürü "ne uygun şekilde kullanılmalıdır.
- Bilgi işlem sistemlerinin teknik güvenlik gereksinimlerine uygun durumda bulunup bulunmadığı, "Teknik Açıklıklarının Kontrolü Prosedürü"ne uygun şekilde kontrol edilmelidir.
- Platform'a ait bilgi işlem sistemlerini izinsiz olarak kullanım dışı bırakılmamalı, yer değiştirilmemeli ve Platform dışına çıkartılmamalıdır.
- Kullanım gerekliliği Platform tarafından yazılı olarak belirtilen güvenlik yazılımlarını (Örneğin; Anti virüs, kişisel güvenlik duvarı, vb.) bilgi işlem sistemlerden kaldırmamalı veya devre dışı bırakmamalıdır.
- İstemciden istemciye dosya paylaşım programlarını Platform bilgisayarlarına yüklememeli ve kullanmamalıdır.
- Platform'a ait bilgisayarlara, Platform'un yasakladığı yazılımları yüklememeli ve çalıştırmamalıdır.
- Platform tarafından lisanslanmış yazılımları çoğaltmamalı, paylaşıma açmamalı ve Platform dışına çıkarmamalıdır.
- Etki alanına dâhil olmayan sistemler ile etki alanına dâhil olan sistemler arasında bilgi aktarımı yapılmamalıdır.
- Taraflar ile gizlilik sözleşmesi imzalanmadan ve yetkili Platform çalışanınca nezaret edilmeden Platform bilgi işlem sistemlerine ve donanımlarına bağlanmamalı ve çalışmalarına izin verilmemelidir.
- Sunucu sistemleri üzerinde, kişisel bilgisayar uygulamalarını (Örneğin; e-posta programları, ofis uygulamaları, yazılım geliştirme araçları, network test araçları, vb.) kurulmamalı ve kullanılmamalıdır.
- İş süreçleri için gerekmeyen ve kullanılmasına izin verilmeyen sunucu hizmetlerini (Örneğin; HTTP, Telnet, SSH, vb.) bilgi işlem sistemleri üzerinde çalıştırılmamalıdır.
- Platform tarafından sağlanan ve kullanım amaç ve biçimleri yazılı olarak bildirilen Platform ağ bağlantı yöntemleri dışında bir yöntemle (Örneğin; ADSL modem, 3G modem, GPRS, vb.) internete veya başka ağlara bağlanmak için kullanılmamalıdır.
- Çalışanlar, Platform içi ya da Platform dışı bilgi sistemlerine yetkisi olmadığı halde zorla girmeye çalışmamalıdır.
- Platform'a ait bilgi işlem sistemlerine şifreleme ve parola mekanizmalarını kırmaya yönelik program ve araçlarını yüklenmemeli ve kullanılmamalıdır.
- Platform'a ait bilgi sistemleri üzerinde, Platform'un bilgisi ve izni olmadan değişiklik, yükseltme, genişletme yapılmamalıdır.
- İşle ilgili olmayan veya telif hakları ile korunan dosyaları (Örneğin; Müzik, film, kitap dosyaları, vb.) Platform bilgisayarlarına ve bilgi sistemlerine indirilmemeli, depolanmamalı, çoğaltılmamalı ve paylaşıma açılmamalıdır.
- Platform bilgi işlem sistemlerini iş dışında, eğlence amaçlı (oyun vb.) kullanılmamalıdır.
- Platform e-posta hesabı ile zincirleme e-posta gönderilmemelidir.
- Platform bilgi işlem sistemlerinde veya süreçlerinde gözlenen güvenlik zafiyetlerini, açıklarını veya oluşmuş saldırıları Bilgi Güvenliği İhlal Olayı Yönetim Prosedüründe belirtilen "bildirme" yöntemi ve muhatapları dışında ilgili olmayan kişilere iletilmemeli, açıklanmamalı, yayınlanmamalı veya bu zafiyetleri yetkisi dışındaki sistem ve bilgilere erişmek için veya kendi yetkilerini arttırmak için kullanılmamalıdır.

Yaptırım

Madde 25 - Platform politika ve prosedürlerine uyulmadığının tespit edilmesi halinde, bu ihlalden sorumlu olan çalışan ya da 3. taraf için geçerli olan usul, esas ve sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.

Yönetim Taahhüdü

Madde 26 - Platform hedef ve politikalarını gerçekleştirmek için Bilgi Güvenliği Yönetim Sistemini gereksinimleri yerine getirecek şekilde kurarak yürütür. Platform Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder. Bu taahhüdün sonucu olarak, Platform genelinde bilgi güvenliği farkındalık programları düzenler ve alt yapı yatırımlarını sürdürür.
BBGYS kurulurken üst yönetim tarafından BGYS Yönetim Temsilcisi ve BGYS Yöneticisi, atama yazısı ile atanır. BGYS Yönetim Temsilcisi ve BGYS Yöneticisi değiştiğinde, işten ayrıldığında üst yönetim tarafından doküman revize edilerek atama tekrar yapılır. BGYS Yöneticisini belirlemek ve değiştirmek üst yönetimin yetkisindedir.
Yönetim kademelerindeki yöneticiler güvenlik konusunda alt kademelerde bulunan personele sorumluluk verme ve örnek olma açısından yardımcı olurlar. Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, Platform'un en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden Platform yöneticilerinin gerek yazılı gerekse sözlü olarak güvenlik prosedürlerine uymaları, güvenlik konusundaki çalışmalara katılmaları konusunda güvenlik ile ilgili çalışmalarda bulunan personele destek olurlar. Platform üst yönetimi, bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

Yönetim Gözden Geçirmesi

Madde 27 - Platform Yönetim Gözden geçirme toplantıları BGYS Yürütme ve Yönetim Komitesi tarafından yapılır.

Üçüncü Tarafların Bilgiye Erişimi

Madde 28 - Platform çalışanı olmayan 3. tarafların, bilgi sistemlerini kullanma ihtiyacı olması durumunda (Örneğin: Platform dışı bakım onarım personeli) BGYS Yöneticisi, bu kişilerin Platform ile ilgili bilgi güvenliği politikalarından haberdar olmalarından sorumludur. Bu amaçla geçici ya da sürekli çalışma sözleşmelerinde sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları yapılmalıdır. Gerektiği takdirde üçüncü taraf personelinin politikaya uyması için süre tahsis edilmelidir.

Platform'un ilgili mevzuat gereği sistem entegrasyonu bulunan Merkezi Kayıt Kuruluşu, Takasbank A.Ş. ve Türksat (E-Devlet) ile yapılan veri paylaşımları bu maddenin kapsamına girmez.

Bilgi Güvenliği Politikasının Güncellenmesi ve Gözden Geçirilmesi

Madde 29 - Platform Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yöneticisi sorumludur. Bilgi Güvenliği Politikası organizasyonel değişiklikler, iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından değerlendirilir.

Bilgi Güvenliği Politikası Dokümanı, en az yılda bir kez gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa versiyon değişimi olarak kayıt altına alınmalı ve her versiyon üst yönetime onaylatılmalıdır. Her versiyon değişikliği tüm kullanıcılara e-mail, sunucu üzerinden ya da yazılı olarak yayımlanmalıdır. Gözden geçirmelerde;

- Politikanın etkinliği, kaydedilmiş güvenlik arızalarının yapısı, sayısı ve etkisi aracılığıyla gözlemlenmelidir.
- Politikanın güncelliği teknolojik değişimlerin etkisi vasıtasıyla gözlemlenmelidir.
- Politika, sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra gözden geçirilmelidir.

DÖRDÜNCÜ BÖLÜM
DİĞER HUSUSLAR

Politikada Yer Almayan Diğer Hususlar

Madde 30 - 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 31 - Politika hükümlerini değiştirme yetkisi iç kontrolden sorumlu yönetim kurulu üyesinin tavsiyesi ile yönetim kuruluna aittir.

Ekler:

Madde 32 - İşbu Politikanın ekleri şu şekildedir.

- İş Sürekliliği Planı,
  - İş Sürekliliği Yönetimi Prosedürü,
  - Acil Durum Eylem Planı,
  - Acil Telefonlar Listesi.

Yürütme

Madde 33 - Bu Politika hükümleri Ecofolio Kitle Fonlama Platformu A.Ş. tarafından yürütülür.

Yürürlük

Madde 34 - İş bu Politika hükümleri Ecofolio Kitle Fonlama Platformu A.Ş. Yönetim Kurulunun 07/02/2023 tarihli kararı ile kabul edilmiştir. İşbu Bilgi Güvenliği Politikası YK Karar tarihi itibarıyla yürürlüğe girer.

Doküman Adı :	İş Sürekliliği Planı
Versiyon :	1.0
Yayınlanma Tarihi :	
Dağıtım Grubu :	Tüm Çalışanlar
Uygulama Alanı :	Ecofolio Kitle Fonlama Platformu A.Ş.

Değişiklik ve/veya Ekler :

Versiyon	Tarih	Değişiklik Nedeni ve Kapsamı	İlgili Kişi

Onay :
Bu dokümanın, içerik ve düzeni gözden geçirilmiş ve onaylanmıştır.

Versiyon	Onaylanma Tarihi	Geçerlilik Tarihi	Onaylayan

1. AMAÇ

Kurumun faaliyetlerini destekleyen bilgi sistemleri servislerinin sürekliliğini sağlamak üzere BT Süreklilik Planı oluşturulması ve Üst Yönetim tarafından onaylanmasına yönelik bir süreç tasarlanması ve uygulamaya koyulması amaçlanır.

2. KAPSAM

Bu plan Ecofolio Kitle Fonlama Platformu A.Ş. ziyaretçileri, çalışanları ve BT varlıkları için güvenli bir çevre oluşturmayı, iç ve dış olağanüstü durumlar için hazırlıklı olmayı, olay anında ve sonrasında yapılacak işlemleri tanımlamayı kapsar.

3. TANIMLAR

Olağanüstü Durum: Can kaybı, yaralanma, fiziksel hasarlar, çevresel zararlar ile kurumun faaliyetlerini kısıtlayan beklenmedik, planlanmadık her türlü olaya / tehlikeye verilen isimdir.

BT Sürekliliği: Kurumun kritik süreçlerinin devamlılığını sağlamak, sağlanamadığı durumlarda ön görülen kesinti süreleri içerisinde yeniden çalışır hale getirmek için gerçekleştirilen çalışmalara verilen isimdir.

İş Etki Analizleri: Olası kesintilerin iş ve BT süreçlerine ve dolayısıyla kuruma olan etkisinin belirlenmesi çalışmasıdır. BT sürekliliğine yönelik olarak ilgili iş birimlerinin katılımı ile yapılan iş etki analizi çalışmaları ile kritik iş süreçleri ve bu kritik iş süreçlerini destekleyen BT servisleri belirlenir.

Kurtarma Süre Hedefi (RTO - Recovery Time Objective): Kesintiye uğrayan sürecin ne kadar süre sonra çalışır hale getirileceğine dair hedef süredir. Bu sebeple kesintiye uğrayan sürecin veya BT bileşeninin belirlenen RTO süresi içerisinde tekrar çalışır hale getirilmesi için gerekli planlamanın yapılması gereklidir.

Veri Kurtarma Hedefi (RPO-Recovery Point Objective): Kesintiye uğrayan sürecin veya BT bileşeninin ne kadarının kaybedilebileceğini gösterir. Ne kadar süre öncesine dönülebileceği anlamına gelir.

ODM: Olağanüstü Durum Merkezidir. Ecofolio Kitle Fonlama Platformu A.Ş.'nin Olağanüstü Durum Merkezi için, üçüncü parti firmadan hizmet alınmaktadır.

4. GÖREV VE SORUMLULUKLAR

BT Süreklilik Yöneticisi: Kurumun kritik süreçlerinde yer alan BT yazılım ve altyapılarının iş sürekliliğini yönetecek ve koordine etmekten sorumludur.
Acil Durum Ekibi: Felaket durumunda görev yapmak üzere oluşturulmuş ekiplerdir. Ekiplerde yer alacak personelin atamasını, değişikliğini, süresini BT Sürekliği Yöneticisi belirler.
Üst Yönetim: BT süreklilik planının yıllık olarak güncellenmesi ve onaylanmasından sorumludur.

5. UYGULAMA

BT Sürekliliği Planı'nın temel hedefi bir olay, kesinti veya felaket sonrasında Ecofolio Kitle Fonlama Platformu A.Ş.'nin kritik iş ve BT süreçlerini belirlenmiş kabul edilebilir süreler içerisinde, kabul edilebilir seviyede işlevsel hale getirmektir. BT sürekliliği planlamasının diğer hedefleri aşağıdaki gibi detaylandırılabilir:

- Olağanüstü Durum sırasında hataların oluşmasını önleyici süreçleri devreye almak, uygulamak ve iş yapış şekillerindeki hataları önlemek,
- Olağanüstü Durum sırasında kurum varlıklarının korunmasını sağlamak,
- Yasal yükümlülüklerin her an ve her zaman yerine getirilmesini sağlamak,
- Kurumun marka imajını ve saygınlığını korumak,
- Olağanüstü Durum sonucu katlanılacak maliyetleri en aza indirmek,

Olağanüstü Durum'un gerçekleşmesinden sonra Ecofolio Kitle Fonlama Platformu A.Ş.'nin yaklaşımı aşağıdaki maddeleri temel alacaktır:

- Personeli korumak ve sağlığından emin olmak,
- Olayın büyüklüğünü değerlendirmek,
- Tehditleri kontrol etmek,
- Olağanüstü Durum sonrasında ortaya çıkan sorunları ve sonuçları değerlendirmek,
- Kritik süreçleri belirlenen süreler içerisinde başlatmak ve iletişimi yönetmektir.

BT Sürekliliği Planı kapsamında dikkate alınan varsayımlar aşağıdaki gibidir:

- Birincil sistem ve bina içerisindeki çalışma ortamı ve ekipmanları (printer, fax, telefon vs.), BT sistemleri hasarlı veya kullanılamaz durumdadır.
- Olağanüstü Durum Merkezlerindeki BT altyapı ve sistemleri kullanılabilir durumdadır. Olağanüstü Durum sırasında BT sistemlerine uzaktan bağlanabilmek için gerekli altyapı hazır durumdadır.
- ODM'de yedeklenen BT servislerinin kritik iş süreçlerine yönelik tüm BT varlıklarını kapsamaktadır.
- Kurumda uygulama ve fonksiyonlar için gerekli veri kurtarma hedeflerine uygun yedekleme

mekanizmaları kurulmuş ve test edilmiş durumdadır.

- Kurumda çalıştırılacak uygulama ve işletilecek süreçler için gerekli veri kurtarma süreleri tahammül edilebilir kesinti süreleri ile uyumlu haldedir.
- Kritik dış tedarikçilerden hizmet alımlarının sürekliliğinde bir sorun bulunmamaktadır.
- Acil Durum Ekipleri'nde hem kendi ekip üyelerinin hem de diğer ekiplerdeki üyelerin erişim bilgileri mevcuttur. Kullanılabilen tüm iletişim araçları ile haberleşme sağlanır.
- Olağanüstü Durum'da çalışacak olan personel BT süreklilik planına hakimdir.
- Felaket durumunda uzaktan çalışabilecek personel belirlenmiş durumdadır. Uzaktan çalışma talimatları, gerekli donanımlar ve donanım üzerindeki uygulamalar (laptop, VPN, telefon), hesaplar hazır durumdadır.
- Uygulama ve altyapı sistemlerine erişim için kullanılan yönetici şifrelerinin güncel birer kopyası BT Yöneticisi'nin kontrolündeki bir kasada saklanır. Bu amaçla yönetici hesaplarına ait şifreler de arkası imzalı zarf içinde bu kasada korunur. Kasaya erişim için gerekli anahtar BT Süreklilik Yöneticisinin yetki verdiği iki (2) farklı kişide bulunur.
- E-posta sunucusu olarak Google altyapısı kullanıldığından BT Süreklilik Planında posta sunucuları kapsam dışı bırakılmıştır.

Acil Durum Ekibinin Yapılanması

Ecofolio Kitle Fonlama Platformu A.Ş. ve kritik üçüncü parti firmaların yapılanması aşağıdaki gibidir:

Ecofolio Kitle Fonlama Platformu A.Ş.:

Adı Soyadı	Departman	Mobil Telefon
Arif ÜNVER	Genel Müdür	5332839270
Burak Kamil UYANIK	İdari İşler	5422504690

Firmalar

Firma Adı	Sorumlu Temsilci	Telefon / E-mail
Innovation and Partners Yazılım ve Teknoloji Ltd. Şti.	Zafer Yasir YILMAZ	53677261865 yilmaz@innovatonandpartners.com
Innovation and Partners Yazılım ve Teknoloji Ltd. Şti.	Arif KAZANCI	5384816401 arif@innovatonandpartners.com

Innovation and Partners Yazılım ve Teknoloji Ltd. Şti.	Hamza KARAOGUL	5449429710 hamzakaraogul@innovatonandpartners.com

Olağanüstü Durum İlanı, Plan Başlatma Kararı ve Olağanüstü Durum Yönetimi

Olağanüstü durumlar iç ve dış olağanüstü durumlar olarak iki sınıfta değerlendirilir. İç Olağanüstü Durumlar aşağıdaki şekilde maddelendirilir:

- Yangın
- Su Basması
- Güç Kaynağı Kesintisi
- Personel Devamsızlığı
- İletişim Kesintisi
- Kurum BT Sistemlerinin Çalışmaması

Dış olağanüstü durumlar aşağıdaki şekilde maddelendirilir:

- Doğal Afetler (Deprem, Sel Basması)
- Terörizm
- İletişim Kesintisi
- Hırsızlık
- Protesto/Mitingler

HAZIRLAYAN:	ONAYLAYAN:

Bir olayın ya da önemli bir kesintinin Olağanüstü Durum olup olmadığı konusunda BT Sürekliliği Yöneticisi'nden gelen bilgiye göre karar verilir. Genel Müdür veya bu görevi delege ettiği ilgili yönetici bu bilgilendirmeye dayanarak Olağanüstü Durum'u ilan eder ve plan başlatma kararını verir.

Olağanüstü Durum İlan ve Plan Başlatma Kararı

Olağanüstü durumların önlenmesi ve zararlarının azaltılması amacıyla bir olağanüstü Olağanüstü Durumun kontrol altına alınmasına müteakip kurumun normal faaliyetlerini geri kazanma süreci başlar. Bu süreç içerisinde şirketin kritik süreçleri Olağanüstü Durum öncesine döndürülmesi için İş Etki Analizleri kapsamında belirlenecek öncelik sırasına uyulması gereklidir. BT sürekliliğine yönelik olarak ilgili iş birimlerinin katılımı ile yapılan iş etki analizi çalışmaları ile kritik iş süreçleri ve bu kritik iş süreçlerini destekleyen BT servisleri belirlenir. Kritik iş süreçlerine yönelik olarak her bir servis için kabul edilebilir kesinti süreleri belirlenerek, bu kesinti süresi içerisinde servisin tekrar erişime açılabilmesine imkân tanıyacak kurtarma süreçlerinin BT süreklilik planı içerisinde yer alması beklenmektedir.

BT Süreklilik Planında kritik olarak belirlenmiş sistemler:

Altyapı Sistemleri:

Internet Altyapısı : Turhost dedicated Sunucunun bağlı olduğu paylaşımsız olarak tahsis edilmiş internet altyapısı

Veritabanı : MySQL - Turhost dedicated Sunucu

Arkauç (Backend) API servisleri - Turhost dedicated Sunucu

Kritik Sistemler:

Web sitesi : ecofolio.com.tr - Turhost dedicated Sunucu

Yedek Sistemeler

DB, Backenend ve Frontend – Natro İzmir Bölgesi Sunucuları

Entegrastonlar:

MKK servisleri

Takasbank Servisleri

ParatikEcofolio Kitle Fonlama Platformu A.Ş. Sistemleri

Acil Durum Ekipleri iş bölümlerinin minimumda ihtiyacı olan personel ihtiyacına göre oluşturulur. Ayrıca ekiplerin normal faaliyetlerini geri kazanma süreci boyunca ihtiyaçları olacak ve kurtarılması gereken veriler İş Etki Analizlerinde tanımlıdır.

HAZIRLAYAN:	ONAYLAYAN:

BT Süreklilik Yöneticisi ile birlikte Genel Müdür, olağanüstü duruma geçiş gibi normale dönüş kararını vermeye yetkilidir.

BT Süreklilik Planının Test edilmesi

BT Süreklilik Planı kurum tarafından yıllık olarak, kurumun süreçleri ile organizasyonel yapıdaki değişiklikler dikkate alınarak gözden geçirilir ve söz konusu dokümanlarda gerekli değişiklikler gerçekleştirilir. Güncellemeler, iş birimleri sorumlularının geri bildirimlerinden yararlanılarak BT Süreklilik Yöneticisi tarafından gerçekleştirilir ve Genel Yöneticisin onayı alınır. Güncelleme süreci tamamlandıktan sonra ilgili personel ve bölümlerin haberdar olması sağlanır.

Planın güncellenmesinde aşağıdaki kriterler dikkate alınır:

- Geliştirilen yeni ürün ve hizmetler,
- Mevcut ürün, hizmet ve iş süreçlerinde gerçekleştirilen değişiklikler,
- Ürün, hizmetler ve iş süreçlerinde gerçekleştirilen değişiklikler nedeniyle ortaya çıkan yeni ekipman ve altyapı ihtiyaçları,
- Çalışma yerlerindeki altyapı değişiklikleri,
- Planda yer alan personelin transferi, işten ayrılması, terfisi, adres / telefon değişikliği veya kurumdaki organizasyon değişiklikleri,
- Hizmet alınan üçüncü tarafların, alınan hizmetlerin veya süreçlerin değişmesi,

Kurum personelinin olağanüstü durum organizasyon yapısı ve olağanüstü durum sırasında üzerlerine düşen görev ve sorumluluklar hakkında bilgi sahibi olması için BT Sürekliliği dokümanlarına Dokümantasyon Sistemi üzerinden erişim sağlanır. Plan, elektronik ortamda yer alan Dokümantasyon Sistemi ile birlikte, birincil merkezde ve Olağanüstü Durum Merkezi'nde basılı doküman olarak da saklanır.

Test planı kapsamında uygulama bazında test senaryoları, başarı kriterleri ve test personeli belirlenir. Test gerçekleştirilirken Acil Durum Ekipleri yanı sıra şirketin üçüncü parti firmalarından da ekipler bulunur.

Yukarıda tanımlanan kritik sistemler için aşağıdaki senaryolar belirlenmiştir:

Senaryo 1: Çalışanlar, olağanüstü durum nedeni ile İstanbul ofise ulaşamamaktadır.

Senaryo 2: Olağanüstü durum nedeni ile internet uzun süreli kesintiye uğramıştır.

BT sürekliliği planının hazırlanması aşamasında gerçekleştirilen iş etki analizleri sonucunda tüm Ecofolio Kitle Fonlama Platformu A.Ş. için bir iş kurtarma önceliği tespit edilmiştir. Faaliyetlerin geri kazanımları 6 ayrı zaman dilimine yayılmıştır. İş kurtarma sürecinde aşağıdaki önceliklendirme dikkate alınmıştır.

- Çok yüksek öncelikli faaliyetlerin geri kazanımı (ilk 4 saat içinde)
- Yüksek öncelikli faaliyetlerin geri kazanımı (1 gün içinde)
- Öncelikli faaliyetlerin geri kazanımı (2 gün içinde)

- Orta öncelikli faaliyetlerin geri kazanımı (4 gün içinde)
- Düşük öncelikli faaliyetlerin geri kazanımı (1 hafta içinde)
- Çok düşük öncelikli faaliyetlerin geri kazanımı (1 haftadan sonra)

İş süreçlerinin bağlı bulunduğu BT uygulamalarının önceliklendirme seviyeleri aşağıda belirtildiği gibidir.

Uygulama	Öncelik Seviyesi
İnternet Altyapısı	Çok yüksek öncelikli
Backend Servisleri	Yüksek öncelikli
Veritabanı	Yüksek öncelikli
Web sitesi	Yüksek öncelikli

BT Süreklilik Planı Eğitimi

BT Süreklilik Planı, tüm çalışanlarının erişebileceği şekilde tutulur. Çalışanlara BT Süreklilik Planı hakkında eğitim verilmesi sağlanır. Eğitim bölüm içi toplantılarla veya bilgilendirmelerle sağlanır.