

BİLGİ GÜVENLİĞİ POLİTİKASI

AMAÇ

Bu Bilgi Güvenliği Politikası, Fuze'un faaliyetleri kapsamında kullandığı Bilgi Sistemlerinin işletilmesi ve yönetilmesinde gizlilik, bütünlük ve erişilebilirlik kavramları dikkate alınarak hazırlanmıştır.

KAPSAM

Bu Politika, tüm Fuze çalışanları ve diğer tüm paydaşlar için geçerlidir.

UYGULAMA

Fuze, sahip olduğu verileri korumayı taahhüt eder. Müşterilerimiz ve diğer paydaşlarımız, kaynaklarının korunması konusunda bize güvenmektedir.

Üst yönetimimiz, bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı göstererek yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmiştir. Bu kapsamda aşağıdaki mekanizmalar oluşturulmuştur.

- Bilgi güvenliği politikalarının ve tüm sorumlulukların yılda en az bir kez gözden geçirilmesi ve onaylanması.
- Bilgi sistemlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetimi sürecinin oluşturulması.
- Bilgi güvenliği ihlallerinin takip edilmesi ve yılda en az bir kez değerlendirilmesi.
- Personele bilgi güvenliği gereksinimleri, riskler ve güncel tehditler konusunda bilgi düzeyini artırmaya yönelik eğitimlerin rol ve sorumluluklarına uygun şekilde yılda en az bir kez verilmesi.

Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen kontroller, Kurum, Kuruluş ve Ortaklıkların organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir ve işletimine ilişkin gözetim ve denetim süreçleri tesis edilir.

Asgari olarak kritik iş süreçlerini ve faaliyetlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak üzere iş sürekliliği planının bir parçası olan bilgi sistemleri süreklilik planı hazırlanır.

Görevler Ayrılığı İlkesi

Bilgi Sistemleri ve diğer operasyonel süreçlerdeki hataların veya kötüye kullanımların azaltılması için bir görevler ayrılığı ilkesi uygulanır.

Yüksek riskli veya finansal değeri yüksek işlemlerin tek bir kişi tarafından gerçekleştirilmemesi esastır.

Bilgi Güvenliği Sorumlusu

Herhangi bir Bilgi Sistemleri veya diğer Fuze bünyesindeki operasyonel süreçler içerisinde sorumluluğu bulunmayan, Bilgi Sistemleri Denetimi veya Bilgi Sistemleri Yönetişimi alanlarının en az birinde yetkinliğe sahip ve Fuze içerisindeki Bilgi Sistemleri faaliyetlerinin güvenliğini tesis etmekle görevli bir Bilgi Güvenliği Sorumlusu ataması yapılır.

Bilgi Güvenliği Sorumlusu tarafından, İç denetim raporunda yer alan tespitlere göre yapılacaklar gerçekleştirme tarihleriyle beraber bir aksiyon planına dönüştürülür, üst yönetime onaylatılır. Aksiyon planına uyum üst yönetim tarafından takip edilir ve bir sonraki iç denetim faaliyetinde dikkate alınır.

Veri Gizliliği

Fuze, operasyonel faaliyetlerde kullanılan veya üretilen tüm verilerin, başta bağlı olunan yasal mevzuatlar göz önünde bulundurularak korunmasını sağlar. Veri gizliliğinin korunmasında aşağıdaki başlıklar gözetilir:

- Verilerin güvenlik sınıfına uygun şekilde korunması.
- Verilere erişim haklarının kişilerin görev ve sorumlulukları çerçevesinde belirlenmesi, erişimlerin kayıt altına alınması, bu kayıtların yetkisiz erişim ve müdahalelere karşı korunması.
- Hassas verilerin tüm ortamlarda şifrelenerek saklanması, iletilmesi ve yedeklenmesi.
- Veri gizliliğini sağlamada şifreleme tekniklerinin kullanılması durumunda, güvenilirliği ve sağlamlığı ispatlanmış algoritmaların kullanılması; geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılmasının engellenmesi, verinin ve operasyonun önem düzeyine göre anahtarların değiştirilme sıklıklarının belirlenmesi ve anahtarların güvenli saklanması.

Fuze iç ağındaki verilerin, gizlilik seviyeleri temelinde dış ağa çıkışının kontrolleri DLP gibi araçlarla sağlanır.

Yasal olarak kullanım süresi dolmuş veya iş ihtiyacı kalmamış verileri içeren varlıklar uygun kullanım sırasına göre fiziksel imha, manyetik yok etme (degaussing), kriptografik silme veya yazılımsal silme (wipe) yöntemlerinden biriyle Fuze ağından kaldırılır.

Kişisel veriler, ulusal veya uluslararası yasaların gerektirdiği kurallar neticesinde toplanır, saklanır ve imha edilir.

Müşterilerin Bilgilendirilmesi

Müşteriler, Fuze platformlarını kullanmadan önce hem platformların genel riskleri hem de diğer bilgi güvenliği zafiyetleri konusunda bilgilendirilir.

Müşterilerin Fuze ürünlerini kullanırken herhangi bir sorun yaşamaları halinde, Fuze ile nasıl iletişime geçebileceklerine ilişkin bilgilendirme müşterilere sağlanır.

Müşterilerin Dikkat Etmesi Gereken Sektör Riskleri

Müşteriler, Fuze'un doğrudan müdahale edemeyeceği, kripto varlık alanındaki aşağıdaki riskler ile ilgili farkındalığını oluşturmalıdır:

- Müşteri IBAN'larına veya cüzdan adreslerine yönelik **sosyal mühendislik** faaliyetleri sebebiyle, kripto varlıkların veya geleneksel paraların istenmeyen taraflara aktarımı
- Kullanıcıların web sitelerine ait kimlik doğrulama veya diğer hassas verilerinin çalınması (**XSS**)
- Kullanıcıların oturumları açıkken, oturumlarının açık olduğu başka web sitelerinde finansal işlem yapacak linklere tıklaması veya diğer işlemleri gerçekleştirmesi (**CSRF**)
- Firmanın şifreleme protokolleri desteklemeyen veya güncel olmayan tarayıcıların kullanılması
- Müşterilerin kendi cihazlarındaki yetersiz anti-virüs koruması nedeniyle maruz kalınabilecek erişim veya kullanım problemleri
- Müşterilerin e-postalarına veya telefonlarına gelen linklere tıklaması nedeniyle doğabilecek zararlar (**Oltalama**)

Müşterinin Sorumlulukları

Müşteriler Fuze web platformlarını kullanırlarken;

- Sitenin firmaya ait olduğunu doğrulamak
- Şifre belirlerken platformun belirlediği kurallara uymak ve mevcut şifrelerini paylaşmamak
- Tek kullanımlık kimlik doğrulama verilerini ve kendi hesabını kimseyle ortak kullanmamak
- Fuze platformlarında oturumları açıkken oturumlarının açık olduğu diğer platformlarda, özellikle finansal süreçlerini etkileyen işlemler yapmamak
- Hesabının çalındığını, olası bir dolandırıcılık olayı yaşadığını veya herhangi anormal bir durumla karşılaştığı senaryoda Fuze ile doğrudan iletişime geçmek

Üçüncü Taraflarla Bilgi Değişimi

Fuze platformlarında oluşan veya kullanılan bilgilerin müşteri dışında bir tarafa aktarılması konusunda, başta ulusal ve uluslararası yasalar olmak üzere, tüm parametreler göz önünde bulundurulur.

Fuze, müşteri verilerini yetkili kamu kurum ve kuruluşları dışında hiçbir üçüncü tarafa paylaşmamaktadır.

Uyumsuzluk

Bilgi güvenliği ihlali veya ihlal şüphesi halinde;

- Olay derhal değerlendirilir,
- Gerekli teknik ve idari önlemler alınır,
- Mevzuat kapsamında gerekli bildirimler yapılır.