Bilgi Güvenliği Politikası

Bilgi Güvenliği Politikasının amacı, hukuka, yasal düzenleyici ya da sözleşmeye tabi yükümlülüklere bilgi güvenliği gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetimin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat kurum açısından en önemli varlıklardan biridir. Bilgi güvenliği yönetim sistemimiz ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardına uygun olarak kurulmuş ve bu standardın gerekliliklerini karşılayacak şekilde PUKÖ (Planla, Uygula, Kontrol Et, Önlem Al) sürekli iyileştirme döngüsü çerçevesinde bir süreç olarak uygulanmaktadır. Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımızın genel özeti bu politikada verilmektedir. Uygulama detay bilgileri için sistem dokümantasyonuna, ilgili prosedürlere, rehberlere, planlara ve raporlara bakılmalıdır. Bu politika bilgi güvenliği politikası ve detaylı kullanım politikalarını da kapsayan bir üst dokümandır.

Bilgi kaynakları, ofis ve cihazlar gibi Tugay açısından büyük önem taşıyan varlıklardır. Bilgi varlıklarını ve kaynaklarını kullanan veya bilgi sağlayan herhangi bir kişi, bilgi varlıklarını korumakla yükümlüdür. Ortak bilgi varlıklarını kullanan tüm çalışanların, gereken duyarlılığı göstermesi ve diğer meslektaşlarını, kurum çalışanlarını ve kurumsal değerleri gözeterek hareket etmesi beklenir. Kurumsal değerlerin gereği olarak gizliliğe önem verilir, her türlü kişisel bilgi en yüksek güvenlik standartlarına sahip sistemlerle korunur. Bilginin sahibi istemedikçe, yetki verilmedikçe veya yasal gereklilikler oluşmadıkça bilgi paylaşılmaz.

Tugay için tüm bu bilgi varlıkları ve kaynakları içerisinde en kritik olanı, özenle korunması, gizliliğinin sağlanması, ihtiyaç duyulduğu anda erişilmesi gereken bilgi varlıkları, ofiste ve sunucu hizmeti alınan Netinternet Bilişim Teknolojileri firmasında dır. (Veri merkezi) Bilgi varlıkları ve kaynakları farklı konumlarda veya ortamlarda bulunabilir. Hangi konumda veya ortamda olursa olsun müşteri iletişim gereksinimleri ve kurumsal değerler bu varlıkların ve kaynakların kullanımını belirler. Bilgi güvenliği, sadece bilginin gizliliğinin değil, bütünlüğünün ve kullanılabilirliğinin de sağlanması ile mümkündür. Bilginin gizlilik gerekliliği, sadece yetkilendirme

dâhilinde gereken bilgi varlıklarına erişim verilmesi anlamına gelir. Bilginin bütünlüğü, tüm bilgi varlıklarının tamlığını ve doğruluğunu sağlamayı gerektirir. Bilginin kullanılabilirliği, bilgi varlıklarının ihtiyaç duyulduğu anda ulaşılabilir ve kullanılabilir olması anlamına gelir.

Bilginin kullanımı, yerleşimi ve korunması ile ilgili ihtiyaçların karmaşıklığı ve çokluğu, kapsamlı ve geniş bilgi güvenliği süreçlerinin ve politikalarının tanımlanmasını zorunlu kılmaktadır. Bu nedenle belirlenen süreçler doğrultusunda bilgi güvenliği riskleri, bilgi varlığından sorumlu olan kişiler tarafından değerlendirilir, risklerin önceliği belirlenir ve gereken önlemler alınır.
Sistem odası ve sunucuların güvenliğinin sağlanması öncelikli olarak ele alınır. Varlık envanterinin ve bu envanterin olası risklerinin önceden belirlenerek müşterilerin güven içinde ve kesintisiz hizmet almaları için çalışılır. Karar ve eylemlerde, güvenilir nesnel bilgiler ile teknolojinin tüm olanaklarının kullanılmasına önem ve öncelik verilir. Hareketler sezgilere, duygulara ya da doğru görünene göre değil; bilimsel ve teknolojik gerçeklerin ortaya koyduğu objektif esaslara göre düzenlenir. Bunu sağlamak için bilgi dünyadaki en ileri kaynaklardan transfer edilir, benimsenir ve mesleki uygulamalar bu doğrultuda yapılır. Kaynaklar verimli kullanılarak teknolojiye yatırım yapılır, gelişim bu doğrultuda sürdürülür.

Bu nedenle bilgi güvenliği yönetim sisteminin planlama, uygulama, izleme ve iyileştirme adımları ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına ve bu standardı destekleyen standartlara uygun olarak yürütülür.

Bilgi Varlığı

Tugay'ın sahip olduğu, işlerini aksatmadan yürütebilmesi için önemli olan varlıklardır. Bu politikaya konu olan bilgi varlıkları aşağıdaki gibidir ;

- Kâğıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri
- Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım
- Bilginin transfer edilmesini sağlayan ağlar
- Bölümler, birimler, ekipler ve çalışanlar
- Ofis ve Özel alanlar
- Çözüm ortakları
- Üçüncü taraflardan sağlanan servis ve hizmetler

Bilgi Varlıklarının ve Kaynaklarının Kullanımı

Tugay'da yürütülen işlerin sürekliliğinin ve gelişiminin sağlanması nedeniyle, bilginin gizliliğinin korunması öte yandan bilginin ve fikirlerin paylaşılması ve yaygınlaştırılması gerekir. Bilginin hassasiyeti ve güvenliği ile ilgili ihtiyaçlar gözetilirken, aynı zamanda bilgiye ihtiyaç anında hızla ulaşılması büyük önem taşımaktadır. O nedenle, bilgi kaynaklarının değerinin iyi tespit edilmesi, bilginin

korunmasını sağlayacak çaba ve maliyetin bilginin hassasiyeti ile orantılı olması gerekir. Tugay'ın bilgi kaynaklarını kullanarak etik dışı veya yasalara karşı faaliyetlerde bulunmak, hiç kimse için kabul edilemez bir durumdur. Politikanın asgari gereği olarak ;

- Verinin kasıtlı olarak değiştirilmesi
- Kasıtlı olarak veri' de hataların oluşmasına veya veri kaybına neden olunması
- Bilgi kaynaklarının yasaları ihlal eden bir faaliyet için kullanılması
- Bilgi güvenliğinin ihlal edilmesi veya suiistimal edilmesi
- Cihazların, yazılımların veya herhangi diğer bir bilgi kaynağının çalınması, tahrip edilmesi
- Bilgi kaynaklarının bilişim sistemlerinin performans kaybına sebep olacak şekilde kullanılması
- Tesislerin, fiziksel cihazların, ağların tahrip edilmesi kabul edilemez

Bu ve benzeri faaliyetler ve teşebbüsler disiplin suçu olarak ele alınır, gereken disiplin süreçleri ve yasal süreçler disiplin prosedürüne göre disiplin kurulu tarafından uygulanır. Belirtilen tarzda bilgi güvenliği ihlallerinin, ihlal teşebbüslerinin veya bu tür ihlaller ile sonuçlanabilecek zafiyetlerin, tespit edildiği anda zaman kaybetmeden Bilgi Güvenliği Yöneticisi ve/veya Bilgi Güvenliği Sorumlusuna bildirilmesi gerekir.

Bilgi Güvenliği Organizasyonu

Tugay Siber Savunma Sistemleri 6 bölüm / departmandan oluşmaktadır ;

- Üst Yönetim
- Satış / Pazarlama
- Muhasebe / İnsan Kaynakları
- Bilgi Güvenliği
- Ar-Ge / Yazılım
- Teknik Destek

Sorumluluklar

Üst Yönetim

- Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesi için gerekli kaynak ve yetki / sorumluluk tahsislerini gerçekleştirir
- Sertifikasyon kapsamı için yönetim sistemine sahiplik ve sponsorluk yapmak
- Yönetim kararı gerektiren sorunları çözmek ve karar taleplerini karara bağlamak
- BGYS kapsam ve politikasını onaylamak

Bilgi Güvenliği Yöneticisi / Sorumlusu

- BGYS kurulum çalışmalarını koordine etmek
- BGYS kurulum ve operasyon çıktılarını gözden geçirmek ve geri bildirimde bulunmak
- Bilgi güvenliği uzman bakış açısı ile riskleri giderici uygun kontrollerin seçimini sağlamak
- BGYS'nin temelini oluşturan varlık envanteri hazırlama ve risk analizi çalışmalarının uygun şekilde gerçekleştirilmesini koordine etmek
- BGYS işletim modelini ve uygulanan süreçlerin uyumluluğunu gözden geçirmek
- Çalışanların BGYS hakkında bilgilenmelerini sağlayacak mekanizmaların işletilmesini sağlar
- Çalışanların bilgi güvenliğine ilişkin olarak karşılaşabileceği riskleri anlamasını ve tanımasını gerçekleştirecek eğitici yöntemlerin kullanımını koordine eder
- Güvenliği sağlamaya yönelik olarak tespit edilen ihtiyaçların karşılanmasını talep eder
- Bilgi güvenliği standartlarının kontrolü ve denetimini yapar

Bilgi Güvenliği Kurulu

Bilgi Güvenliği Kurulu (BGK) aşağıdaki kişilerden oluşur;

- Bilgi Güvenliği Sorumlusu
- Bilgi Güvenliği Yöneticisi
- Komisyon Üyeleri

BGK, altı ayda bir, Bilgi Güvenliği Yöneticisinin oluşturduğu gündem çerçevesinde toplanır. Bu toplantılar aynı zamanda yönetim gözden geçirme toplantılarıdır. Toplantılarda görüşülen konular aşağıda belirtilen maddeleri içerir, ancak bunlarla sınırlı kalmayabilir;

- Bilgi Güvenliği Politikasının gözden geçirilmesi.
- Risk Yönetim Metodolojisinin onaylanması.
- Güncel risk raporunun değerlendirilmesi.
- Kabul edilebilir risk seviyesinin Genel Müdür tarafından onaylanması.
- Kabul edilebilir risklerin Genel Müdür tarafından onaylanması.
- Risk işleme planının Genel Müdür tarafından onaylanması.
- Güvenlik ihlal olaylarının değerlendirilmesi.
- İş süreklilik stratejisinin gözden geçirilmesi.
- İş sürekliliği tatbikat sonuçlarının değerlendirilmesi.
- Bilgi güvenliği bilinçlendirme çalışmalarının gözden geçirilmesi.
- İç denetim raporlarının değerlendirilmesi.
- Kurumu etkileyebilecek önemli değişiklikler.
- Bu politika Tugay Siber Savunma Sistemleri Genel Müdürü tarafından gözden geçirilmiş ve onaylanmıştır.

Genel Kurallar

- Bu politika ile belirlenen genel kurallar, aksine istisnalar belirtilmedikçe stajyerler de dâhil tüm çalışanlar ve iş ortakları için geçerlidir.
- Özel bir görev/koşul gereği bu kurallara istisna oluşturacak durumlar için, ilgili standart ve talimatlarla gerekli güvenlik kuralları tanımlanır.
- Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar referans verilen BGYS Prosedürleri ile düzenlenir. Çalışanlar ve iş ortakları bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdürler.
- Bu kural ve prosedürlerin, aksi belirtilmedikçe, kâğıt veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün endüstriyel kontrol sistemleri ve bilgi işlem sistemlerinin kullanımı için dikkate alınması esastır.
- Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27001:2013 “Information Technology — Security Techniques — Information Security Management Systems — Requirements" standardını temel alarak yapılandırılır ve işletilir.
- BGYS’nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların da katkısıyla Bilgi Güvenliği Sorumlusu / Yöneticisi yürütür.
- Şirket tarafından çalışanlara veya firmalara sunulan her türlü endüstriyel kontrol sistemleri ve bilgi işlem sistemi ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün, aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça Tugay Siber Savunma Sistemleri'ne aittir.