RGN İLETİŞİM HİZMETLERİ A.Ş

BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi Güvenliği Yönetim Sistemimiz TS ISO / IEC 27001:2013 standardına uygun olarak kurulmuş ve bu standardın gerekliliklerini karşılayacak şekle sürekli iyileştirme döngüsü çerçevesinde uygulanmaktadır.

Bilgi güvenliğinin hedefi her seviyede kullanıcıya bilgi sistemleri kullanımları sırasında ne şekilde hareket etmeleri gerektiği konusunda yol göstermek, kullanıcıların bilinç ve farkındalık seviyelerini arttırmak ve bu şekilde bilgi sistemlerinde oluşabilecek riskleri minimuma indirmek, RGN' nin güvenilirliğini ve imajını korumak, üçüncü taraflarla yapılan sözleşmelerde bilgi güvenliği gereksinimlerini oluşturmaktır. Ayrıca tedarikçi hizmetlerindeki değişiklikleri yöneterek RGN' nin iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak ve bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğinin sağlanması hedeflenmektedir.

2. KAPSAM

Bilgi Güvenliği Yönetim Sistemi kapsamı olarak RGN bilgi varlıkları, süreçleri, sistem odası, departman odaları, insan kaynakları ve üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ayrıca bilgi sistemleri yapısına hizmet, yazılım veya donanım destek sağlayıcılarını kapsamaktadır. Kanun ve yönetmeliklere uyum bilgi güvenliği kapsamındadır.

3. TANIM

Bilgi Güvenliği: Bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin temin edilmesi ve korunmasıdır:

Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği.

Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliği.

Erişilebilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.)

4. GÖZDEN GEÇİRME VE ONAY

Politikanın sürekliliğinin sağlanmasından ve gözden geçirilmesinden Üst Yönetim sorumludur. BG politikası organizasyonel değişiklikler, iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından değerlendirilir. BG politikası en az yılda 1 kez gözden geçirilir. Bunun dışında sistem yapısını ve risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilir. Güvenlik politikasının güncellenmesi için yeter şartlar aşağıda sıralanmıştır;

- Sistem bileşenlerinde değişiklik olması
- Yeni tipte güvenlik ihlallerinin çıkması
- Mevzuatta, kurumsal süreçlerde ya da işletim talimatlarında değişiklik yapılması
- Güvenlik gereksinimlerinde değişiklik olması

RGN Bilgi Güvenliği Politikası gözden geçirilirken aşağıda listelenen hususlar özellikle göz önünde bulundurulmaktadır:

- Mevcut politikanın etkinliği ve yeterliliği
- Tercih edilen güvenlik önlemlerinin ve korunan varlıkların değerleri
- Teknolojideki değişiklikler

Her güncellemede politika Üst Yönetim tarafından onaylanır. Her versiyon değişikliği tüm kullanıcılara e-mail ve dosya sunucu üzerinden yayımlanır.

5. EĞİTİM

Tüm RGN personeline ve uygun durumlarda üçüncü parti personellere, ilgili politika, talimat ve yönergeler hakkında gerekli eğitimler verilir. Eğitim kapsamına giren kurallar bütününde muhtemel değişiklik ve güncellemeler gerçekleştikten sonra güvenlik eğitimleri tekrarlanır. Değişiklik olmaması durumunda dahi muhtemel personel/kadro değişiklikleri sebebiyle eğitimler tekrarlanabilir. Eğitim içerikleri, katılımcılar için özelleştirilebilir.

6. YÖNETİMİN TAAHHÜDÜ

RGN Yönetimi, belirlediği hedef ve politikalarını gerçekleştirmek için Bilgi Güvenliği Yönetim Sisteminin standartta belirtilen gereksinimlerini yerine getirecek şekilde kurarak yürütür. Üst yönetim, tanımlanmış, yürürlüğe girmiş ve uygulanmakta olan BG Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştirileceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder.

7. BİLGİ GÜVENLİĞİ POLİTİKASI

7.1 Genel Esaslar

7.1.1 Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS prosedürleri ile düzenlenir. RGN çalışanları ve 3. Taraf bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

7.1.2 Bu kural ve prosedürlerin aksi belirtilmedikçe basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.

7.1.3 Kritik iş süreçlerini büyük felaketlerin ve işletim hatalarının etkilerinden korumak amacıyla iş sürekliliği yönetimi uygulanır.

7.1.4 Çalışanların bilgi güvenliği farkındalığını artırmak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut firma çalışanlarına ve yeni işe başlayan çalışanlara verilir.

7.1.5 Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir, ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.

7.2 Temel Prensipler

7.2.1 Gerekli durumlarda çalışanlar ve üçüncü taraflarla RGN' nin gizlilik ihtiyaçlarını güvence altına almayı amaçlayan gizlilik anlaşmaları yapılır.

7.2.2 Dış kaynak kullanım durumlarında oluşabilecek güvenlik gereksinimleri analiz edilecek güvenlik şart ve kontrolleri şartname ve sözleşmelerde ifade edilir.

7.2.3 Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahipleri atanır.

7.2.4 İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.

7.2.5 Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.

7.2.6 Firmaya ait bilgi varlıkları için firma içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.

7.2.7 Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.

7.2.8 Erişim hakları ihtiyaç doğrultusunda atanır. Erişim kontrolü için mümkün olan en güvenli teknikler kullanılır.

7.2.9 Kritik altyapı için süreklilik planları hazırlanır ve tatbikatı yapılır.

7.2.10 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.

8. UYULMASI GEREKEN BGYS KURALLARI

8.1 Çalışma alanlarında "Temiz masa ve Temiz ekran" prensiplerine uygun olarak, hizmete özel bilgiler dışındaki bilgilerin başkalarınca görülmesine imkan verilmeyecek şekilde önlemler alınmalıdır.

8.2 Bilgisayarlar aktif kullanım dışındayken şifreli ekran koruyucular devreye alınmalıdır.

8.3 Mesai zamanları dışında bilgisayar sistemleri kapalı tutulmalıdır.

8.4 Çalışanlar, kendilerine ait olan kullanıcı adı ve şifrelerini sadece kendileri kullanmalıdır.

8.5 Hassas bilgiler elektronik ortamda firma içine ve özellikle firma dışına gönderilmeden önce şifrelenmelidir.

8.6 RGN' ye ait bilgi işlem sistemlerini, veritabanlarını, dosyaları, ağ topolojilerini vb. kaynakları firma tarafından açıkça yetkilendirilmedikçe 3. Taraflarla paylaşılmamalıdır.

8.7 RGN çalışanları, çalıştıkları sürece veya RGN' den ayrılmaları durumunda firma bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur.

8.8 3. Taraflar ile gizlilik sözleşmesi imzalanmadan ve ilgili kişi tarafından nezaret edilmeden bilgi işlem sistemlerine ve donanımlarına bağlanmamalı ve çalışmalarına izin verilmemelidir.

9. VARLIKLARIN SINIFLANDIRILMASI

RGN bünyesinde kullanılmakta olan her varlık envanter kayıtlarına geçirilir. Envanter kayıtları sürekli olarak güncel tutulur ve yeni varlıkların envanter kayıtlarına hemen girmesi önerilir. Bilgi varlıklarının sahipleri atanarak envanter listesi hazırlanır. Tüm bilgi, veri ve dökümanlar anlaşılır bir biçimde etiketlenir.

10. ÜÇÜNCÜ TARAF ERİŞİMİ

Üçüncü şahıs ve kurumların RGN ve RGN bilgi sistemlerine erişimlerinin güvenli olarak gerçekleştirilmesi amacıyla gerekli düzenlemeler yapılır. Bu çerçevede, riskler analiz edilir, erişim gereksinimleri belirlenir ve sınıflandırılır. Anlaşmalı kurumların personeli ve diğer üçüncü taraflar için ilkeler belirlenir ve uygulanır. Üçüncü taraf erişimleri için uygun risk analizi yapılır. Güvenlik sorumluluklarını da içeren hizmet sözleşmeleri hazırlanır.

11. FİZİKSEL VE ÇEVRESEL GÜVENLİK

RGN'de fiziksel ve çevresel güvenliğin eksiksiz olarak sağlanması amacıyla düzenlemeler ve denetimler yapılır. Hassas varlıkların bulunduğu ve hassas süreçlerin yapıldığı yerler güvenlikli olmak zorundadır. RGN güvenli bölgeleri bu amaçla hazırlanır ve bu bölgelerin güvenliği sağlanır. İhtiyaca göre farklı güvenlik seviyeleri tanımlanarak her bir seviye için farklı güvenlik mekanizmaları devreye sokulabilir. Fiziki güvenlik çevresi oluşturulur ve fiziki giriş denetimleri yapılır. Bürolar, odalar ve araçlar güvenlik altına alınır. Güvenli alanlarda çalışmanın usul ve esasları belirlenir. Donanım güvenliği düşünülerek bu cihazların yetkisiz fiziksel erişim, yangın, su baskını gibi tehdit ve tehlikelere karşı korunması sağlanır. Donanımların yerleştirilmesi, güç kaynaklarının kurulumu, kablolamanın gerçekleştirilmesi güvenlik düşünülerek yapılır. Donanımların düzenli bakımı gerçekleştirilir. Donanımların yapılandırılması esnasında güvenlik ilkelerine dikkat edilir.

12. RİSK YÖNETİM ÇERÇEVESİ

RGN, risk yönetimi çerçevesi; Bilgi Güvenliği ve Hizmet Yönetimi risklerinin tanımlanması, değerlendirilmesini ve işletilmesini kapsar. Risk Analizi ve Risk İşleme Planı risklerin nasıl kontrol edildiğini tanımlar. Risk işleme yönteminden Bilgi Güvenliği Komitesi sorumludur. Risklerinin değerlendirme işlemi ve uygun risk tedavi planının hazırlanıp uygulamaya geçirilmesi devamlı bir süreçtir.

13. İŞ SÜREKLİLİĞİ

RGN yönetimi iş süreklilik ilkelerini belirler ve iş süreklilik ilkelerinin hayata geçirilmesi için bir iş süreklilik planı oluşturulmasını ve değişen koşullara göre güncel tutulmasını sağlar. Güncel iş sürekliliği planı, ilgili roller ve sorumluluklar RGN İş Sürekliliği Planı'nda belirtilir.

14. YASAL UYUMLULUK

RGN, faaliyet alanları ile ilgili yayınlanmış kanun, yönetmelik ve tebliğlere uygun olarak hizmet vermek için gerekli tüm çalışmaları yapar.

15. FİKRİ MÜLKİYET HAKLARI

RGN sistemlerinde, fikri mülkiyet hakkı taşıyan ürün, yazılım, hizmet veya sistemler sahibinden izin alınmadan veya kullanım lisansı olmadan kullanılamaz.

16. SÜREKLİ İYİLEŞTİRME VE DÜZELTİCİ FAALİYET

İç tetkiklerde, ihlal olaylarıyla veya kullanıcının kendi gözlemleriyle tespit ettikleri uygunsuzlukların tespitinde ve standartta, politikalarımıza, prosedür ve kurallarımıza uymayan durumların tespitinde ortaya çıkan uygunsuzluğun nasıl giderileceğine ilişkin Düzeltici Faaliyet Prosedürü uygulanmaktadır.

17. DEĞERLENDİRME

Bilgi güvenliği kapsamında yapılan tüm çalışmalar risk analizi, varlık envanteri, iç ve dış denetimler, farkındalık eğitimleri vb. çalışmalar Bilgi Güvenliği Komitesi ve Yönetim Gözden geçirme toplantılarında ele alınır ve değerlendirilir.

18. DENETİMLER

RGN Bilgi Güvenliği Yönetim Sistemi, yılda bir defa, RGN iç denetim ekibi tarafından denetlenir. Ayrıca Bilgi Güvenliği Komitesinin gerek görmesi halinde üçüncü taraf bağımsız denetim uzmanlarından bağımsız denetim hizmeti veya iç denetimlere danışmanlık hizmeti alınabilir.

19. YAPTIRIM

RGN veya Müşterilerine veya Tedarikçilerine ait bilgilerin güvenliğini tehlikeye atacak her hangi bir kasti hareket, disiplin cezasına ve/veya hukuki (bilişim suçları) önleme tabidir.

20. YÖNETİM DESTEĞİ

RGN İletişim Hizmetleri A.Ş Genel Müdür bilgi güvenliğinin tesis edilmesi için gerekenin yapılacağını açıkça ifade eder. Yönetim, bilgi güvenliği tesisinde ve güvenlik denetimleri esnasında hızlı ve etkili olunabilmesini destekler.

Saadet Gonca Ergün
RGN İletişim Hizmetleri A.Ş
Genel Müdür