BGYS POLİTİKASI

BGYS politikası, yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır. Bu politikada tüm bölümleri ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır.

1. AMAÇ

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde erişilebilirliğini sağlamaktır. Bilgi diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat kurum açısından en önemli varlıklardan biridir. Bilgi güvenliği yönetim sistemimiz TS ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Standardına uygun olarak kurulmuş ve bu standardın gerekliliklerini karşılayacak şekilde 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. Yönetim tarafından onaylanmış ve yayınlanmıştır. Yönetim tarafından düzenli olarak gözden geçirilmektedir.

2. KAPSAM

KABLOSUZ AĞLAR ÜZERİNDEN İNTERNET ERİŞİMİNİN SAĞLANMASI olarak belirlenmiştir.

3. TANIMLAR ve KISALTMALAR

a- BGYS: Bilgi Güvenliği Yönetim Sistemi

b- **BTHYS:** Bilgi Teknolojileri Hizmet Yönetim Standardı

c- Risk Yönetimi: Bilgi güvenliği risklerinin analizi, değerlendirilmesi, işlenmesi ve sürekli iyileştirilmesi amacıyla yürütülen yönetimsel faaliyetler.

d- Risk Analizi: Tehdit ve iş etkisinin çarpımı olan risk puanının bulunması amacıyla her bir bilgi varlığı için zayıflıkların, tehditlerin, iş etkilerinin bulunması ve hesaplanması çalışması.

e- Risk Değerlendirme: Risk analizi sonucunda bulunan değerlerin yorumlanması ve derecelendirilmesi.

f- Risk İşleme: Risk değerlendirme sonuçlarına bağlı olarak kaçınma, kabul, kontrol, transfer seçeneklerinden birinin seçilmesi ve uygulama planı.

g- Artık Risk: Risklerin işlemeden sonra kalan miktarıdır.

h- Risk Derecelendirmesi: Riskin önemini tayin etmek amacıyla tahmin edilen riskin, verilen risk kriterleri ile karşılaştırılması sürecidir.

i- Riskin Kabulü/Kabul edilebilir Risk: Bir riski kabul etme kararı. Bir riskin zararını (negatif sonuçlarını) kabullenme.

j- Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar.

k- Bilgi güvenliği ihlal olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

l- Bilgi güvenliği yönetim sistemi (BGYS) : Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir.

m- Uygulanabilirlik Bildirgesi (SOA-Statement of Applicability): Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirgedir. Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır.

n- Etki: İş hedeflerinin başarısını etkileyen değişim.

o- Bilgi Güvenliği Riski: Açıklıklardan fayda sağlamak suretiyle kuruluşa zarar verebilecek varlık ya da varlık gruplarının potansiyel tehdididir. Bir olayın ve sonucunun olasılığının kombinasyon koşulları olarak ölçülür.

p- Riskten kaçınma: Riski oluşturan durumdan kaçınma kararıdır.

q- Risk iletimi: Karar verici veya diğer ortaklar arasında risk hakkındaki bilgiyi paylaşım ya da değişimdir.

r- Riski belirleme: Riski oluşturan öğelerin ortaya çıkartılması, tasnif edilmesi ve özelliklerinin belirlenmesini içeren süreçtir.

s- Riski transfer etme: Bir riskin kayıplarını diğer paydaşlarla paylaşma. (Sigorta yaptırma gibi)

t- YGG: Yönetimin Gözden Geçirilmesi

u- PUKÖ: Planla, Uygula, Kontrol Et, Önlem Al

4. BİLGİ GÜVENLİĞİ HEDEFLERİ VE PRENSİPLERİ

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir. Her bir varlık için risk seviyesinin kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir. Risk yönetimi ve kontrollerin uygulanması sürekli bir faaliyettir ve kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılması hedeflenmektedir.

5. BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU

5.1.BGYS TAKIMI VE YETKİLERİ

bu politika metninde madde-2 de tarif edilen kapsam dahilinde TSE ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerini yürütmek üzere, BGYS Sorumlusu ve BGYS Yöneticisi Atanmış, BGYS KOMİTESİ kurulmuştur.

BGYS SORUMLUSU

BGYS YÖNETİCİSİ

BG Üst Yönetim Görev, Yetki ve Sorumluluklar:

- Bilgi Güvenliği Politikasını onaylamak.
- Güvenlik Politikasının kurum içinde uygulanmasına destek vermek.
- BGYS sorumlusunu atamak.
- Bilgi Güvenliği konularında geliştirilen politikaları uygulamak amacı ile gerekli altyapıyı oluşturmak üzere hazırlanmış projelere gerekli kaynağı sağlamak
- Çalışmaların yürütülebilmesi için yatırım kararlarına ve üçüncü taraf hizmet alımlarına onay vermek.
- Belirli aralıklarla yapılacak olan BGYS YGG (Bilgi Güvenliği Yönetim Sistemi Yönetim Gözden Geçirme) toplantılarına başkanlık etmek.
- Kurum bünyesinde bilgi işleme olanaklarını kullanarak bilginin üretilmesini, taşınmasını, geliştirilmesini, yönetilmesini ve saklanmasını sağlayan tüm çalışanlarda (Danışmanlar ve yüklenici firma personeli dahil) Bilgi Güvenliği farkındalığının artırılmasına yönelik planlanan çalışmaların etkinliğinin artırılması için teşvik edici faaliyetleri onaylamak.
- Bilgi Güvenliği konularında yapılacak olan çalışmalarına işlerlik kazandırmak, sürdürmek iyileştirmek ve gözden geçirmek için gerekli iç denetimlerin yapılmasına onay vermek.
- Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak.

BG Sorumlusu Görev, Yetki ve Sorumluluklar:

- BGYS politikalarını gözden geçirerek uygunluğuna karar vermek, üst yönetimin onayını almak
- BGYS kurulması ve işletilmesi için gerekli kaynak ve sorumluluk tahsislerini gerçekleştirmek,
- BGYS Yöneticilerini atamak,
- BGYS için hazırlamış dokümanları onaylamak ve uygulanmasını sağlamak,
- BGYS Kontrollerini gözden geçirerek uygunluğuna karar vermek.
- Gereken iyileştirmeler ve geliştirmeler konusunda gerekli bilgi akışını sağlamak.

- Risk Kabul Kriterlerinin uygunluğuna karar vererek üst yönetime sunmak
- BGYS konularında geliştirilen politikaları uygulamak üzere oluşturulan altyapının uygunluğuna karar vererek üst yönetimin onayını almak.

BG Yöneticisi Görev, Yetki ve Sorumlulukları:

- BGYS Politikasını hazırlamak ve BGYS yöneticisinin kabulüne sunmak
- Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesini sağlamak,
- Bilgi Güvenliği Politikası'nı belli aralıklarla gözden geçirmek ve BGYS Sorumlusunun onayına sunmak
- BGYS komitesinin gündemini belirlemek, alınan kararların uygulamasını takip etmek, BGYS gözden geçirme toplantılarını koordine etmek,
- BGYS dokümanlarının revizyonunu ve kontrolünü yapmak,
- Çalışanların bilgi güvenliği farkındalık eğitimlerinin koordine edilmesi ve eğitim etkinliklerinin değerlendirilmesini sağlamak
- Risk analizi sonuçlarını değerlendirmek, kontrollerin belirlenmesi ve uygulanmasını koordine etmek,
- Bilgi Güvenliği İhlal olaylarını değerlendirmek ve takibini yapmak,
- Bilgi Güvenliği'ne ilişkin düzeltici faaliyetleri takip etmek ve kayıtları onaylamak,
- BGYS için gerekli eğitimleri planlamak ve gerçekleştirilmesini sağlamak,

BGYS Komitesi Görev, Yetki ve Sorumluluklar:

- BGYS Komisyonu BGYS Yöneticisi ve/veya BGYS Sorumlusu tarafından oluşturulur, kurum yöneticisi tarafından onaylanır. BGYS Yöneticisi bu komisyona başkanlık eder.
- Bilgi Güvenliği konularının altyapısını oluşturacak projelere katkı sağlamak.
- bünyesinde ki birimlerde uygulanması gereken Bilgi Güvenliği politikaların geliştirilmesi için hazırlanan projelere katkı sunmak.
- BGYS Yöneticisi veya BGYS Sorumlusu tarafından gerekli görüldüğünde toplantılara katılmak.
- Kapsam kararları, risk değerlendirme metodolojisi, kontrollerin uygulanması konularında onay vermek ve bağlı oldukları birimlerde uygulanmasını sağlamak.
- BGYS Kapsam ve Politikalarının gerekliliği olan, birim çalışanlarının, danışmanların ve yüklenici firma personellerinin farkındalık düzeylerinin artırılmasına yönelik organize edilen çalışmaların tüm tabana yayılması için gerekli desteği vermek.

5.2 BGYS ORGANİZASYONU

BGYS SORUMLUSU

BGYS YÖNETİCİSİ

5.3 YGG (BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNETİM GÖZDEN GEÇİRME)TOPLANTILARI

BGYS Komitesi ve üst yönetimin bilgi güvenliğinin uygunluğunu, verimliliğini, risk yönetiminin işlevselliğini, tetkik sonuçlarını, düzeltici faaliyetleri ele aldığı yılda en az bir defa düzenlenen bir toplantıdır. Bu toplantıda yönetim risk kabul kriterlerini ve kaynak ihtiyaçlarını değerlendirir. Çalışmaların, risk değerlendirme ve işleme faaliyetlerinin verimliliğini inceler. Bu toplantılarda standarda göre girdi ve çıktılar **YGG Toplantı Tutanağı Formu** kullanılarak kayıt altına alınmaktadır.

6. RİSK YÖNETİMİ

6.1.Risk Analizi ve Yönetim Stratejisi

Risk analizi için aşağıdaki metot uygulanmaktadır. Bu faaliyetle ilgili kayıtlar risk değerlendirme raporunda tutulmaktadır. Kapsam dahilinde ki ve bilgi ile ilişkisi olan her varlığın tespiti için varlık keşif çalışması yapılır. Varlık envanteri ile her kullanıcının sahip olduğu (kullandığı ve yönettiği) varlıklar tespit edilir ve varlıkların sorumluları atanır. Risk analizi çalışması Tehdit Olasılığı ve İşe etkisi boyutlarında değerlendirilecektir. Risk hesaplama formülü kullanılarak her bir varlık için var olan risk değeri hesaplanır. Risk takip tablosunda tanımlanan her bir risk için 6 aylık risk durum değerlendirmeleri yapılarak son durum hesaplanır. Risk değerleri için Risk Değerlerine Göre İşleme Seçeneklerinden uygun olanı seçilir. Kontroller ISO 27001:2022'ün Ek-A maddesinden seçilerek uygun olanlar her bir riske atfedilir. Kontrolün nasıl uygulanacağı, kim tarafından uygulanacağı Risk İşleme Takip Tablosunda izlenir. 6 Aylık periyotlarla risk işleme faaliyetlerinin durumu varlık sahiplerinin de katıldığı BGYS komisyonunda değerlendirilir

6.2.SOA – Uygulanabilirlik Bildirgesi

Risk işleme seçenekleri standardın EK-A bölümünde verilen listeden seçilebilir. Seçilen kontrollerin her birinin seçilme amacı, kontrolün içeriği, kontrolün uygulanma biçimi ve uygulanmıyorsa nedeni kısa adı SOA (Statement of Applicability) olan dokümanda belirtilmektedir. SOA Gizli bilgi sınıfındadır. BGYS Sorumlusu, Yöneticisi ve Komitesinin erişimine açıktır. Bilgi güvenliği amaçları ve uygulamaları SOA'da detaylandırılmıştır. Risk İşleme planı ve SOA paralel dokümanlardır. Risk işleme planında seçilen kontrollerin isimleri veya EK-A'dan

seçilmişlerse A.X.X şeklinde kontrol numarasına atıf yapılırken SOA'da kontroller detaylandırılmıştır. Uygulanan ve uygulanacak tüm kontroller SOA'da kaydedilir. Bu doküman risk işleme planı ile bir çapraz kontrol sağlayarak herhangi bir kontrolün atlanmamasını sağlamaktadır.

7. BİLGİ HASSASİYETİ VE RİSKLER

7.1.Bilgi Varlıklarımız

bünyesinde Madde 2 de belirtilen kapsam dahilinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları işlerde üretilen bilgiler bilgi varlıklarımızı oluşturmaktadır. Masaüstü bilgisayarlar, laptoplar, teyp kaset, CD ve DVD ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (internet, e mail, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

7.2.Varlık Sınıflandırılması

Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmalıdır.

8. BİLGİ GÜVENLİĞİ POLİTİKA, PROSEDÜR VE KILAVUZU

BGYS Politikası yayınlanan bir çok farklı politika, prosedür, talimat ve rehberi kontrol ve risk yönetimi amaçları çerçevesinde adresler.

8.1.Bilgi Güvenliği Politikaları

yayımlanan Bilgi Güvenliği Politikaları çerçevesinde, Bilgi sistemleri tarafından yayınlanan bu dokümanda genel bilgi güvenliği kuralları tanımlanmıştır. Her çalışan bu dokümanlarda belirtilen kurallara uymakla sorumludur.

8.2.Bilgi Güvenliği Prosedürleri ve Planları

Bilgi yedekleme, ihlal olayı müdahale, iç denetim, doküman ve kayıtların kontrolü, kullanıcı tanımlama, iş sürekliliği planı, acil durum eylem planı, risk işleme planı gibi prosedür ve planlarda sistemin işleyişi anlatılmaktadır. İlgili çalışanlar yönetimce tanımlanan ve yayınlanan bu prosedür ve planlara uygun hareket etmelidirler.

8.3.Bilgi Güvenliği Sözleşmeleri

Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.

9. BİLGİ GÜVENLİĞİ EĞİTİMLERİ

Bilgi güvenliği eğitimleri periyodik olarak yılda en az bir kez ve yeni işe başlayan personele işe başladığı tarihi takip eden günlerde verilmektedir.

10. DOKÜMAN VE KAYITLARIN KONTROLÜ

BGYS ile ilgili dokümanların hazırlanması, yayınlanmadan önce onaylanması, değişikliklerinin revizyonlarının takibi, gerekli noktalarda doğru versiyonun ulaşılabilir olması amaçlarını yerine getirecek **Doküman Hazırlama ve Kodlama Prosedürü** hazırlanmıştır. Dokümanların kontrolü bu prosedüre uygun olarak yapılmaktadır. Kayıtların kontrolü, saklanması, yedeklenmesi, gerektiğinde tekrar elde edilebilmesini sağlamak amacıyla **Kayıtların Kontrolü Prosedürü** hazırlanmış ve uygulanmaktadır.

11. BİLGİ GÜVENLİĞİ İÇ DENETİMLERİ

Kurulan bilgi güvenliği yönetim sisteminin standarda ve tanımlanan politika ve prosedürlere uygunluğunun tespiti için düzenli olarak gerçekleştirilecek iç tetkikler planlanmıştır. İç tetkiklerin nasıl gerçekleştirileceği **İç Tetkik Prosedüründe** tanımlanmıştır ve bu prosedüre uygun olarak düzenli iç tetkikler yapılarak sistemdeki uygunsuzluklar tespit edilmektedir.

12. SÜREKLİ İYİLEŞTİRME VE DÜZELTİCİ FAALİYETLER

İç tetkiklerde, ihlal olaylarıyla veya personelin kendi gözlemleriyle tespit ettikleri uygunsuzlukların tespitinde ve standarda, politikalarımıza, prosedür ve kurallarımıza uymayan durumların tespitinde ortaya çıkan uygunsuzluğun nasıl giderileceği ve potansiyel uygunsuzlukların henüz ortaya çıkmadan önce nasıl önleneceğine ilişkin **Düzeltici Faaliyetler Prosedürü** hazırlanmış ve uygulanmaktadır. Tüm personel düzeltici faaliyetlere katılmakla sorumludur.

13. DİSİPLİN PROSESİ

Kurum içi veya yasal kurallara aykırı davranmanın yanı sıra bilgi güvenliği politika ve prosedürlerine uyulmaması durumunda da işlenen suçun boyut ve sonuçlarına göre ilgili disiplin sürecinin başlatılması uygulama esaslarındandır. Suçu işleyen personel suçun mahiyetine göre yasal hükümlere aykırı davranış halinde T.C. Anayasasında belirtilen müeyyidelere göre cezalandırılır.