1. AMAÇ

Bu politika, hukuka, yasal, düzenleyici, ya da sözleşmeye tabi yükümlülüklere, iç ve dış tarafların her türlü Bilgi Güvenliği Yönetim Sistemi gereksinimlerine ilişkin, Üst Yönetim'in bilgi güvenliği yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedeflerin uygulanmasına dair bilgiyi amaçlar.
Bilgi Güvenliği Politikası kurumsal bilgi güvenliği ilkelerini ana hatlarıyla belirler. Bilgi Güvenliği Politikası, kurumda bilginin ve işlenme yöntemlerinin güvenli olarak gerçekleştirilmesi amacıyla düzenlemeler yapar.

2. KAPSAM

Bu politika Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında bulunan tüm çalışanları ve bilgi varlıklarını kapsamaktadır.

3. SORUMLULUKLAR

Bilgi Güvenliği Kurulu Bilgi Güvenliği Politikasının tüm çalışanlara ve ilgili üçüncü taraflara duyurulmasını sağlar.
Bu politika periyodik olarak senede bir defa veya gerekli görülen hallerde Bilgi Güvenliği Kurulu tarafından gözden geçirilir.

4. TANIMLAR

Gizlilik: Bilgiye erişimin, sadece bilgiyi görüntülemeye izin verilen yetkili kişilerin erişimi ile kısıtlanmasıdır.
Bütünlük: Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin, tahrip edilmesinin sağlanması ve tespit edilebilirliğin sağlanmasıdır.
Erişilebilirlik/Kullanılabilirlik: Bilginin bilgiye erişim yetkisi olanlar tarafından istenildiği anda ulaşılabilir, kullanılabilir olmasıdır.
Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için iş riski yaklaşımına dayalı yönetim sistemidir.
Bilgi Varlığı: Kuruluşun sahip olduğu, işlerini aksatmadan yürütebilmesi için gerekli olan dolayısıyla korumakla yükümlü olduğu bilgi içeren varlıklardır. Bu politikaya konu olan süreçler kapsamındaki bilgi varlıkları şunlardır:
4.5.1. Kağıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri,
4.5.2. Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım,
4.5.3. Bilginin saklanmasını, erişilmesini, transfer edilmesini sağlayan servis veya ürünler,
4.5.4. Çalışanlar,
4.5.5. Çözüm ortakları,
4.5.6. Üçüncü taraflardan sağlanan servis, hizmet veya ürünlerdir.

5. BİLGİ GÜVENLİĞİ POLİTİKASI

5.1.Üst Yönetim Taahhüdü

Yorglass Üst Yönetimi Bilgi Güvenliği Yönetim Sisteminin gerçekleştirilmesi, işletimi, izlenmesi, gözden geçirilmesi, bakımı ve iyileştirilmesi için gerekenin yapılacağını taahhüt eder.
Yorglass, Bilgi Güvenliği Yönetim Sistemi ile ilgili olarak aşağıdaki ilkeleri benimsemektedir;

- Müşterilerine ve paydaşlarına sunduğu ürün ve hizmetlere ilişkin faaliyetlerini yürütürken veri güvenliğinin sağlanmasına önem vermektedir.
- Tüm iş süreçlerinin birbiri ile entegre, uyumlu ve dengeli olması hedeflenmektedir.

Entegre ve dinamik iş stratejisi bilgi varlıklarının güvenliğini ve sürekliliğini gerekli kılmaktadır.

- Müşteri ve paydaşlarına değer sağlayan ürün ve hizmetlerinin gizlilik, bütünlük ve erişilebilirliğini tehdit edebilecek risklere karşı tedbir almayı ilke edinir.
- Bu politika ve organizasyonun amacı ile uyumlu bilgi güvenliği hedefleri belirlenir ve düzenli aralıklarla uyumluluk ölçülerek, sürekli iyileştirme fırsatları değerlendirilir.

5.2. Bilgi Güvenliği Politikası

Yorglass olarak:
Bilgi sistemlerinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanmasını
Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetilmesini,
Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmeyi,
Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamayı,
Bilgi Güvenliği Yönetim Sistemi'nin yaşatılması için sürekli iyileştirme fırsatlarının değerlendirmeyi ve çalışmalarını gerçekleştirmeyi,
Bilgi güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmeyi,
Kişisel verilerin mahremiyetini sağlamak adına idari ve teknik tedbirleri almayı taahhüt ederiz.

5.3.Uygulama

Kuruluşta bilgi varlıkları uygun şekilde sınıflandırılır. Varlıkların değerlemesi yapılır ve uygun seviyede kontrol geliştirmek için varlıkların değeri hesaplanır.

Risk Değerleme ve Risk İşleme: Risklerinin değerleme işlemi ve uygun risk işleme planının hazırlanıp uygulamaya geçirilmesi devamlı bir süreçtir.

Fikri Mülkiyet Hakları: Yorglass çalışanları fikri mülkiyet hakkı taşıyan ürün, yazılım, hizmet veya sistemler sahibinden izin alınmadan veya kullanım lisansı olmadan kullanılamaz.

Eğitim: Tüm personele ve uygun durumlarda üçüncü taraf personellere, ilgili politika, talimat ve süreçler hakkında gerekli eğitimler ve bilgi güvenliği farkındalık eğitimler verilir. Eğitim kapsamına giren kurallar bütününde muhtemel değişiklik ve güncellemeler gerçekleştikten sonra eğitimleri tekrarlanır.

Yasal Uyumluluk: Yorglass, faaliyet alanı ile ilgili yayınlanmış kanun, yönetmelik ve tebliğlere uygun olarak hizmet vermek için gerekli tüm çalışmaları yapar.

İş Sürekliliği: Bilgi Güvenliği Kurulu iş süreklilik ilkelerini belirler ve iş süreklilik ilkelerinin hayata geçirilmesi için bir İş Süreklilik Planı oluşturulmasını ve değişen koşullara göre güncel tutulması için uyarıları yapar. Güncel İş Sürekliliği Planı ile ilgili roller ve sorumluluklar İş Sürekliliği Planı'nda belirtilir. İş sürekliliğine ilişkin genel prensipler İş Sürekliliği Politikasında yer almaktadır.

Sürekli İyileştirme: Bilgi güvenlik politikasını, denetim sonuçlarını, izlenen bilgi güvenliği olaylarının analizini, düzeltici ve önleyici faaliyetleri ve yönetim gözden geçirmelerini kullanarak Bilgi Güvenliği Yönetim Sistemini sürekli olarak iyileştirir.

Bilgi Güvenliği Organizasyonu: Bilgi güvenliği organizasyonu Üst Yönetim tarafından belirlenir ve uygulaması takip edilir. Bilgi güvenliği ile ilgili ekipler, roller ve sorumluluklar, Roller ve Sorumluluklar dokümanında belirtilir. Kapsam dahilindeki tüm personel bu dokümanda açıklanan sorumluluklara uygun şekilde çalışmaktan sorumludur.

• Bilgi güvenliği ile ilgili kritik kararların alınması, onaylanması ve gözden geçirilmesi Bilgi Güvenliği Kurulu tarafından yerine getirilir.
• Varlıkların korunması ve politikanın gerçekleştirilmesiyle ilgili güvenlik rollerinin Yorglass personeline atanması gerçekleştirilir. Hassas sistemlere erişim yetkisi olan kullanıcılar için gerekli güvenlik gözetimlerine dikkat edilir. Çalışanların sorumluluklarından haberdar olmaları sağlanır.
• Tüm personel sahibi olduğu varlıkların değerlerini atamaktan sorumludur.
• Tüm personel, kuruluş varlıklarının güvenliğini gözetmekle sorumludur.
• Varlıklarda gerçekleşmesi muhtemel ekleme ve çıkarma işlemleri sonrası gerekli durumlarda risk değerlemesi ve risk işleme yapılmalıdır. Bu işlem için Bilgi Güvenliği Kurulu haberdar edilir.
• Güvenlik sorunları ve bozulmaları Bilgi Güvenliği Kuruluna acilen raporlanır. Raporlanmış bir güvenlik sorunu öncelikli olarak ele alınır. Yazılım problemlerinden kaynaklanan sorunlar da aynı şekilde ele alınır. Geçmişte raporlanmış güvenlik sorunlarından ders alınarak aynı sorunların tekrar yaşanmaması sağlanır.
•Tüm personel, bilgi bulunan ortamların (doküman, manyetik ortam, elektronik ortam vb.) oluşturulması, işlenmesi, saklanması ve imha edilmesi konusundaki esaslara uymakla yükümlüdür.
• Tüm personel, erişim kontrolü gerektiren kaynak ve bilgilere erişirken, BGYS tarafından tanımlanan esaslara uymakla yükümlüdür.

Üçüncü Taraf Erişimi: Üçüncü şahıs ve kurumların 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 Gizlilik Sözleşmeleri hazırlanır.

Fiziksel ve Çevresel Güvenlik: Fiziksel ve çevresel güvenliğin eksiksiz olarak sağlanması amacıyla düzenlemeler ve denetimler yapılır. Hassas varlıkların bulunduğu ve hassas süreçlerin yapıldığı yerler güvenlikli olmak zorundadır. Güvenli bölgeler 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 ve kablolamanın gerçekleştirilmesi güvenlik düşünülerek yapılır. Donanımların düzenli bakımı gerçekleştirilir. Donanımların yapılandırılması esnasında güvenlik ilkelerine dikkat edilir.

Denetimler: Yorglass Bilgi Güvenliği Yönetim Sistemi, yılda bir defa denetlenir. Ayrıca Bilgi Güvenliği Kurulunun gerek görmesi halinde üçüncü taraf bağımsız denetim uzmanlarından bağımsız denetim hizmeti veya iç denetimlere danışmanlık hizmeti alınabilir.

Disiplin Süreci ve Yasal Yükümlülükler: Çalışanlar, bu politikaya uymakla yükümlüdür. Çalışanlar, çalışma saatleri dışında veya çalışma alanı dışında da bilgi güvenliği ile ilgili yükümlülüklere sahiptir. Bilgi Güvenliği Politikası ve talimatlara uyulmaması durumunda ilgili disiplin süreci uygulanır.

5.4. Bilgi Güvenliği Amaçları

Yorglass yukarıda belirtilen ilkelerden taviz vermeden bilgi güvenliği çalışmalarını aşağıda belirtilen amaçlarla gerçekleştirmeyi hedefler;
• İlgili kanun ve yönetmeliklere uyumlu hale gelinmesi,
• BGYS'nin sürekli iyileştirilmesi için gerekli iç denetim, yönetimin gözden geçirmesi, düzeltici faaliyetler ile risklerin ve fırsatların belirlenmesi,
• Paydaşları ile birlikte Yorglass'ın rekabet avantajını olumsuz yönde etkileyebilecek maddi ve manevi kayıplar engellenmesi
• Bilgi varlıklarının sınıflandırılması ve bu varlıkların gizlilik, bütünlük ve erişilebilirlik değerlendirmesinin yapılabilmesi,
• Bilgi güvenliği risklerini yönetmek için risklerini değerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirilerek, gerekli tedbirler geliştirilmesi,
• Çalışanların kişisel bilgilerinin mahremiyetinin sağlanması,
• Müşteri bilgilerinin yetkisiz kişilerin eline geçmesinin engellenmesi,
• Önemli bilgilerin bütünlüğünün sağlanması,
• Tedarikçi nezdinde bilgi güvenliği sağlanması,
• Operasyonel bilginin (Know-How) sürekli geliştirilmesi ve korunması sağlanması,
• Son kullanıcı bilgi güvenliği farkındalığını ve bu farkındalığın sürekli arttırılması,
• Bilgi güvenliğini etkin biçimde yöneterek bilgi güvenliği kaynaklı yaşanabilecek zararları asgariye indirilmesi,
• Kritik iş süreçlerinde yaşanabilecek Bilgi güvenliğini kaynaklı kesintilerin önüne geçilmesi,
• İnsan kaynakları yönetiminde istihdam öncesi, sırası ve sonrasında güvenliği sağlama açısından kuralların belirlenmesi,
• Güvenli çalışma alanları, arşiv odaları, sistem odaları gibi kurum içi çalışma bölgelerinde ve kurum çevresinde güvenliğin sağlanması için gerekli önlemlerin alınması,
• Tedarikçi ilişkilerinin güvenli bir şekilde yürütülmesi amacıyla; tedarik hizmetlerinin gözden geçirilmesi ve 3 taraf bilgi güvenliği gereksinimlerinin belirlenmesi.