1. Amaç

Bu politikanın amacı, hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, Üst Yönetim'in bilgi güvenliği ve gizlilk yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

Bilgi Güvenliği ve Gizlilik Politikası kurumsal bilgi güvenliği ve gizlilik ilkelerimizi ana hatlarıyla belirler. Bilgi Güvenliği ve Gizlilik Politikası, kurumda bilginin ve işlenme yöntemlerinin güvenli olarak gerçekleştirilmesi amacıyla düzenlemeler yapar.

2. Kapsam

Bu politika Bilgi Güvenliği ve Kişisel Veri Yönetim Sistemi kapsamında bulunan tüm çalışanları, bilgi varlıklarını, gizli bilgileri, ofisten ve evden yürüttüğü çalışmaları kapsamaktadır.

3. Tanımlar

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.

Bilgi Varlığı: Konecta'nin sahip olduğu, işlerini aksatmadan yürütebilmesi için gerekli olan dolayısıyla korumakla yükümlü olduğu varlıklardır.

4. Roller, Sorumluluklar ve Yetkiler

Bu politika periyodik olarak senede bir defa veya gerekli görülen hallerde Bilgi Güvenliği Uzmanı tarafından gözden geçirilir. Konecta Üst Yönetimi Bilgi Güvenliği ve Gizlilik Politikası'nın tüm çalışanlara ve ilgili üçüncü taraflara duyurulmasını sağlar.

Politikanın tanımı içerisinde bahsi geçen ilgili rol, birim ve departmanların görev ve sorumluluk tanımları "Konecta Görev Tanımları" içerisinde detaylı olarak anlatılmıştır.

5. Uygulama

5.1 Üst Yönetim Bağlılığı

Konecta Üst Yönetimi bilgi güvenliğinin gerçekleştirilmesi, işletimi, izlenmesi, gözden geçirilmesi, bakımı ve iyileştirilmesi için gerekenin yapılacağını taahhüt eder.

5.2 Bilgi Güvenliği Hedefleri

- Bilgi güvenliği ve gizliliği etkin biçimde yöneterek bilgi güvenliği kaynaklı yaşanabilecek zararları asgariye indirmek.
- Bilgi güvenliği ve Kişisel Veri ihlal olayı yaşama ihtimalini düşürmek, yaşanması durumunda koordineli biçimde yanıt verebilmek.

- Kritik iş süreçlerinde yaşanabilecek kesintilerin önüne geçmek, geçilemediği durumda hedeflenen kurtarma süresi içerisinde tekrar çalışabilir hale gelmek.
- Yasal yükümlülüklere uyumlu hale gelmek.
- Bilgi Güvenliği ve Kişisel Veri Yönetim Sistemi kapsamında müşterilerimizin bilgi varlıklarının gizliliğini, bütünlüğünü ve erişebilirliğini sağlamak. Müşteri ile ilgili kritik iş süreçlerinin devamlılığını sağlamak.
- Bilgi Güvenliği ve Kişisel Veri Yönetim Sistemi'nin sürekli iyileştirilmesini sağlamak.
- Bilgi Güvenliği Hedefleri (F.BGY.08) dokümanında hedefler güncellenmekte ve takip edilmektedir.

5.3 Bilgi Güvenliği Politikası

Bilgi güvenliği, bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ile mümkündür.
Bilginin;

- Gizlilik gerekliliği, bilginin sadece yetkili kişiler tarafından erişilebilir olmasını,
- Bütünlük gerekliliği, bilgi varlıklarının tam ve doğruluğunun sağlanmasını, yetkisiz değişimlerden korunmasını,
- Erişilebilirlik gerekliliği, bilgi varlıklarının ihtiyaç duyulduğu anda yetkili kullanıcılar tarafından kullanılabilir olmasını ifade eder.

Konecta bilgi güvenliğini ve gizliliği sağlamak amacıyla kendi kurumsal işleyişini düzenleyici prensipleri oluşturur. Bilgi Güvenliği ve Gizlilik Politikası'nın belirlenmesi, güvenlik rollerinin tanımlanması ve ilgili tüm güncellemelerin yapılması Üst Yönetim'in desteği ve tüm birimlerin koordinasyonuyla gerçekleştirilir. Konecta gerekli durumlarda iç ve dış uzmanların görüşüne başvurabilir.

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

Talimatlar: Sistemin uygun şekilde işletilebilmesi, işletmenin genel kurallara bağlı, denetlenebilir, tekrar edilebilir ve iyileştirilebilir olması amacıyla gerekli talimatlar hazırlanır.

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

Fikri Mülkiyet Hakları: Konecta' de 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 prosedürler hakkında gerekli eğitimler verilir. Eğitim kapsamına giren kurallar bütününde muhtemel değişiklik ve güncellemeler gerçekleştikten sonra güvenlik eğitimleri tekrarlanır.

Yasal Uyumluluk: Konecta, faaliyet alanı ile ilgili yayınlanmış kanun, yönetmelik ve tebliğlere uygun olarak hizmet vermek için gerekli tüm çalışmaları yapar.
Konecta; Kişisel Verilerin Korunması Kanununda belirtilen önlemleri almayı ve Kişisel Verilerin Korunması Politikasına tam uyumlu çalışmayı taahhüt eder.

İş Sürekliliği: Üst Yönetim iş süreklilik ilkelerini belirler ve iş süreklilik ilkelerinin hayata geçirilmesi için bir İş Süreklilik Planı oluşturulmasını ve değişen koşullara göre güncel tutulmasını sağlar. Güncel İş Sürekliliği Planı ile ilgili roller ve sorumluluklar İş Sürekliliği Planı'nda belirtilir. İş sürekliliğine ilişkin genel prensipler İş Sürekliliği Politikası'nda yer almaktadır.

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

Bilgi Güvenliği ve Gizlilik 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. Tüm personel bu dokümanda açıklanan sorumluluklara uygun şekilde çalışmaktan sorumludur.

- Bilgi güvenliği ve gizlilik ile ilgili kritik kararların alınması, onaylanması ve gözden geçirilmesi Bilgi Güvenliği Yöneticisi tarafından yerine getirilir.
- Bilgi güvenliği ve gizlilik kontrol önlemlerinin uygulamaya alınması ve kontrolü BGYS Kurulu tarafından gerçekleştirilir.
- Varlıkların korunması ve politikanın gerçekleştirilmesiyle ilgili güvenlik rollerinin Konecta personeline atanması gerçekleştirilir. Hassas sistemlere erişim yetkisi olan yeni ve deneyimsiz kullanıcılar için gerekli gözetimlere dikkat edilir. Çalışanların sorumluluklarından haberdar olmaları sağlanır.
- Kapsam dahilindeki personel sahip olduğu varlıkların değerlerini atamaktan sorumludur.
- Tüm personel, Konecta varlıklarının güvenliğini gözetmekle sorumludur.
- Varlıklarda gerçekleşmesi muhtemel ekleme ve çıkarma işlemleri sonrası gerekli durumlarda risk değerlemesi ve risk tedavisi yapılmalıdır. Bu işlem için Bilgi Güvenliği Yönetim Temsilcisi haberdar edilir.
- Güvenlik sorunları ve bozulmaları Bilgi Güvenliği Yönetim Temsilcisi'ne acilen raporlanır. Raporlanmış bir güvenlik sorunu öncelikli olarak çözümlendirilmelidir. 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 v.b.) 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 usül 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.

- **Denetimler:** Konecta Bilgi Güvenliği ve Kişisel Veri Yönetim Sistemi, yılda bir defa, bağımsız olarak denetlenir. Ayrıca Bilgi Güvenliği Yöneticisi'nin gerek görmesi halinde üçüncü taraf bağımsız denetim uzmanlarından bağımsız denetim hizmeti veya iç denetimlere danışmanlık hizmeti alınabilir.

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

Danışmanlık: Kurumsal bilgi teknolojileri altyapısının ve varlıkların güvenlik seviyesini arttırmaya yönelik Bilgi Güvenliği danışmanlık hizmeti alınır. Bilgi Teknolojileri güvenlik altyapısını inceleme ve güçlendirmeye yönelik haftalık toplantılar yapılır.

6. Politikanın Gelişimi

6.1 Kalite Kayıtları

Kayıt Ad/Tanımı	Saklandığı Ortam	Sorumlu	Saklama Süresi
Güvenlik Olay - Zayıflık - İhlal Bildirim Formu	Ortak Alan	Bilgi Güvenliği Yöneticisi /Kalite yönetim Temsilcisi/Bilgi Güvenliği Uzmanı	Süresiz

6.2 Referanslar

- ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
- ISO 27701 Kişisel Veri Yönetim Sistemi Standardı

6.3 Arayüzler

- QDMS (Yönetim Sistemleri Yazılımı)