NURUS BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ:

Bu politikanın amacı, hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetiminin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

2. REFERANS DOKÜMANLAR:

3. SORUMLULUK:

Bilgi Güvenliği Politikasının hazırlanması, gözden geçirilmesi ve güncellenmesinden Bilgi Güvenliği Yöneticisi ve/veya Bilgi Güvenliği Yönetici Yardımcısı sorumludur. NURUS yönetimi Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar.

4. POLİTİKA DETAYI:

4.1. TANIMLAR

4.1.1. 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.

4.1.2. Bilgi Güvenliği Yöneticisi:

Bilgi Güvenliği Yönetim Sistemi'nin operasyonundan ve sürekli iyileştirilmesinden sorumludur. Bilgi Güvenliği Yöneticisi, Sistem Yöneticisidir.

4.1.3. Bilgi Güvenliği Yönetici Yardımcısı:

Bilgi Güvenliği Yöneticisi'ne destek olmak ve tüm bilgi güvenliği süreçlerinde Bilgi Güvenliği Yönetici ile yer almaktan sorumludur. Bilgi Güvenliği Yönetici Yardımcısı, Bilgi İşlem Teknisyeni'dir

Bilgi Varlığı:

NURUS'un sahip olduğu, işlerini aksatmadan yürütebilmesi için önemli olan varlıklardır.

Bu politikaya konu olan bilgi varlıkları şunlardır:

- **a.** Kağıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri
- **b.** Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım
- **c.** Bilginin transfer edilmesini sağlayan ağlar
- **d.** Bölümler, birimler, ekipler ve çalışanlar
- **e.** Tesisler ve Özel alanlar
- **f.** Çözüm ortakları
- **g.** Üçüncü taraflardan sağlanan servis, hizmet veya ürün

4.1.4. Bilgi Varlığının İş Sahibi:

Bilgi varlıklarının üretimi, geliştirilmesi, bakımı, kullanımı ve güvenliğini kontrol etmek için onaylanmış yönetim sorumluluğu bulunan kişi veya varlıkları tanımlar. 'Sahip' terimi, gerçekten varlık üzerinde mülkiyet hakları olan kişi anlamına gelmez.

4.1.5. Bilgi Varlığının Teknik Sahibi:

Bilgi varlıklarının kurum içinde kullanılması için gerekli olan teknik operasyonda sorumluluğu bulunan kişi veya ekipleri tanımlar.

4.2. POLİTİKA:

Bilgi kaynakları, tesisler ve cihazlar gibi NURUS 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.

NURUS BİLGİ GÜVENLİĞİ POLİTİKASI

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.

NURUS için tüm bu bilgi varlıkları ve kaynakları içerisinde en kritik olanı, özenle korunması, gizliliğinin sağlanması, ihtiyaç duyulduğu anda erişilmesi gereken bilgi varlıkları, **NURUS içinde barındıran sunucu sistemi ve bu sistemi barındıran sistem odasıdır.**

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 dahilinde 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.

4.2.1. Bilgi Varlıklarının ve Kaynaklarının Kullanımı

NURUS'ta yürütülen yazılım ve danışmanlık hizmetlerinin doğası gereği, 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.

NURUS'un bilgi kaynaklarını kullanarak etik dışı veya yasalara karşı faaliyetlerde bulunmak, hiç kimse için kabul edilemez.

Bu politikanın asgari gereği olarak,

- Verinin kasıtlı olarak değiştirilmesi;
- Kasıtlı olarak veride 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 İnsan Kaynakları 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 Yönetici Yardımcısı'na bildirilmesi gerekir.

4.2.2. Rol ve Sorumluluklar

Bilgi varlıklarının teknik sahipleri bilginin gizlilik bütünlük ve kullanılabilirliğini sağlamak için;

- Bilgi varlıklarına yetkisiz olarak erişilmesini; bilgi varlıklarının yetkisiz olarak değiştirilmesini veya tahribatını önlemek suretiyle, bilgi varlıklarını korurlar.
- Operasyonun mümkün olan en kısa hizmet kesintisi ile devam etmesini sağlamak için gerekli süreçlerin tanımlanmasını ve uygulanmasını sağlarlar.
- Bilgi güvenliği gerekliliklerini gözetirken, ihtiyaç duyulduğunda bilgiye hızla erişilebilmesi için karmaşıklığı ortadan kaldıracak dengeyi kurarlar.
- Çalışanlarını ve birlikte çalıştıkları üçüncü taraf çalışanlarını bilgi güvenliği gereklilikleri, rolleri ve sorumlulukları konusunda bilgilendirirler ve bilinçlendirirler.

4.2.3. Bilgi Güvenliği Kurulu

Bilgi Güvenliği Kurulu (BGK) aşağıdaki kişilerden oluşur:

- Satış Operasyon Direktörü
- Operasyon Yöneticisi
- Proje ve Ürün Yöneticisi
- Mali ve İdari İşler Sorumlusu
- Yönetim Sistemleri Mühendisi
- Bilgi İşlem Ekibi
- Bilgi Sistemleri Sorumlusu

BGK, yılda en az bir kere, Bilgi Güvenliği Yöneticisi'nin 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 Politikası'nın gözden geçirilmesi
- Risk Yönetim Metodolojisinin onaylanması
- Güncel risk raporunun değerlendirilmesi
- Kabul edilebilir risk seviyesinin üst yönetim tarafından onaylanması
- Artık risklerin üst yönetim tarafından onaylanması
- Risk işleme planının üst yönetim 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 NURUS Yönetimi tarafından gözden geçirilmiş ve onaylanmıştır.