

BİLGİ GÜVENLİĞİ

Güvenlik Hedefleri

Bilgi Güvenliği Yönetim Politikamız aşağıdaki temel kavramlara dayanmaktadır:

Gizlilik (Confidentiality): Bilginin, yetkisiz kişi, kurum veya süreçler tarafından erişilemez ve ifşa edilemez olmasını ifade eder.

Bütünlük (Integrity): Bilgi varlıklarının doğruluğunun, tamlığının ve tutarlılığının korunmasını ifade eder.

Erişilebilirlik (Availability): Bilginin, yetkili kullanıcılar tarafından ihtiyaç duyulduğunda erişilebilir ve kullanılabilir olmasını ifade eder.

Kapsam

Bu politika; bilgi sistemleri altyapısını kullanan tüm birimleri, bilgi sistemlerine üçüncü taraf olarak erişim sağlayan kişi ve kuruluşları ile bilgi sistemlerine teknik destek sağlayan yazılım ve donanım hizmet sağlayıcılarını kapsamaktadır.

Bu kapsamda tüm çalışanlar, Bilgi Güvenliği Yönetim Sistemi (BGYS) ile ilgili dokümanları benimsemek ve bu dokümanlara uygun hareket etmekle yükümlüdür.

Politika

Nart Bilişim (TechNarts), yürürlükteki yasal düzenlemeler, operasyonel gereklilikler ve sözleşmesel yükümlülüklerin yerine getirilmesini sağlamak amacıyla kuruma ait tüm fiziksel ve elektronik bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı taahhüt eder.

TechNarts'ın bilgi güvenliği hedefleri aşağıdaki gibidir:

* Yürürlükte bulunan tüm kanunlara, yönetmeliklere ve ilgili düzenlemelere uyum sağlamak.



+90 (0312) 354 98 68



ODTÜ TEKNOKENT MET YERLEŞKESİ, Mustafa
Kemal Mah. Dumlupınar Bulvarı No:280 E
Blok 2/A, 06530 Çankaya/Ankara



www.technarts.com

- * TechNarts çalışanları ve diğer kullanıcılar açısından gizlilik, bütünlük ve erişilebilirlik gerekliliklerini yerine getirmek.
- * Bilgi ve bilgi sistemlerini hırsızlık, kötüye kullanım ve diğer zarar veya kayıp risklerine karşı koruyacak kontrolleri oluşturmak.
- * Güvenlik olaylarının riskini en aza indirmek amacıyla yöneticilerin ve çalışanların bilgi güvenliği konusundaki sorumluluk, sahiplenme ve farkındalık düzeylerini artırmak.
- * Büyük ölçekli bilgi güvenliği olayları yaşansa dahi TechNarts'ın hizmetlerini kesintisiz sürdürebilmesini sağlamak.
- * Kişisel verilerin korunmasını ve gizliliğini güvence altına almak.
- * TechNarts tarafından sunulan ve işletilen ağ altyapısı ile hizmetlerin sürekliliğini ve güvenilirliğini sağlamak.
- * ISO/IEC 27001 başta olmak üzere uluslararası bilgi güvenliği standartlarına uygun yöntemleri uygulamak.
- * Dış hizmet sağlayıcılarının TechNarts'ın bilgi güvenliği gereksinim ve beklentilerine uygun hareket etmelerini sağlamak.

Sorumluluklar

Şirket yönetimi, yürürlükteki mevzuat, kurumsal gereklilikler ve sözleşmeler doğrultusunda TechNarts'ın varlıklarının etkin ve güvenli şekilde yönetilmesinden genel olarak sorumludur.

Şirket Genel Müdürü; personel güvenliği ve bilgi teknolojileri güvenliği de dâhil olmak üzere TechNarts bünyesindeki bilgi güvenliğinin sağlanmasından nihai düzeyde sorumludur.

Risk Yönetimi

TechNarts'ın bilgi güvenliği yaklaşımı, risk değerlendirmelerine dayalı olarak yürütülmektedir.

Bu kapsamda;



+90 (0312) 354 98 68



ODTÜ TEKNOKENT MET YERLEŞKESİ, Mustafa
Kemal Mah. Dumlupınar Bulvarı No:280 E
Blok 2/A, 06530 Çankaya/Ankara



www.technarts.com

- * Bilgi güvenliği riskleri sürekli olarak değerlendirilmeli ve gerekli koruyucu tedbirlerin uygulanmasına yönelik ihtiyaçlar düzenli olarak gözden geçirilmelidir.
- * Bilgi sistemlerine ilişkin kapsamlı bir risk değerlendirmesi yılda en az bir kez gerçekleştirilmelidir.
- * Risk değerlendirmelerinde, kabul edilebilir risk kriterleri doğrultusunda riskler belirlenmeli, analiz edilmeli, ölçülmeli ve önceliklendirilmelidir.
- * Sistem sahipleri, sorumluluk alanlarına giren sistemlerde risk değerlendirmelerinin bu politikaya uygun şekilde gerçekleştirilmesini sağlamakla yükümlüdür.
- * Risk yönetimi faaliyetleri, TechNarts yönetimi tarafından onaylanan kriterler doğrultusunda yürütülmelidir.
- * Gerçekleştirilen risk değerlendirmeleri, TechNarts yönetimi ve/veya ilgili sistem sahipleri tarafından onaylanmalıdır.
- * Risk değerlendirmesi sonucunda kabul edilemez seviyede risk tespit edilmesi halinde, bu riskleri kabul edilebilir seviyeye indirecek uygun kontrol ve iyileştirme faaliyetleri uygulanmalıdır.

TechNarts



+90 (0312) 354 98 68



ODTÜ TEKNOKENT MET YERLEŞKESİ, Mustafa
Kemal Mah. Dumlupınar Bulvarı No:280 E
Blok 2/A, 06530 Çankaya/Ankara



www.technarts.com

INFORMATION SECURITY

Security Goals

Our information security management policy is related to the following basic concepts:

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. **Integrity:** The property of safeguarding the accuracy and completeness of assets. **Availability:** The property of being accessible and usable upon demand by an authorized entity.

Scope

This policy includes all the units using the information systems infrastructure, reaching the information systems as third parties, and software and hardware service providers providing technical support for information systems. In this context, employees are required to embrace the related documents for Information Security Management System and act accordingly.

Policy

Nart Informatics (TechNarts) is committed to safeguard the confidentiality, integrity, and availability of all physical and electronic information assets of the institution to ensure that regulatory, operational, and contractual requirements are fulfilled. The overall goals for information security at TechNarts are the following:

- Ensure compliance with current laws, regulations, and guidelines
- Comply with requirements for confidentiality, integrity, and availability for TechNarts's employees, and other users
- Establish controls for protecting TechNarts's information and information systems against theft abuse and other forms of harm and loss
- Motivate administrators and employees to maintain the responsibility for, ownership of, and knowledge about information security, in order to minimize the risk of security incidents
- Ensure that TechNarts is capable of continuing its services even if major security incidents occur
- Ensure the protection of personal data (privacy)



+90 (0312) 354 98 68



ODTÜ TEKNOKENT MET YERLEŞKESİ, Mustafa
Kemal Mah. Dumlupınar Bulvarı No:280 E
Blok 2/A, 06530 Çankaya/Ankara



www.technarts.com

- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by TechNarts
- Comply with methods from international standards for information security, e.g. ISO/IEC 27001
- Ensure that external service providers comply with TechNarts 's information security needs and requirements

Responsibilities

The administration has the overall responsibility for managing TechNarts's values in an effective and satisfactory manner according to current laws, requirements, and contracts. The Chancellor/President has the overall responsibility for information security at TechNarts, including information security regarding personnel and IT security.

Risk Management

- TechNarts's approach to security should be based on risk assessments.
- TechNarts should continuously assess the risk and evaluate the need for protective measures.
- An overall risk assessment of the information systems should be performed annually.
- Risk assessments must identify, quantify and prioritize the risks according to relevant criteria for acceptable risks.
- The system owners are responsible for ensuring that risk assessments within their area of responsibility are implemented in accordance with the policy.
- Risk management is to be carried out according to criteria approved by the management at TechNarts.
- Risk assessments must be approved by the management at TechNarts and/or the system owners.
- If a risk assessment reveals unacceptable risks, measures must be implemented to reduce the risk to an acceptable level.

TechNarts



+90 (0312) 354 98 68



ODTÜ TEKNOKENT MET YERLEŞKESİ, Mustafa
Kemal Mah. Dumlupınar Bulvarı No:280 E
Blok 2/A, 06530 Çankaya/Ankara



www.technarts.com