Bilgi Güvenliği Politikası

Amaç ve Kapsam

Bu Bilgi Güvenliği Politikası, FORGESAN bünyesinde üretilen, kullanılan, işlenen veya muhafaza edilen tüm bilgilerin **gizlilik, bütünlük ve erişilebilirlik** ilkelerine uygun şekilde korunmasını sağlamak üzere oluşturulmuştur. Politika; çalışanları, tedarikçileri, iş ortaklarını ve FORGESAN adına bilgiye erişen tüm tarafları kapsar.

Bilgi Güvenliği Yönetimi Yaklaşımımız

FORGESAN, bilgi varlıklarının korunmasını stratejik bir öncelik olarak görür ve ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi prensiplerine uygun şekilde yönetim proseslerini yapılandırır.
Kuruluşumuz, bilgi güvenliği süreçlerini iş hedefleriyle entegre eder, sürekli iyileştirmeyi esas alır ve bilgi güvenliğini kurumsal kültürün ayrılmaz bir parçası olarak kabul eder.

Temel Taahhütlerimiz

FORGESAN, bilgi güvenliğini sağlamak amacıyla aşağıdaki taahhütleri üstlenir:

Yasal Uyum ve Standartlar

Bilgi güvenliği alanında geçerli tüm ulusal mevzuata, sözleşmesel gerekliliklere ve uluslararası standartlara uyum sağlamak FORGESAN'ın temel sorumluluğudur.

Gizlilik, Bütünlük ve Erişilebilirlik

Bilgi varlıklarının yetkisiz erişime karşı korunması, değiştirilmeden saklanması ve ihtiyaç duyulduğunda erişilebilir olması için teknik ve idari kontrol mekanizmaları uygulanır.

Risk Yönetimi

Bilgi varlıklarına yönelik tehditler düzenli olarak analiz edilir; riskler tanımlanır, sınıflandırılır ve uygun kontrol tedbirleri planlanarak uygulanır. Kritik riskler için aksiyon planları oluşturulur ve takip edilir.

Fiziksel ve Dijital Koruma

Bilgi varlıklarının bulunduğu fiziksel alanlar kontrol altında tutulur, dijital sistemlerde güvenlik duvarları, erişim kontrol mekanizmaları, kayıt izleme ve zararlı yazılım önleme sistemleri bulundurulur.

İş Sürekliliği ve Olay Yönetimi

Bilgi teknolojilerine ilişkin kesinti riskleri değerlendirilir; iş sürekliliğini destekleyen altyapılar ve yedekleme mekanizmaları işletilir.
Olası bilgi güvenliği ihlallerinde hızlı müdahale, kontrol, raporlama ve öğrenme süreçlerini içeren etkin bir olay yönetim modeli uygulanır.

İnsan Kaynağı ve Farkındalık

Çalışanlar, bilgi güvenliği kültürünün en önemli parçasıdır. Bu nedenle tüm personele rol ve sorumluluklarına uygun güvenlik farkındalık eğitimleri düzenli olarak verilir.
FORGESAN çalışanlarının, bilgi güvenliğini zedeleyebilecek davranışlardan kaçınması ve politikaya uygun hareket etmesi kurumsal bir zorunluluktur.

Tedarikçiler ve İş Ortakları ile Uyum

FORGESAN, bilgi güvenliği gerekliliklerinin yalnızca kurum içinde değil, tedarikçiler ve dış hizmet sağlayıcılarla yürütülen tüm süreçlerde sağlanmasını bekler.
Bilgi güvenliğini etkileyebilecek herhangi bir dış kaynaklı risk tespitinde karşı taraflarla ortak aksiyon planları geliştirilir; uyumsuzlukların devamında iş ilişkisi sonlandırılabilir.

Sürekli İyileştirme

Bilgi Güvenliği Yönetim Sistemi, performans göstergeleri, denetimler, testler, geri bildirimler ve olay analizleri ile düzenli olarak değerlendirilir.
Sistemin etkinliğini artırmak için iyileştirme fırsatları tespit edilir ve uygulanır.

Sorumluluklar

Bu politikanın uygulanmasından tüm çalışanlar, yöneticiler ve ilgili paydaşlar sorumludur.
Bilgi Güvenliği Yönetim Sistemi'nin koordinasyonu ve takibi, FORGESAN'ın atanmış ilgili birimi tarafından yürütülür.

Politika İhlal Bildirimi

Bilgi güvenliğini tehlikeye atabilecek her türlü olay, ihlal şüphesi veya güvenlik zafiyeti gecikmeden bildirilmelidir.
Çalışanlar ve iş ortakları, güvenlik konularına ilişkin bildirimlerini etik@forgesan.com adresine iletebilirler.

FORGESAN Makina adına
Nuh Atila
Genel Müdür
FORGESAN Makine Metal Endüstri A.Ş.

Information Security Policy

Purpose and Scope

This Information Security Policy is established to ensure that all information created, processed, stored, or transmitted within FORGESAN is protected in accordance with the principles of confidentiality, integrity, and availability. The policy applies to all employees, suppliers, business partners, and any third parties accessing information on behalf of FORGESAN.

Information Security Management Approach

FORGESAN considers the protection of information assets a strategic priority and structures its management processes in alignment with ISO/IEC 27001 Information Security Management System principles.
Information security processes are integrated with business objectives, continuously improved, and embedded into the organizational culture.

Core Commitments

FORGESAN undertakes the following commitments to ensure the protection of information assets:

Legal Compliance and Standards

The company complies with all applicable national regulations, contractual obligations, and international standards related to information security.

Confidentiality, Integrity, and Availability

Technical and administrative controls are implemented to prevent unauthorized access, ensure the accuracy of information, and maintain availability when required.

Risk Management

Threats to information assets are regularly analyzed; risks are identified, assessed, and managed with appropriate control measures. Action plans are developed and monitored for high-priority risks.

Physical and Digital Protection

Physical environments hosting information assets are controlled, and digital systems are secured through access controls, firewalls, monitoring mechanisms, and anti-malware protections.

Business Continuity and Incident Management

Risks that may disrupt information technology services are assessed, and infrastructures supporting business continuity and backup processes are maintained.
In the event of an information security incident, effective detection, response, reporting, and recovery procedures are applied.

Human Resources and Awareness

Employees are essential to maintaining information security. FORGESAN provides regular awareness and competency-based training to ensure compliance with security requirements.
All personnel are expected to avoid actions that may jeopardize information security and to adhere to this policy.

Suppliers and Business Partners

FORGESAN expects all suppliers and external service providers to comply with information security requirements.
When external risks are identified, joint action plans are developed; persistent non-compliance may result in termination of cooperation.

Continuous Improvement

The Information Security Management System is periodically reviewed through audits, performance indicators, tests, feedback, and incident analyses.
Improvement opportunities are identified and implemented to enhance system effectiveness.

Responsibilities

All employees, managers, suppliers, and relevant stakeholders are responsible for complying with this policy. Coordination and monitoring of the Information Security Management System are carried out by the designated FORGESAN unit.

Reporting Policy Violations

Any suspected information security breach, vulnerability, or incident must be reported without delay.
Employees and partners may submit concerns or notifications to **etik@forgesan.com**.

On behalf of FORGESAN Machinery
Nuh Atila
General Manager
FORGESAN Makine Metal Industry Inc.