Information Security Policy (Public Version)

Effective Date: June, 2026

Introduction

At COCUS, we prioritize safeguarding information and maintaining the highest standards of security, data protection and business continuity. Our commitment ensures the confidentiality, integrity, and availability of all systems and data critical to both our operations and our customers.

We continuously improve our Information Security Management System (ISMS), security controls, technologies, and employee awareness to ensure the ongoing protection of information and compliance with applicable legal, regulatory, and contractual requirements.

Information security is a responsibility shared across the entire organization. Management demonstrates its commitment by establishing the Information Security Management System (ISMS), allocating appropriate resources, communicating security objectives, and promoting a culture of continuous improvement.

This document provides an overview of COCUS' approach to protecting information and maintaining compliance with internationally recognized standards and best practices.

Organizational Security

Dedicated Security Teams

COCUS has dedicated teams responsible for Information Security and Data Protection:

Information Security Team

Responsible for information security governance, risk and incident management, awareness, compliance, the Information Security Management System (ISMS) and business continuity.

Data Protection Team

Responsible for ensuring compliance with applicable privacy legislation and regulations, supporting COCUS in its role as both Data Controller and Data Processor.

IT Secure Operations Team

Responsible for secure IT operations, including vulnerability management, monitoring, identity and access management, incident response, infrastructure resilience, and implementation of security controls supporting business continuity.

Integrated Information Security Management Systems

COCUS has established and maintains an Information Security Management System (ISMS) in accordance with **ISO/IEC 27001** and supporting compliance with **TISAX®** requirements.

The scope of the ISMS includes:

> Design, development, delivery, operation, and support of secure IT infrastructure and consulting services, including industrial private networks, digital products, data analytics and AI/ML solutions, infrastructure and network automation, and proactive IT security and compliance services.

The ISMS consists of policies, standards, procedures, and technical controls designed to systematically identify, assess, and manage information security risks.

These documents are communicated to relevant employees and contractors, reviewed at least annually, and cover topics including Information Security Governance; Information Classification; Risk Management; Identity and Access Management; IT Secure Operations; Incident Management; Business Continuity; Third-Party Security; Human Resources Security; Data Protection; Secure Software Development; Asset Management

The Information Security Team monitors compliance with these policies and supports their continuous improvement.

Information Classification

COCUS has implemented an Information Classification process to ensure that information is identified, handled, stored, transmitted, and disposed of according to its sensitivity and business value.

Classification supports the protection of confidentiality, integrity, and availability throughout the entire information lifecycle.

Confidentiality Agreements

Employees, contractors, partners, and service providers handling COCUS or customer information are required, where applicable, to sign confidentiality and non-disclosure agreements to protect sensitive information throughout their engagement.

Human Resources Security

Employees, contractors, and other authorized users accessing COCUS information or systems are required to comply with applicable security policies throughout their entire engagement lifecycle.

Security responsibilities are communicated before access is granted and continue after employment or contractual relationships end.

Code of Conduct

COCUS' Code of Conduct and Internal Regulations define employees' responsibilities regarding the appropriate use and protection of company information.

Violations of security policies or the Code of Conduct may result in disciplinary measures in accordance with applicable legislation.

Security and Data Protection Awareness

COCUS maintains a detailed security awareness program, including:

- Information Security and Data Protection training during onboarding
- Regular refresher training
- Targeted role-based security training
- Company-wide security alerts and awareness campaigns
- Continuous communication regarding emerging threats and best practices

Offboarding Processes

COCUS maintains formal offboarding procedures to ensure that:

- Access rights are promptly removed
- Company assets are returned
- Information remains protected
- Confidentiality obligations continue after employment where applicable

Infrastructure Security

COCUS has established policies, standards, and operational procedures to protect its infrastructure, networks, systems, and information assets throughout their lifecycle.

These include controls covering Identity and Access Management; Password Management; Secure Operations; Asset Management; Secure Configuration; Vulnerability Management; Patch Management; Logging and Monitoring; Cryptography; Change Management

Technical and organizational controls include encryption, authentication mechanisms, endpoint protection, vulnerability management, centralized logging, and secure configuration management.

For further information regarding our ISMS, please contact the Information Security Team.

Physical Security

Access to COCUS facilities is restricted to authorized personnel.

Security zoning, physical access controls, visitor management, and environmental safeguards are implemented to protect facilities and critical infrastructure.

Security Operations

Vulnerability Management

COCUS continuously identifies, evaluates, prioritizes, and remediates vulnerabilities affecting its infrastructure and services through a structured vulnerability management process.

Patch Management

Systems are patched according to defined processes based on vendor recommendations, risk assessments, operational impact, and business criticality.

Security updates are regularly reviewed and deployed following testing and approval where required.

Penetration Testing

Independent penetration tests are periodically performed using recognized industry methodologies to assess the effectiveness of implemented security controls.

Change Management

Changes to production environments follow a formal change management process including planning, risk assessment, testing, approval, implementation, and post-implementation review.

Segregation of Duties

Responsibilities are appropriately segregated to reduce the risk of unauthorized or unintended activities and to ensure appropriate oversight.

Asset Management

COCUS maintains an inventory of information assets, including hardware, software, cloud services, and business applications.

Assets are managed throughout their lifecycle, including ownership, classification, secure configuration, maintenance, and secure disposal.

Identity and Access Management

Access to information and systems is granted according to business need and the principle of least privilege.

Access rights are regularly reviewed and promptly removed when no longer required.

Backups

Backup processes are implemented based on business requirements and disaster recovery objectives.

Recovery testing is performed regularly to verify that backup data can be successfully restored within defined recovery objectives.

Endpoint Security

COCUS protects endpoints through centrally managed security controls, including device management, malware protection, encryption, secure configuration, and monitoring.

Incident Management

COCUS maintains formal incident management procedures for security events affecting confidentiality, integrity, availability, or privacy.

This policy covers four key stages of the incident lifecycle: detection and reporting; analysis and triage; containment and treatment; recovery; and post-incident with lessons learned and continual improvement.

Risk Management

COCUS applies a structured risk management process to identify, assess, treat, monitor, and periodically review information security risks.

Risk management supports informed decision-making and continual improvement of security controls.

Crisis Management and Business Continuity

COCUS has established Crisis Management and Business Continuity processes to ensure organizational resilience.

The goal of these processes is to maintain organizational stability and effectively coordinate the recovery of essential business functions in the event of disruption or crisis. COCUS ensures that disaster recovery plans and backup policies are regularly tested to ensure continuity of business and operations.

Third-party Risk Management

COCUS evaluates suppliers before engagement to ensure they meet appropriate information security and data protection requirements.

Formal agreements are established with these third parties, which include, where applicable, clearly defined responsibilities, information security incident management protocols, established communication channels, and designated points of contact for security and data protection matters.

Periodic due diligence activities are performed based on supplier criticality to monitor ongoing compliance and risk.

Audit and Compliance

COCUS performs regular internal and external audits to verify compliance with applicable policies, standards, contractual obligations, and legal requirements.

Audit results support continual improvement of the Information Security Management System.

Secure Software Development

COCUS integrates security throughout the software development lifecycle by applying secure development practices, security testing, code quality controls, and controlled change management appropriate to the associated risks.

Data Protection Management

Data Protection by Design and by Default

Privacy and information security requirements are integrated into projects, systems, and services from their earliest stages.

All customer projects undergo a security assessment process involving the Information Security and Data Protection teams to identify risks and define appropriate mitigation measures.

COCUS applies the principles of Data Protection by Design and by Default to ensure that personal data processing is limited to what is necessary for the intended purpose.

Information Protection

COCUS protects sensitive information through a combination of technical and organizational controls, including Information classification; Role-based access control; Encryption; Secure collaboration platforms; Microsoft 365 information protection capabilities; Secure configuration of corporate systems; Monitoring and auditing of access to sensitive information

These controls help reduce the risk of unauthorized disclosure, alteration, or loss of information.

Customer Data

COCUS take it seriously to protect customer data. We are fully committed to protecting our customers' data and take this responsibility seriously.

Employees receive regular training on the secure handling of customer information, while appropriate technical and organizational measures are implemented to safeguard confidentiality, integrity, and availability throughout the information lifecycle.

COCUS complies with the General Data Protection Regulation (GDPR) and other applicable privacy requirements.

1.1 Continuous Improvement

Information security is an ongoing commitment at COCUS.

We continuously review and improve our Information Security Management System, processes, technologies, and awareness programs to address evolving threats, changing business needs, and regulatory requirements.

Through skilled professionals, effective governance, secure technologies, and a secure culture, COCUS remains committed to protect information and maintain the trust of our customers, partners, and employees.