Information Security Policy (Public version)

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 are continuously improving our information security management system (ISMS), processes, and implementing robust security controls, technologies and investing in our people training and awareness.
COCUS commitment involve the entire organization, with the Management assuming responsibility for its communication and implementation, committing itself to act with a focus on achieving the established goals.
This document provides COCUS approach to protecting data and maintaining compliance with international standards and best practices, highlighting the main components of our information security policies.

Organizational Security

Dedicated Teams:

In COCUS we have three teams dedicated to information security and data protection which are:

- The Information Security Team is responsible for governance, risk, compliance, second line of defense, management system, and overall security and business continuity program management.

- The Data Protection team is responsible for ensuring compliance with privacy laws and regulations that apply to COCUS as a controller and/ or processor.

- The IT Secure Operations team. It is responsible for vulnerability management, incident detection and response, monitoring, identity and access control, resilience and implementation of the measures defined for business continuity.

Integrated Management System:

COCUS has an integrated management system aligned with:

- TISAX and ISO 27001 standards for Information Security Management System (ISMS).

Our management system includes policies, guidelines, and standards designed to provide a systematic approach to protecting company information and assets. This approach ensures protection based on the criticality and sensitivity of information, mitigating internal and external threats and reducing risk to acceptable levels.

These policies are acessible to all employees and other staff. They are reviewed at least annually and cover several areas related to security and data protection, including governance, risk management, incident management, human resources security, third-party management, data protection management, among others.

The Information Security team is responsible for monitoring compliance with the aforementioned policies and guidelines and standards.

Classification of Information

COCUS has implemented a classification of information process to ensure that data is appropriately identified, handled, and protected based on its sensitivity, reducing risks and safeguarding confidentiality, integrity, and availability of information.

Confidentiality Agreements

COCUS requires partners, service providers, and employees to sign non-disclosure and confidentiality agreements, ensuring their commitment to the company's information security principles.

Human Resources Security

People connecting to COCUS systems are required to adhere to company security policies. This includes responsibilities during and after employment with COCUS.

Code of Conduct

COCUS' code of conduct and internal regulation addresses the appropriate use of company management of information to which employees have access to during the execution of the work agreement with COCUS. Violations of the code or company policies will be subject to a disciplinary process, in accordance with local labor laws.

Security and Data Protection Training and Awareness

COCUS offers a security and data protection training and awareness program that includes:

- COCUS employees undergo security and privacy training as part of the onboarding process.

- COCUS provides regular training and awareness to reinforce the security and data protection principles and policies, as well as industry best practices and common pitfalls.

- COCUS provides target training and awareness to ensure the right training is provided to those roles that, based on their responsibilities, access levels, and function may represent a risk to COCUS.

Additionally, the Information Security team distributes company-wide security alerts when necessary.

Offboarding Processes

COCUS has a defined offboarding process that outlines the responsibilities for collecting information assets and removing access rights for employees who leave our company.

COCUS has established and implemented policies and standards to ensure infrastructure security, physical security and secure operations. These include key policies such as Identity and Access Management, Password Management, Risk Management, Incident Management, Change Management, Third-party management, Audit Management and more. All policies and related documents have been developed and maintained in alignment with TISAX and ISO 27001 requirements, as well as industry best practices.
COCUS has implemented several requirements related to encryption of data, password complexity and password manager system, authentication mechanisms, endpoint security, event logging and auditing.
For more information about our Information Security Management System (ISMS) and associated policies, please contact our team.

Physical Security

Access to COCUS facilities is restricted to authorized employees and contractors. COCUS implemented a security zoning approach, with specific organizational and technical safeguards in place for areas requiring high-level protection needs.

Security Operations

Vulnerability Management

COCUS' dedicated teams are regularly identifying, assessing, and remediating security vulnerabilities through patches and updates.

Patching
COCUS has implemented a patch management process to ensure systems and infrastructure systems are patched according to vendor recommendations.
The process includes steps to review proposed patched to determine the risk of applying or not applying patched based upon the security and availability impact of those systems, and any critical applications hosted on them. COCUS continually reviews patched and updated as they are released to determine their criticalities.

Penetration Testing
Independent penetration tests are conducted to evaluate the security posture of a target system or environment. These tests follow recognized industry-standard methodology.

Change Management
The goal of COCUS change management process is to prevent unplanned service disruptions and maintain the integrity of services provided to customers. Therefore, all changes are reviewed, tested, and approved before deployment.

Segregation of duties
Responsibilities are clearly segregated within COCUS to reduce opportunities for unauthorized or unintentional modifications to infrastructure or systems.

Asset Management
COCUS uses an asset management solution to manage all mobile devices, automating device setup, updates for apps and operating systems, and security protocols.

Backups
Regular backups are performed and tested to ensure reliability. The frequency of backups is aligned with our business impact analysis and disaster recovery requirements.

Endpoint Security
COCUS has implemented Endpoint Security measures to safeguard mobile devices and servers from cyber threats, ensuring a secure and protected environment across all endpoints.

Incident Management

COCUS follows a robust incident management policy and procedures for events and incidents that may affect the confidentiality, integrity, or availability of systems or data, or that could potentially violate COCUS policies and controls.

This policy covers four key stages of the incident lifecycle: detection/reporting, triage, containment/ treatment, and post-incident. Each stage has clearly defined objectives, some major guidelines and designated responsibilities.

Risk Management

COCUS has implemented a risk management process to support the identification, evaluation, treatment, and monitoring of risks that could impact the confidentiality, integrity, availability, and privacy of personal data, customer data, and information systems.

Crisis Management and Business Continuity

COCUS established a Crisis Management process for crisis situations that may affect COCUS business. COCUS has also defined a business impact analysis for critical systems.

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 new third-parties to ensure they are aligned with COCUS security, data protection standards, and best practices.
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.
Additionally, COCUS conducts regular due diligence based on the third party's risk level to ensure their information security and data protection posture remain strong and that their commitment has not declined over time.

Audit and Compliance Management

COCUS conducts regular audits to assess compliance with security policies, standards, and regulations.

Secure Software Development

COCUS established security best practices to be integrated into the software development lifecycle.

Data Protection Management

Data Protection by Design and by Default

COCUS is committed to adhering to data protection regulations and standards by integrating data protection and privacy considerations into every stage of its processing activities—from the earliest phases of any new process, system, or product. To achieve this, all customer projects must undergo through a security demand process, ensuring that the information security and data protection teams are involved early to assess risks and define appropriate mitigation actions.

COCUS has implemented a Data Protection by Design and by Default policy to ensure that processes, systems and products are developed in a way that limits the collection and processing of personal data to only what is necessary for the identified purpose.

Customer Data

COCUS take it seriously to protect customer data. We are fully committed to protecting our customers' data and take this responsibility seriously. At COCUS, All COCUS employees are continuously trained and understand how to securely handle customer data to protect their privacy and confidentiality.
COCUS fully embraces and adheres to GDPR requirements, reflecting our dedication to maintaining the highest standards of data protection.

Conclusion

Security and Data Protection are an ongoing process at COCUS. We take these responsibilities seriously and work daily to improve and safeguard information. Protecting user data is a top priority across all COCUS infrastructre, applications, and operational activities.

To achieve this, COCUS relies on talented, skilled professionals, industry-leading technology to address risks, and well-defined policies and processes that ensure everything functions optimally. With a mindset focused on continuous improvement, we remain committed to the highest standards of security and data protection.

Content reviewed on March 5th, 2025.