EN

CERRIX

Strategic
Information Security Policy

This document outlines CERRIX's policies, procedures, and guidelines for managing Information Security.

RESTRICTED

CERRIX B.V.
September 2024

Document management

Information about this document and version are shown in the tables below.

Document Properties

Classification:	CERRIX Restricted
Subject:	Information Security Policy
Author(s):	R.M. van der Horst
Initial date of effect:	01-12-2023
Current version:	2.1
Status:	Final
Distribution:	CERRIX clients, Suppliers, Employees and Prospects.

Version Management

Version	Date	Author	Description of changes
0.1	08-11-2023	N. van der Heijden	Initial document set-up
0.2	10-11-2023	N. van der Heijden	Concept policy
1.0	28-12-2023	N. van der Heijden	Final document
1.1	23-8-2024	R.M. van der Horst	- Redefined the Information Security Objectives - Updated the Glossary of Terms (annex A)
2.0	15-10-2024	R.M. van der Horst	Review of the Information Security Policy by Ilse Vinke and René van der Horst. - Full text review and updates - Added a Privacy chapter - ISMS structure added - Major revision of the SDLC description
2.1	18-12-2024	R.M. van der Horst	Updated the glossary of terms Signed by Niels van Weereld to go into effect January 1, 2025.

CLASSIFICATION: CERRIX RESTRICTED

This document has been classified as CERRIX Restricted. The information contained within this document and any accompanying appendices is exclusively meant for the addressees that this document is directly distributed to. Distribution of this document, its contents and attachments by any party or person other than those listed in the distribution list is prohibited unless explicit prior written permission is extended by CERRIX B.V. This document, its contents, and attachments are subject to a Non-Disclosure Agreement.

If you received this document in error and/or you do not have explicit permission in the sense stated above, CERRIX B.V. requests you close this document immediately and destroy it and any copies made.

Nothing in this document may be duplicated, in part or in its entirety, and/or made public by any means without prior written authorization of CERRIX B.V. No rights can be deduced from the content of this document.

Table of Contents

1. Introduction

This document outlines the CERRIX B.V. rules, procedures, and guidelines for managing and protecting its information assets. It defines how data should be handled to ensure **Confidentiality**, **Integrity**, and **Availability** of our information.

1.1. Purpose

The purpose of this document is to set clear principles and policies to protect the critical assets of CERRIX B.V., and safeguard the information of clients, employees, and business partners.

1.2. Scope

This **Information Security Policy** covers all information, either electronic or physical, which is processed by CERRIX B.V. and its suppliers. Therefore, the policy also applies to all systems and equipment leased by CERRIX B.V.

1.3. Intended Audience

This document is intended for all of CERRIX's stakeholders, including:

1. Employees

   Ensuring they understand their roles and responsibilities in safeguarding company and customer data.

2. Suppliers

   Ensuring they understand their roles and responsibilities in safeguarding company and customer data.

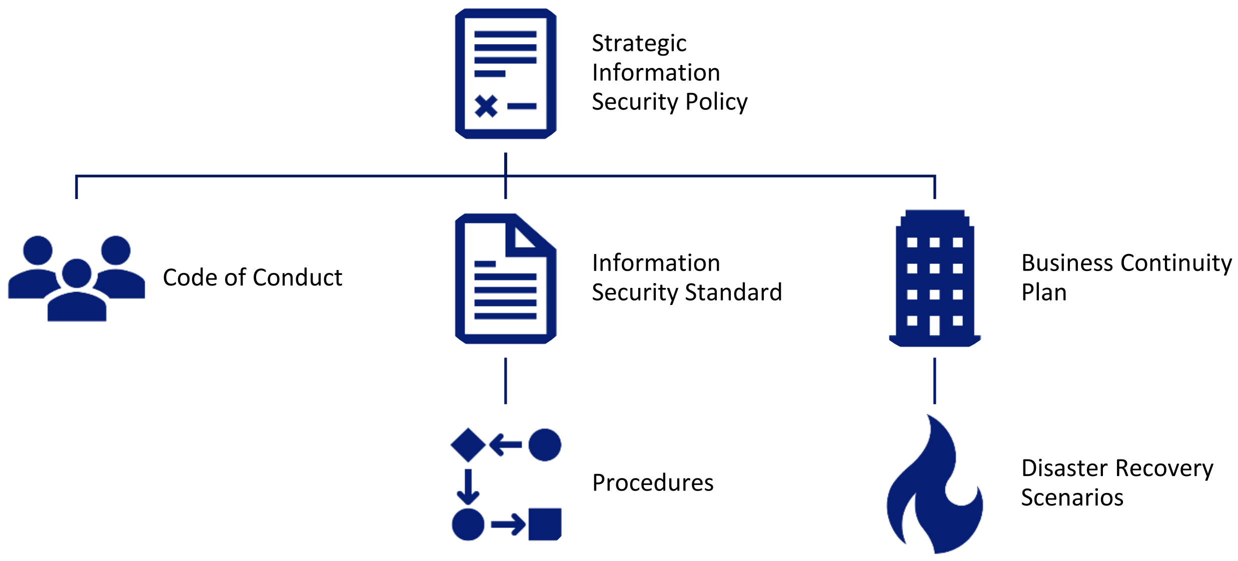
3. Customer and Prospects

   Customers can rely on the policy to ensure their data is handled securely, while prospects may review it as part of their decision-making process, evaluating CERRIX's commitment to robust information security practices.

1.4. Ownership

The CTO of CERRIX is accountable for the Information Security Management System, including this Strategic Information Security Policy.

1.5 Information Security Management System structure


Strategic Information Security Policy
Code of Conduct
Information Security Standard
Business Continuity Plan
Procedures
Disaster Recovery Scenarios

Strategic Information Security Policy

A high-level document that outlines an organization's approach to managing and protecting its information assets.

Code of Conduct

A set of guidelines or rules that define acceptable behavior and ethical standards for employees, contractors, and third parties when handling information and using information systems.

Information Security Standard

A set of policies and procedures with regards to Information Security.

Procedures

Specific procedures like the Incident Management Procedure and Change Management Procedure.

Business Continuity Plan

A comprehensive strategy that outlines how we will continue to operate during and after a significant disruption, such as a natural disaster, cyberattack, or system outage.

Disaster Recovery Scenarios

Specific scripts for Business Continuity Scenarios which describe in detail on how to respond.

2. Information Security Principles

To ensure safe and reliable SaaS-services for all its clients and to safeguard the information CERRIX B.V. processes, we have defined and apply, the following security principles:

1. Security & Privacy by Design

Proactively embed security and privacy protections into systems, services, and products from the very beginning, ensuring they are resilient, trustworthy, and compliant with legal and ethical standards.

2. Zero Trust

Enhance security by eliminating the assumption that anything inside or outside a network perimeter is automatically trustworthy. Instead, it operates on the principle of **"never trust, always verify."** This framework continuously authenticates and authorizes every user, device, and connection before granting access to resources, regardless of their location.

3. Defense in Depth

Provide comprehensive protection against security threats by using multiple layers of security controls. Instead of relying on a single defensive measure, this strategy creates a multi-tiered approach to protect systems, data, and networks, ensuring that if one layer is compromised, others remain in place to mitigate the risk.

4. Simplicity & Proportionality

Create effective, manageable, and balanced security measures that align with the specific needs and risks of our organization. Security solutions should be straightforward and easy to implement and maintain, reducing complexity that can lead to misconfigurations or gaps. Security measures should match the level of risk associated with the assets being protected.

3. Information Security Governance

This chapter describes how information security is managed and controlled within CERRIX B.V.

3.1. Management Commitment

Senior leadership will demonstrate their commitment by actively supporting the establishment, implementation, and continual improvement of the Information Security Management System (ISMS). This includes allocating necessary resources, assigning clear roles and responsibilities, and ensuring that the policy aligns with CERRIX's strategic objectives. Management should foster a security-conscious culture by promoting awareness, ensuring compliance with legal and regulatory requirements, and leading by example.

3.2. Information Security Roles and Responsibilities

The **RASCI-matrix** in this paragraph describes the roles and responsibilities with regards to Information Security within CERRIX:

Task	CTO	Management Team	Security Officer	DevOps	All Employees	Suppliers
Define overall security strategy	AR	I	S	S		
Promote security culture	R	A	S			
Security policy development	A	I	R			
Security compliance oversight	A	I	R			
Incident response leadership	AR	I	S			
Security risk assessments	A	C	R			
Vulnerability management	A		R	S		
Vendor risk management	A		R			
Security training and awareness	A		R			
Secure software development practices	A		I	R		
Pentesting	A		C	S		R
Security monitoring and detection (SOC)	A		S	I		R

Data encryption and protection	A		C	R		
Patch management	A		C	R		
Compliance with security policies	R	A	S	S		
Reporting security incidents		A	C		R	
Responding to information security incidents	A		R	S		
Third-party security audits	A	I	C			R
Implement, maintain and improve the ISMS	A		R			
Maintaining documentation of the ISMS	A		R			
Main point of contact for stakeholders on ISMS matters	A		R			
Reporting on information security performance	A	I	R			
Acting conform Information Security Policy	A				R	R
Continuous Improvement of the ISMS	A	S	R			

Legenda		
Letter	**Meaning**	**Description**
R	Responsible	The person who does the work.
A	Accountable	The person who makes key decisions and is ultimately answerable.
S	Supportive	People who provide assistance.
C	Consulted	People who are consulted and give input to the matter.
I	Informed	People kept up-to-date on progress and/or decisions..

3.3. Review and Revision of this Policy

The Information Security Policy will be reviewed at least annually to ensure that the content of the policy and the information security objectives remain accurate and effective.

4. Information Security Objectives

Information security objectives are crucial to protect sensitive customer data, ensure service reliability, and maintain compliance. CERRIX has defined the following information security objectives:

1. Ensure Data Confidentiality, Integrity and Privacy
   - Ensure that we protect information (client, internal, employee) from unauthorized access, loss, tampering or leakage.
   - Ensure that information remains accurate and consistent.
   - Ensure that information is recoverable in case of unforeseen events.

2. Guarantee Service Availability
   - Ensure continuous access to our SaaS GRC platform.
   - Ensure platform performance and scalability to avoid outages and bottlenecks.

3. Comply with Regulatory and Legal Requirements
   - Ensure that we comply with relevant regulations, depending on the clients and regions served.

4. Maintain Secure Software Development Practices
   - Ensure that we comply with CERRIX internal security standards.
   - Ensure that we limit security vulnerabilities.
   - Ensure that we limit security incidents.

5. Enhance Incident Detection and Response
   - Ensure that incidents are detected in a timely manner.
   - Ensure that the incident response is adequate and incidents are resolved within the agreed Service Levels.

6. Control Internal, External and Third-Party Risks
   - Ensure that Risks are identified, prioritized and mitigated.
   - Ensure business continuity by protecting against identified as well as unidentified risks (preparedness).

7. Foster a Security-Aware culture
   - Ensure employee awareness of security risks.
   - Promote Secure Behavior and Best Practices.

5. Classification and Handling of Assets and Information

To identify and protect critical information and assets, CERRIX B.V. will ensure that the following measures are in place:

- Critical information and assets are identified and classified.
- Classified information is labelled.
- Information and assets have been assigned an owner.
- Information and assets will be used according to CERRIX's Acceptable Use Policy.
- Information and assets are secured as defined in CERRIX's Information Security Standard.
- Information and assets must be returned to CERRIX B.V. at the end of the contractual agreement.

5.1 Storage & Transfer of Information

CERRIX will ensure that appropriate measures are in place to protect information during storage and transfer. Back-ups and encryption of data will be applied based on the classification of the information. The following measures are in place:

- Information is stored and handled based on its CIA-classification.
- Data will have a back-up scheme based on its CIA-classification.
- Back-up and restore tests will be executed at least twice year.
- Encryption-at-rest will be applied to data in accordance with the Encryption Policy
- The storage and transfer of information is safeguarded by complying to the Information Security Standard.

5.2 Retention & Disposal of Information

CERRIX will ensure that the following measures are in place to protect information during its retention and disposal:

- CERRIX implemented a secure method to dispose of physical and digital data.
- CERRIX established clear and documented retention periods based on legal and contractual requirements.
- Only authorized personnel will be permitted to initiate, authorize, and oversee the data disposal process.

6. Access Control

To prevent unauthorized access to information and information processing, CERRIX has established the following the methods:

- User access to the network, systems, and information of CERRIX will be regulated in accordance with the Access Management Policy.
- The use of Multi-Factor Authentication and/or SSO is mandatory.
- Privileged accounts must use Multi-Factor Authentication and/or SSO.
- Access to systems and applications is only authorized if passwords are used according to the Password Policy.
- Access control for systems and applications is regulated according to the Access Management Policy.
- During the employee offboarding process, the user account will be blocked on, or before the day of contract termination. Application accounts where SSO is not possible will be manually removed.

7. Physical Security

To prevent unauthorized physical access to information and assets, CERRIX will ensure that the following measures are in place:

- Physical access to the CERRIX office is only possible with authorization and all access is logged.
- Burglary and *fire protection systems* will continuously monitor and report unauthorized access.
- Within the CERRIX office, secure zones are defined and protected based on the accessible information and assets within that zone.
- A clear-screen & clear-desk policy is used ensure no confidential data is visible to unauthorized persons.
- *The use of removable storage media is limited to the company storage media.*
- Physical security during remote working is ensured in accordance with the Remote Working Policy.

8. Employee Security

To ensure that CERRIX personnel meet the integrity, awareness, competence, and vigilance requirements, CERRIX has established the following measures:

- HR is familiar with the requirements and responsibilities of submitting a VOG.
- New employees must hand in a VOG before the start of employment.
- Upon termination of employment, (ex-)employees must still adhere to the signed non-disclosure agreement (see Chapter 3.2.3.).
- A competence and awareness plan are drawn up and directed by management annually.
- Human factor security is implemented in accordance with the Remote Working Policy
    - A disciplinary process is implemented to act against violation of this policy (see Chapter 14).

9. Information Security Incident Management

To guarantee a consistent and effective approach to information security incidents, the following measures are in place:

- Procedures are implemented to report and report to information security incidents.
- Incidents can be scaled up to a disruption followed by the Business Continuity Plan.
- Procedures are implemented regarding the handling of (forensic) evidence.
- Incidents are followed by an improvement action to learn from and prevent these incidents.

10. Secure Software Development Lifecycle

As part of our commitment to safeguarding information security, we adhere to a robust Secure Software Development Lifecycle (SDLC) in alignment with ISO 27001 standards. This process ensures that security is integrated into every phase of software development, from requirements to deployment and operations. The SDLC framework is designed to minimize risks, protect sensitive data, and maintain the integrity, confidentiality, and availability of the software and its associated assets.

1. Requirements

During the requirements phase, security considerations are integrated into the initial requirements of our software. This includes defining security requirements, and identifying regulatory and compliance needs (such as GDPR, DORA and NIS2).

2. Design

We follow the principles of **Least Privilege**, **Defence-in-Depth**, and **Security & Privacy-by-design** to ensure that potential vulnerabilities are addressed before development begins. Architectural decisions are documented, and security controls are identified, including encryption, access controls, and audit logging requirements.

We also ensure that all third-party software components and libraries undergo security reviews to minimize the risk of introducing vulnerabilities through external dependencies.

3. Development

Developers are required to follow secure coding standards and best practices, as outlined in recognized guidelines such as OWASP. All code must be developed to prevent common vulnerabilities, such as SQL injection and cross-site scripting (XSS).

Peer code reviews are required to ensure compliance with our standards.

4. Testing

Testing is an integral part of our SDLC. We utilize:

- Functional Testing
- Regression Testing
- Unit Testing
- Automated Testing

Separately our application undergoes a extensive Penetration Test, at least once a year, by and independent third-party.

5. Deployment

Prior to deployment a Regression Test is performed to validate the proper operations of our software, The deployment process is tightly controlled, and access to production environments is limited to authorized personnel only. Security patches and updates are regularly reviewed and applied promptly.

We also ensure that the production environment is configured securely, including the implementation of network security controls. Cloud infrastructure is subject to security best practices such as encryption, key management, and logging.

6. Operations

After deployment, software is continuously monitored for potential security incidents, and vulnerabilities are managed throughout its lifecycle. This includes regular security assessments, and timely application of security patches.

Incident management procedures, in alignment with ISO 27001, ensure that any security breach or threat is promptly addressed, with clear roles and responsibilities for identifying, responding to, and recovering from incidents.

Regular updates to the software, including security patches, must be applied as part of ongoing maintenance efforts.

11. Security in Supplier Relationships

To guarantee that confidentiality, integrity, and availability of data is safeguarded in outsourced (cloud) services, CERRIX will ensure that appropriate measures are in place:

- Supplier relationships are identified and documented.
- Sufficient agreements on information security are made with all suppliers.
- Critical suppliers will be periodically assessed by CERRIX.

12. Business Continuity Management

To guarantee strong operational resilience and business continuity in case of disruptions, CERRIX will ensure that appropriate measures are in place:

- A Business Continuity Plan is in place and available as documented information.
- Disaster recovery procedures are implemented.
- The disaster recovery procedures will be tested on planned intervals.

13. Privacy

we are committed to safeguarding the privacy of our users, partners, and employees. Our approach to data protection is fully compliant with the General Data Protection Regulation (GDPR) and ISO/IEC 27001 standards. We ensure that all personal data is processed lawfully, transparently, and securely, in accordance with the rights of data subjects.

We implement appropriate technical and organizational measures to protect personal data from unauthorized access, alteration, disclosure, or destruction. Personal data is only collected for legitimate business purposes and is processed in a manner consistent with the principles of data minimization, accuracy, and storage limitation.

Data subjects are granted full control over their personal information, including the right to access, rectify, or erase their data, as well as the right to restrict or object to its processing. In the event of a data breach, we have established protocols to promptly notify the affected parties and relevant supervisory authorities as required by GDPR.

14. Compliance & Assurance

The assurance of compliance with the information security policy is rendered by the monitoring of the Information Security Officer, management reviews and by the internal- and external audits on the design, implementation, and effectiveness of the Information Security Management System.

14.1 Policy Violation & Disciplinary process

Non-compliance with this information security policy or underlaying standards can lead to disciplinary actions, including but not limited to verbal or written warnings, suspension, termination of contract, or legal action, as appropriate for the violation.

15. Signature

In witness whereof, the parties hereto have executed this document as of the date written below.

The Hague, January 1, 2025

Ondertekend door:

2A9B26AACDB4450...

Niels van Weereld

CEO

Annex A: Glossary of Terms

Term	Description
Assurance	Refers to the confidence or certainty that information is accurate, reliable, and trustworthy.
Audit	An independent examination of an organization to ensure accuracy, compliance with applicable laws and regulations.
Availability	Refers to the ability of a system, service, or application to be accessible and operational when needed.
BCP	**Business Continuity Plan** A strategic framework that outlines procedures and instructions an organization must follow to continue operating during and after a disaster or unexpected disruption.
CIA	Refers to **Confidentiality, Integrity, and Availability**. These are the key principles for protecting data.
Clear-Screen/Clear-Desk policy	A security measure implemented by organizations to protect sensitive information and maintain a secure work environment.
Compliance	The act of adhering to established laws, regulations, standards, and internal policies.
Confidentiality	Refers to protecting sensitive information from unauthorized access and disclosure.
Data Controller	An individual or organization that determines the purposes and means of processing personal data.
Data Processor	An individual or organization that processes personal data on behalf of a data controller.
Defense in depth	A strategy that uses multiple layers of security controls to protect systems and data. If one layer is compromised, additional layers still provide protection, reducing the overall risk.
Encryption	An individual or organization that processes personal data on behalf of a data controller.
Encryption-at-rest	Refers to the practice of encrypting data stored on physical devices, such as hard drives or cloud storage, to protect it from unauthorized access.
Encryption-in-Transit	Refers to the practice of encrypting data while it is being transmitted over networks, such as the internet or internal networks, to protect it from unauthorized access during transmission.
GDPR	**General Data Protection Regulation** A European Union law that governs how organizations collect, store, and process personal data of individuals within the EU.

Integrity	Refers to the protection of data from unauthorized modification, ensuring that information remains accurate, consistent, and trustworthy throughout its lifecycle.
ISMS	**Information Security Management System** A structured framework of policies, procedures, and controls designed to manage and protect an organization's sensitive data.
Management	The management board of CERRIX B.V., consisting of the managing director, manager operations and Chief Technology Officer (CTO).
Multi-Factor Authentication	A security process that requires users to provide two or more distinct forms of verification to access an account or system.
Penetration Test	Commonly known as a **pen test**, is an authorized simulated cyberattack on a computer system, network, or web application.
PII	**Personal Identifiable Information** Refers to any data that can be used to identify a specific individual, either directly or indirectly.
Privacy	The right of individuals to control their personal information and protect themselves from unauthorized access or intrusion.
RASCI-matrix	A RASCI matrix is a tool to define roles and responsibilities. It clarifies who is involved in tasks and their level of involvement.
SaaS-service	**Software as a Service** A cloud computing model where software applications are delivered over the internet.
Security by design	Refers to incorporating security measures and practices into the development process from the design phase, rather than as an afterthought.
SSO	**Single Sign On** An authentication method that allows users to access multiple applications or services with a single set of login credentials, reducing the need for multiple passwords and improving user convenience and security.
VOG	**Verklaring Omtrent Gedrag** a Dutch certificate of good conduct that verifies an individual's criminal record status, issued by the Dutch Ministry of Justice and Security.

Zero trust	A security principle that assumes no user or system is inherently trusted, whether inside or outside the network.