Information Security Policy

By Jawa Corporate Real Estate Solutions B.V.

Effective Date: November 10th, 2024
Review Date: November 10th, 2024

1. Introduction

Jawa Corporate Real Estate Solutions B.V. ("Jawa" or "the Company") is committed to safeguarding the confidentiality, integrity, and availability of all business, client, and employee information. As a boutique company, we recognize that information security is critical to protecting the trust of our clients and maintaining the overall integrity of our operations. This Information Security Policy outlines the framework to manage and secure information, ensuring that all employees understand their responsibilities and take appropriate measures to protect sensitive data.

This policy applies to all employees, contractors, and third-party service providers who may have access to information held by the company.

2. Scope

This policy applies to all forms of data and information managed by Jawa, including:

- Client and employee personal data
- Business financial and operational information
- Internal communications and documents
- IT systems, networks, applications, and devices

All employees are required to follow this policy to protect the company's information from unauthorized access, loss, or damage.

3. Core Principles

Jawa is committed to the following core principles of information security:

A. Confidentiality:

- We will protect sensitive information from unauthorized access. Only those who need access to specific information to perform their job functions will have access to it.
- All employees must safeguard the confidentiality of information entrusted to them by clients, partners, and the company.

B. Integrity:

- Information must be accurate, complete, and reliable. We will implement measures to prevent unauthorized changes or corruption of data.
- Employees are responsible for ensuring that the data they manage is correct and up-to-date.

C. Availability

- Information and systems must be available when needed by authorized users. We will implement safeguards to ensure that critical systems and data remain accessible and protected against potential disruption.
- Regular backups and disaster recovery protocols will be in place to minimize the impact of any data loss or system failures.

4. Roles and Responsibilities

Each employee at Jawa CRES has a role in maintaining information security, with the following responsibilities:

- Jeroen Lubbers / Managing Director: bears overall responsibility for ensuring the security of company data and the implementation of this policy. He will coordinate with employees to ensure proper security practices are followed and will oversee the implementation of any necessary security measures (e.g., backup systems, encryption, software updates).
- All other employees are responsible for following the information security practices outlined in this policy. Specific responsibilities include:
  - Protecting passwords and confidential information.
  - Reporting any suspicious activity, potential security incidents, or data breaches to you immediately.
  - Participating in any security training and following data protection protocols.
- External Contractors/Third Parties: Any contractors or third parties who have access to the company's data or systems must adhere to the same information security standards, and contracts will specify security requirements.

5. Information Security Measures

A. Access Control

- Access to sensitive or confidential information will be granted based on the principle of least privilege—employees will only have access to the information they need to perform their specific job functions.
- Access controls will be reviewed periodically to ensure that only authorized individuals have access to systems or data.

B. Passwords and Authentication

- Strong passwords (at least 12 characters, including upper and lowercase letters, numbers, and special characters) are required for all systems and applications.
- Passwords must not be shared, and employees should change them periodically. Where possible, multi-factor authentication (MFA) will be implemented.

C. Data Protection and Encryption

- Sensitive and confidential information (e.g., personal data, financial information) will be protected using encryption methods when stored and transmitted.
- Secure methods (e.g., encrypted email, password-protected files) will be used for sharing sensitive data with clients, partners, and third parties.

D. System and Device Security

- All devices used to access company data (laptops, smartphones, etc.) will be equipped with antivirus software and firewalls. These devices will also be kept up-to-date with security patches and software updates.
- Devices will be configured to lock after a period of inactivity to prevent unauthorized access if left unattended.
- Employees are responsible for reporting any lost or stolen devices immediately.

E. Data Retention and Disposal

- We will only retain data as long as necessary for business purposes, legal compliance, or contractual obligations.
- When data is no longer required, it will be securely deleted or destroyed. For physical documents, shredding will be used, and digital files will be securely wiped using appropriate data destruction tools.

F. Backup and Disaster Recovery

- Regular backups of critical data will be performed and stored in secure, separate locations (e.g., cloud storage, external drives).
- A disaster recovery plan will be in place to ensure that data can be restored in the event of an emergency, such as a system failure, data breach, or cyberattack.

G. Incident Reporting and Response

- Employees must immediately report any suspected security incidents or breaches (e.g., data theft, unauthorized access, phishing attempts) to the company owner.
- The company will investigate any security incidents and take appropriate action to mitigate any potential harm, including notifying clients or regulatory bodies if necessary, in compliance with GDPR and other applicable regulations.

H. Employee Training and Awareness

- Employees will receive regular training on information security best practices, including how to recognize phishing attempts, safe handling of sensitive information, and proper use of company systems.

- Employees will be encouraged to stay vigilant and report any unusual activities or potential security risks.

I. Compliance with Legal and Regulatory Requirements

- The Company will ensure compliance with data protection regulations, including the General Data Protection Regulation (GDPR), Dutch Data Protection Act, and any other relevant industry-specific regulations.
- Any third-party vendors or partners who handle client or employee data will be required to comply with the same data protection standards.

6. Third-Party Security

When sharing data with third-party service providers (e.g., IT service providers, external contractors), the company will:

- Ensure that contracts with third parties contain appropriate data protection clauses.
- Require that third parties adhere to the same information security standards, including maintaining secure systems and processes for handling sensitive information.
- Regularly assess the security posture of third-party vendors and partners, especially those who have access to sensitive or critical company data.

7. Monitoring and Auditing

The Company will regularly monitor and review its information security practices to identify potential vulnerabilities and ensure compliance with this policy. This may include:

- Conducting periodic risk assessments and security audits.
- Reviewing user access logs and security reports to identify unauthorized access or unusual activity.

8. Enforcement

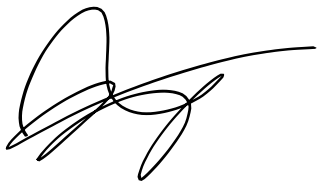
Failure to comply with this Information Security Policy may result in disciplinary action, including termination of employment for serious violations. All employees are expected to understand and follow the principles outlined in this policy.

9. Review and Updates

This policy will be reviewed annually, or whenever there are significant changes in regulations, business processes, or technology. Updates will be made as necessary to ensure that the company continues to meet the highest standards of information security.

Conclusion

Jawa Corporate Real Estate Solutions B.V. is committed to ensuring the security of all information entrusted to us by clients, employees, and other stakeholders. By adhering to this Information Security Policy, we will protect sensitive data from unauthorized access, maintain the integrity of business information, and ensure that our operations comply with applicable laws and regulations. All employees share responsibility for information security, and by following the practices outlined in this policy, we will ensure that our business remains secure and trusted.



Jeroen Lubbers
Managing Director
Jawa Corporate Real Estate Solutions B.V.

Date: November 10th, 2024
Place: Arnhem, The Netherlands