Information Security Policy

Security Policy

Introduction

This Information Security Policy has been established to protect the confidentiality, integrity, and availability of Build38's information assets. It complies with the ISO/IEC 27001:2022 standard and applies to all employees, freelancers, business partners, suppliers, and third-party users who access or use the information assets of Build38.

Purpose

This policy aims to protect information assets from all threats, whether internal or external, deliberate or accidental. It also aims to ensure compliance with all applicable laws, regulations, and contractual obligations.

The policy establishes a framework for setting, reviewing, and achieving information security objectives. It defines the responsibilities of employees, freelancers, business partners, suppliers, and third-party users in protecting Build38's information assets.

Additionally, the policy aims to promote awareness and guide decision-making processes related to information security within the organization.

Scope

Build38, a company dedicated to developing software to help global companies issue locally compliant invoices, has decided to introduce an Information Security Management System based on ISO27001:2022 certification to improve the services provided to its clients.

This policy applies to all information assets owned, leased, handled, or otherwise controlled by Build38, including information stored on physical or electronic media, information transmitted over

networks or through any communication channels, and information processed or handled by employees, contractors, or third-party users.

Objectives

The primary objectives of this policy are to protect the **confidentiality** of information to prevent unauthorized disclosure, ensure the **integrity** of information to prevent unauthorized modification, and ensure the **availability** of information to authorized users when needed.

Additionally, the policy seeks to ensure compliance with **applicable laws, regulations, and contractual obligations** such as the General Data Protection Regulation (GDPR), the Spanish Data Protection Act (LOPDGDD),Law 10/2021 on Remote Work, etc.. while continuously **improving** the information security management system (ISMS).

Security Organization & Responsibilities

Build38 Management is responsible for providing leadership and commitment to information security. They ensure adequate resources are available to implement and maintain the information security management system and review and approve information security policies and procedures.

The Information Security Management System Responsible (ISMS Responsible) is responsible for developing, implementing, and maintaining the information security management system. This includes conducting risk assessments, implementing appropriate controls, and reporting on the effectiveness of the information security management system to senior management.

Employees, contractors, and third-party users are responsible for complying with this policy and all related information security procedures. They must report any suspected information security incidents or vulnerabilities to the ISMS Responsible and participate in information security training and awareness programs.

Security Measures

Aligned with our commitment to safeguarding information assets and maintaining the integrity of our operations, we have established a comprehensive set of security measures. These measures encompass a range of strategies and technologies to protect our systems, data, and resources

from potential threats and ensure the confidentiality, integrity, and availability of information critical to our business.

- **Human Resources:** Human resource security measures are implemented to ensure that employees, contractors, and third-party users know their responsibilities and are equipped to safeguard information assets.
- **Physical Security:** Physical security measures are implemented to protect information assets from unauthorized access, damage, or interference.
- **Asset Management:** Asset management measures are implemented to ensure that all information assets are properly identified, classified, and secured throughout their lifecycle. This includes maintaining an accurate inventory of assets, assigning ownership, and defining usage guidelines. Regular audits and reviews are conducted to ensure assets are adequately protected.
- **Access Control:** Access to information assets is limited to authorized users only. Strong authentication and authorization mechanisms are implemented, and access rights are periodically reviewed to ensure they remain appropriate.
- **Network Security:** Measures are implemented to secure the company's network infrastructure against unauthorized access, breaches, and other security threats. This includes firewalls, intrusion detection systems, and regular network monitoring.
- **Operations Security:** Operations security measures are enacted to preserve the integrity of operational processes and guarantee the secure execution of daily activities. This includes implementing robust monitoring systems and logging mechanisms to swiftly identify and respond to suspicious activities.
- **Secure Development:** Security practices are integrated into the software development lifecycle to ensure that applications are designed, developed, and maintained securely. This includes code reviews, vulnerability assessments, and regular security testing.
- **Risk Management:** Regular risk assessments are conducted to identify and evaluate risks to information assets. Appropriate controls are implemented to mitigate identified risks, and the effectiveness of these risk management activities is continuously monitored and reviewed.
- **Data Management:** Information is classified based on its sensitivity and criticality. Appropriate handling procedures are defined for each classification level to ensure the protection of information throughout its lifecycle.
- **Incident Management:** An incident management process is established and maintained to detect, respond to, and recover from information security incidents. All security incidents must be reported promptly to the designated incident response team. Incidents are investigated to determine the root cause and to prevent recurrence.

- **Business Continuity:** Plans are established and maintained to ensure the continuation of critical business functions in the event of a disruption. These plans are regularly tested and updated to ensure their effectiveness.
- **Compliance:** Compliance with all relevant laws, regulations, and contractual obligations related to information security is ensured. Regular audits and reviews are conducted to verify compliance with this policy and the information security management system.
- **Third-Party Management:** Security requirements are defined and enforced for third-party vendors and partners. Regular assessments and reviews are conducted to ensure that third parties comply with the company's information security standards.
- **Awareness and Communication:** All employees, contractors, and third-party users receive regular information security training. The organization promotes awareness of information security policies, procedures, and best practices.

Security Improvement

Build38 is committed to the principle of continuous improvement in its information security management practices. Regular assessments and reviews are conducted to identify areas for enhancement in the ISMS. Feedback from audits, incident reports, and employee suggestions are systematically evaluated to implement improvements. Metrics and performance indicators are monitored to measure information security controls' effectiveness and identify opportunities for refinement. Continuous improvement efforts ensure that the ISMS remains effective, responsive to emerging threats, and aligned with the strategic objectives of Build38.

Compliance

Build38 reserves the right to audit and/or monitor employee activities and information handled through information systems, in accordance with the applicable and current regulations.

All employees are expected to adhere to the Information Security Policy and Topic-Specific Policies, and failure to comply will result in appropriate disciplinary measures proportional to the violation committed.

Review

This policy undergoes regular review on an annual basis and is updated as necessary whenever significant changes occur in the information security management system (ISMS).

It is continuously enhanced through internal audits, certification audits, and Management Reviews to ensure ongoing improvement.

Change Management

Version	Date	Description
1.0	05/07/2024	Policy Definition
2.0	04/06/2026	Policy Review