Classification	**Internal Use**
Information Owner	**IT Security Team**

IT Security Policy

AUG 2024

Prepared for: Grant Transformers

Prepared by: Binary IT, IT Security Team

Contents

1. Purpose

The purpose of this IT Security Policy is to define the principles and requirements for the protection of information assets at **Grant Transformers** in accordance with ISO/IEC 27001:2013 standards. This policy aims to safeguard the confidentiality, integrity, and availability of company information and to support the establishment, implementation, maintenance, and continual improvement of the Information Security Management System (ISMS).

2. Scope

This policy applies to all Grant Transformers employees, contractors, vendors, and third parties who access or handle the company's information assets. It encompasses all information systems, data processing facilities, and physical and electronic data storage, regardless of their location.

3. Information Security Objectives

Grant Transformers is committed to:

- Ensuring the confidentiality, integrity, and availability of information.
- Protecting information against unauthorized access.
- Complying with legal, regulatory, and contractual obligations.
- Managing risks to information assets effectively.
- Continually improving the ISMS (**I**nformation **S**ecurity **M**anagement **S**ystem**).**

4. Roles and Responsibilities

4.1 Top Management

- Provide leadership and commitment to the ISMS.
- Ensure alignment of the ISMS with the company's strategic objectives.
- Allocate necessary resources for the ISMS.
- Review and approve the IT Security Policy and ISMS objectives.

4.2 Information Security Manager (ISM)

- Oversee the implementation and maintenance of the ISMS.
- Ensure that the IT Security Policy is communicated, understood, and adhered to.
- Conduct regular risk assessments and ensure appropriate controls are in place.
- Report on the performance of the ISMS to top management.

4.3 IT Security Team

- Implement and manage security controls in accordance with the ISMS.
- Monitor compliance with the IT Security Policy and report deviations.
- Conduct regular security awareness training.
- Respond to and manage information security incidents.

4.4 Employees and Contractors

- Follow the IT Security Policy and procedures.
- Report any security incidents or weaknesses.
- Participate in security awareness training.

5. Information Classification and Handling

5.1 Information Classification

Information must be classified based on its sensitivity and criticality:

Public	Non-sensitive information available to the public
Internal Use Only	Information restricted to internal use within the company
Confidential	Sensitive information accessible only to authorized personnel
Highly Confidential	Critical information with the highest level of protection required.

5.2 Data Handling Procedures

Storage	Confidential and Highly Confidential data must be encrypted and stored in secure locations.
Transmission	Sensitive data must be encrypted during transmission
Disposal	Data no longer needed must be securely disposed of following approved methods (e.g., shredding, degaussing).

6. Access Control

6.1 Access Control Principles

- Access to information assets must be based on business and security requirements.
- Access controls should follow the principle of least privilege (PoLP) and segregation of duties (SoD).
- Multi-factor authentication (MFA) must be implemented for accessing critical systems and data.

6.2 User Account Management

- Accounts must be managed according to documented procedures, including creation, modification, and termination.
- Accounts must be reviewed regularly to ensure that access rights remain appropriate.

6.3 Remote Access

- Remote access must be secured using VPNs or other encrypted methods.
- Remote workers must follow the same security practices as on-site employees.

7. Physical and Environmental Security

7.1 Secure Areas

- Physical access to secure areas must be controlled and monitored.
- Secure areas must be protected against unauthorized access, damage, and interference.

7.2 Equipment Security

- Equipment must be sited or protected to reduce risks from environmental threats and unauthorized access.
- Equipment used outside the organization’s premises must be protected to the same level as internally housed equipment.

8. Operations Security

8.1 Operational Procedures and Responsibilities

- Documented operating procedures must be maintained for all IT operations.
- Changes to information processing facilities and systems must be controlled and approved following a formal change management process.

8.2 Malware Protection

- Appropriate measures must be in place to detect and prevent the introduction of malicious software.
- Anti-virus software and other protective mechanisms must be kept up-to-date.

8.3 Backup

- Regular backups of critical information must be performed and tested.
- Backup data must be securely stored and protected from unauthorized access.

9. Communications and Operations Management

9.1 Network Security Management

- Networks must be managed and controlled to protect information in systems and applications.
- Security measures must be implemented to prevent unauthorized access and attacks on the network.

9.2 Media Handling

- Media containing sensitive information must be protected against unauthorized access, misuse, or corruption.
- Media must be securely disposed of when no longer required.

10. Information Systems Acquisition, Development, and Maintenance

10.1 Secure Development

- Security requirements must be defined and implemented for all new information systems or enhancements to existing systems.
- Development and testing environments must be separated from production environments.

10.2 Supplier Relationships

- Information security requirements must be included in agreements with suppliers and third parties.
- Suppliers must be monitored to ensure compliance with security requirements.

11. Information Security Incident Management

11.1 Reporting Information Security Events

- All employees must report any information security events or weaknesses immediately.
- A formal incident management process must be in place to ensure a timely and effective response.

11.2 Incident Response and Recovery

- The IT Security Team must investigate incidents, mitigate impacts, and restore operations.
- Lessons learned from incidents must be documented and used to improve security controls.

12. Business Continuity Management

12.1 Information Security Continuity

- Information security must be an integral part of the company's Business Continuity Plan (BCP).
- Regular testing and updating of the BCP must be conducted to ensure its effectiveness.

13. Compliance

13.1 Legal, Regulatory, and Contractual Compliance

- The company must comply with applicable legal, regulatory, and contractual requirements related to information security.
- Regular audits and reviews must be conducted to ensure compliance.

13.2 Internal ISMS Audits

- Regular internal audits of the ISMS must be conducted to evaluate its effectiveness and identify areas for improvement.
- Audit results must be reported to top management and actions taken to address any identified issues.

14. Policy Review

This IT Security Policy must be reviewed annually or whenever significant changes occur in the company's operations or external environment. Changes to the policy must be approved by top management and communicated to all relevant stakeholders.

Company Name	Grant Transformers
Policy Written on	Aug 2024
Next Policy Review	Aug 2025