	General Cybersecurity Policy	CORPORATE POLICY
		Code: CS-PL-GE-01-2023-v02-00
- CONFIDENTIAL-	Version: 2. Revision: 1	Approval Date: 2024/Mayo/30
		Effectiveness: 2025/Mayo/30



General Cybersecurity Policy

Cybersecurity Management
IT Research & Development Department

Mexico City, September 2023

CS-PL-GE-01-2023-v02-00


	General Cybersecurity Policy	CORPORATE POLICY
		Code: CS-PL-GE-01-2023-v02-00
		Approval Date: 2024/Mayo/30
- CONFIDENTIAL -	Version: 2. Revision: 1	Effectiveness: 2025/Mayo/30

Tabla de contenido

INTRODUCTION	3
GOALS AND SCOPE	3
ROLES AND RESPONSIBILITIES	3
PROTECTION OF INFORMATION	3
ACCESS AND AUTHENTICATION.....	4
DEVICE PROTECTION.....	4
ACCEPTABLE USE OF COMPUTER SYSTEMS.....	4
USE OF E-MAIL AND THE INTERNET	4
SECURITY AWARENESS AND TRAINING.....	4
SECURITY INCIDENT MANAGEMENT	5
COMPLIANCE AND AUDIT	5
SUPPLIER MANAGEMENT	5
MONITORING AND DETECTION OF THREATS.....	5
PERSONAL DEVICES (BYOD).....	5
PATCHES AND UPDATES.....	6
INFORMATION ENCRYPTION PROTOCOLS	6
BUSINESS CONTINUITY AND DISASTER RECOVERY.....	6
IMPLEMENTATION	6

	General Cybersecurity Policy	CORPORATE POLICY
		Code: CS-PL-GE-01-2023-v02-00
		Approval Date: 2024/Mayo/30
- CONFIDENTIAL -	Version: 2. Revision: 1	Effectiveness: 2025/Mayo/30

INTRODUCTION

Information security is critical to the success of any modern enterprise. This policy establishes the standards and procedures necessary to ensure information security in our company. Employees, contractors and other parties who use the company's resources must abide by this policy and remain actively and permanently vigilant about information security

GOALS AND SCOPE


1. Safeguard critical company information, including customer data, intellectual property, financial and strategic information.
2. Protect the company's information technology resources, including hardware, software, networks and systems.
3. Develop plans (BCP and DRP) that will help ensure a high rate of future business continuity and availability of the company's technology resources in the event of disruptions due to attacks.
4. Comply with applicable laws (Mexican Law) and regulations and maintain the confidentiality, integrity and availability of information.
5. Create work plans to achieve ISO 2700 certification within a reasonable period of time.

ROLES AND RESPONSIBILITIES

1. Senior management is responsible for ensuring that information security is considered in all decisions where sensitive data is involved, and for allocating the necessary resources.
2. The Cybersecurity Manager is responsible for developing, implementing and maintaining the information security policy.
3. Managers are responsible for ensuring that the employees under their charge comply with this policy and that the necessary measures are taken to guarantee information security.
4. Employees are responsible for complying with this policy and taking measures to protect the company's information and resources.

PROTECTION OF INFORMATION

1. Establish access controls to ensure that confidential information is accessible only by authorized personnel.
2. Establish security measures to ensure the integrity and confidentiality of data stored in computer systems.
3. Regularly back up critical information.

	General Cybersecurity Policy	CORPORATE POLICY
		Code: CS-PL-GE-01-2023-v02-00
		Approval Date: 2024/Mayo/30
- CONFIDENTIAL -	Version: 2. Revision: 1	Effectiveness: 2025/Mayo/30

ACCESS AND AUTHENTICATION

1. Provide employees access only to the resources necessary to do their jobs.
2. Employees must use secure passwords and change them regularly. Passwords must contain at least 12 characters, including numbers, upper and lower case letters, and symbols.
3. Employees should not share passwords or allow others to use their accounts.
4. Multi-factor authentication (MFA) is mandatory for all users accessing company resources.

DEVICE PROTECTION

1. All electronic devices, including laptops and cell phones, must have virus and malware protection software and the latest security updates.
2. Devices should be set to automatically lock after a period of inactivity, and strong authentication measures should be implemented for access to sensitive devices and data.

ACCEPTABLE USE OF COMPUTER SYSTEMS


1. Establish regulations and procedures to ensure appropriate use of the company's computer systems.
2. Prohibit unauthorized use of computer systems, such as the downloading or use of unauthorized software.

USE OF E-MAIL AND THE INTERNET

1. Employees and outside parties should use e-mail and Internet access responsibly and only for legitimate business purposes.
2. Users should avoid accessing insecure or unknown websites, and spam and phishing emails should be blocked.

SECURITY AWARENESS AND TRAINING

1. Regular training should be provided to all employees on the importance of information security and how to protect it.
2. Cybersecurity awareness will be encouraged among all employees.

	General Cybersecurity Policy	CORPORATE POLICY
		Code: CS-PL-GE-01-2023-v02-00
		Approval Date: 2024/Mayo/30
- CONFIDENTIAL -	Version: 2. Revision: 1	Effectiveness: 2025/Mayo/30

SECURITY INCIDENT MANAGEMENT

1. Establish procedures for reporting and managing security incidents.
2. Conduct investigations and analysis of security incidents to identify causes and prevent future similar incidents.
3. This cybersecurity policy must be reviewed and updated on a regular basis to ensure that it remains effective and up to date with new technology and security risks. In addition, an audit program must be created to assess the effectiveness of security controls and ensure compliance with this cybersecurity policy.

COMPLIANCE AND AUDIT

1. Conduct regular audits to evaluate compliance with this cybersecurity policy.
2. Audit results will be used to identify areas for improvement and take corrective action as appropriate.
3. Conduct penetration tests to assess the security of the company's IT systems..
4. The cybersecurity policy must be updated regularly to keep up with best practices and regulatory changes.

SUPPLIER MANAGEMENT


1. Establish security measures to ensure that suppliers of technology services and products comply with the security requirements set forth in this cybersecurity policy.
2. Conduct a risk assessment of suppliers to identify potential security risks and take preventive measures.

MONITORING AND DETECTION OF THREATS

1. Establish procedures for monitoring and detection of threats in the company.
2. Procedures must be reviewed and updated on a regular basis to ensure they remain effective and up to date.

PERSONAL DEVICES (BYOD)

1. The use of personal devices to access company systems, networks and resources is strictly prohibited.
2. All employees must use only corporate devices or those provided and managed by the company to access IT resources.

	General Cybersecurity Policy	CORPORATE POLICY
		Code: CS-PL-GE-01-2023-v02-00
		Approval Date: 2024/Mayo/30
- CONFIDENTIAL -	Version: 2. Revision: 1	Effectiveness: 2025/Mayo/30

PATCHES AND UPDATES

1. Establish a policy and procedures for managing patches and upgrades to enterprise systems.
2. Procedures must be reviewed and updated on a regular basis to ensure that they remain effective and up to date.

INFORMATION ENCRYPTION PROTOCOLS

1. Establish a policy and procedures for the company's confidential information encryption protocols.
2. Procedures must be reviewed and updated on a regular basis to ensure that they remain effective and up to date.

BUSINESS CONTINUITY AND DISASTER RECOVERY

1. Establish business continuity and disaster recovery plans to ensure the availability of the company's IT systems in the event of disruptions.
2. Plans must be reviewed on a regular basis to ensure that they remain effective and up to date.

IMPLEMENTATION

This cybersecurity policy must be communicated and distributed to all Vesta employees. In addition, a monitoring and oversight process must be created to ensure that all employees abide by the security requirements set forth in this policy.