Information Protection Policy

Cybersecurity Management
IT Research & Development Department

Mexico City, September 2023

CS-PL-IC-01-2023-v02-00

Tabla de contenido

OBJECTIVE

This Information Protection policy establishes guidelines and practices to ensure the confidentiality, integrity and availability of the information stored and processed in Vesta's computer systems. Its focus is the access controls, security measures and backups that must be established to protect the organization's critical information.

SCOPE

This policy applies to all employees, contractors and outside parties who work with the company's systems and assets.

ACCESS CONTROLS

Access controls must be established to ensure that confidential information is only accessible by authorized personnel.

Appropriate authentication measures, such as strong passwords and multifactor authentication, should be put in place to verify the identity of users.

Access rights should be assigned based on the principle of least privilege, which will be defined in the segregation of duties matrix that will be developed together with each area and the human resource department, ensuring that users have access only to the information required to carry out their job responsibilities.

A regular review of access rights will be conducted to ensure consistency with users' job responsibilities.

DATA INTEGRITY AND CONFIDENTIALITY

Security measures must be put in place to ensure the integrity and confidentiality of data stored in computer systems.

Encryption techniques should be used to protect sensitive data both in transit and at rest.

Computer systems and critical applications should be regularly patched and updated to mitigate vulnerabilities and maintain their integrity and security.

Data loss prevention (DLP) and security monitoring systems should be created to detect and prevent internal and external threats to data integrity and confidentiality.

RESPONSIBILITIES

The Cybersecurity team will be responsible for implementing and keeping the Information Protection policy up to date.

All employees, contractors and outside parties who work with company systems and assets, including information owners, are responsible for complying with the policies and procedures set forth in this policy. The active partnership of information owners is essential to ensure a comprehensive and effective approach to information security throughout the organization.

POLICY UPDATES

This policy will be reviewed and updated annually by the Cybersecurity team to ensure that it remains current with best practices and business needs.

Any changes to this policy will be communicated to all employees, contractors and third parties working with the company's systems.

All employees, contractors and outside parties are required to read and sign a statement of acceptance of the company's patch and update management policy prior to working with company systems.

EXCEPTIONS

In a cybersecurity policy focused on protecting information, exceptions are typically situations that require special treatment of data or a departure from standard rules to facilitate critical operations or meet legal obligations. Some possible exceptions could include:

1. Disclosure authorized by law:

Situations where the organization is legally obligated to disclose confidential or sensitive information, such as in response to subpoenas, court orders or government investigations.

2. Information sharing for partnership purposes:

Sharing of critical data with trusted partners, strategic allies or under inter-agency partnership agreements, where such sharing is vital to the organization's mission but is done under strict confidentiality agreements.

3. Exceptions for senior staff or specific roles:

Managers or employees in critical roles who may need broader access to information or the ability to share data more flexibly to make important strategic decisions.

4. Research and development:

Exceptions for R&D personnel working on innovative projects who may need access to protected information or the ability to use it in unconventional ways, always within a controlled framework.

5. Emergency access:

Emergency situations where it is necessary to access restricted information to solve urgent problems that affect the organization's operability or security.

6. Data transfer across borders:

In the context of global operations, international data transfer may require exceptions due to differences in data protection laws between countries, although users should always endeavor to comply with legal frameworks such the European Union GDPR.

7. Backup copies and archives:

Exceptions may be necessary for handling backups and archived data, which may require a different level of protection or be stored in locations not normally used for active data.

8. Use of data for training and testing:

Use of real data in test or training environments, where depersonalization of information would normally be required, but under certain controlled conditions the use of authentic data is permitted.

For each exception, it is crucial that there are clear procedures for application, approval and registration, ensuring that data are handled transparently and with the necessary safeguards to minimize risks. In addition, there should be regular review of exceptions to ensure their continued relevance and necessity.

CONCLUSION

This policy provides clear guidelines for protecting the organization's critical information, including the establishment of access controls, security measures, and backup practices. Information security is critical to Vesta and this policy ensures that it is appropriately protected. 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.