PiggyCo Cybersecurity Policy

Version: 1.0
Effective Date: 01/02/2025
Owner: CISO
Last Reviewed: 31/12/2024

1. Purpose

The purpose of this policy is to outline PiggyCo's commitment to protecting the confidentiality, integrity, and availability of its information assets from cybersecurity threats. This policy establishes the framework for managing and safeguarding digital information and ensures compliance with applicable laws, regulations, and standards.

2. Scope

This policy applies to all employees, contractors, partners, and third-party service providers who have access to PiggyCo's information systems and data. It covers all information assets, including hardware, software, networks, and data.

3. Policy Statements

3.1 Information Security Governance

3.1.1. PiggyCo will establish and maintain an information security governance framework to oversee the implementation and continuous improvement of cybersecurity measures.

3.1.2. The Executive Leadership team will appoint a Chief Information Security Officer (CISO) responsible for the overall security posture of the organization.

3.1.3. Regular security reviews and audits will be conducted to ensure compliance with this policy and identify areas for improvement.

3.2 Risk Management

3.2.1. A formal risk assessment process will be implemented to identify, assess, and mitigate cybersecurity risks.

3.2.2. Risk assessments will be conducted periodically and whenever significant changes to the information systems or business processes occur.

3.2.3. Risk treatment plans will be developed and monitored to address identified risks.

3.3 Access Control

3.3.1. Access to information systems and data will be granted based on the principle of least privilege, ensuring that individuals have the minimum access necessary to perform their job functions.

3.3.2. Strong authentication and authorization mechanisms, including multi-factor authentication (MFA), will be enforced.

3.3.3. User access rights will be reviewed regularly to ensure appropriate access levels are maintained.

3.4 Data Protection

3.4.1. Sensitive and confidential data will be protected through encryption, both in transit and at rest.

3.4.2. Data classification and handling procedures will be established to ensure proper protection based on data sensitivity.

3.4.3. Backup and recovery procedures will be implemented to ensure data availability in the event of a security incident or system failure.

3.5 Incident Response

3.5.1. An incident response plan will be developed and maintained to address cybersecurity incidents promptly and effectively.

3.5.2. All employees and stakeholders will be trained on their roles and responsibilities in the event of a security incident.

3.5.3. Security incidents will be logged, investigated, and reported to the appropriate authorities as required.

3.6 Training and Awareness

3.6.1. Regular cybersecurity training and awareness programs will be conducted to ensure all employees and stakeholders understand their responsibilities and best practices.

3.6.2. Phishing simulations and other awareness activities will be carried out to reinforce security awareness.

4. Compliance and Enforcement

Non-compliance with this policy may result in disciplinary actions, including termination of employment or contract.

The CISO will ensure that this policy is reviewed and updated regularly to reflect changes in the cybersecurity landscape and business requirements.

5. Policy Review

This policy will be reviewed annually and updated as necessary to ensure its continued relevance and effectiveness.4. Compliance & Enforcement

Violations of this policy may result in disciplinary actions, including termination or legal consequences.