Risk Management Policy Template , version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document Owner: Olumuyiwa Agunbiade
Last Review Date: October 2023

Risk Management Policy Template

Purpose

The purpose of the (Company Name) Risk Management Policy Template is to establish the requirements for the assessment and treatment of information security-related risks facing (Company Name) .

Audience

The (Company Name) Risk Management Policy Template applies to all (Company Name) individuals that are responsible for management, implementation, or treatment of risk activity.

Policy

- Formal organization-wide risk assessments will be conducted by (Company Name) no less than annually or upon significant changes to the (Company Name) environment.
- Risk assessments must account for administrative, physical, and technical risks.
- Information security risk management procedures must be developed and include the following (at a minimum):
    - Risk Assessment
    - Risk Treatment
    - Risk Communication
    - Risk Monitoring and Review
- Risk evaluation criteria should be developed for evaluating the organization's information security risks considering the following:
    - The strategic value of the business information process.
    - The criticality of the information assets involved.
    - Legal and regulatory requirements, and contractual obligations.
    - Operational and business importance of availability, confidentiality, and integrity.
    - Stakeholders' expectations and perceptions, and negative consequences for goodwill and reputation.
- All risks will be classified and prioritized according to their importance to the organization.
- Periodically, (Company Name) may contract with a third-party vendor to conduct an independent risk assessment and/or to validate the effectiveness of the (Company Name) risk management process.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 18
- NIST CSF: ID.GV, ID.RA, ID.RM, PR.IP

Waivers

Waivers from certain policy provisions may be sought following the (Company Name) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	October 2023		Olumuyiwa Agunbiade	Document Origination

Question & Answer?