Organizational Context Policy (GV.OC)

POLICY # CS-1	EFFECTIVE DATE March 1, 2024	APPROVED BY Insert Approver
VERSION # 2.0	LAST REVISED Insert Last Revised Date	REFERENCE NIST CSF: Organizational Context (GV.OC)

Purpose

This policy establishes a framework for aligning cybersecurity strategies and practices with the organization's mission, objectives, and business environment. It is designed to ensure that cybersecurity initiatives support and enhance the organization's operational effectiveness, stakeholder requirements, and compliance with relevant legal and regulatory standards.

Policy

Understanding the Organization's Mission and Objectives

The organization will conduct regular reviews to clearly define and document its mission, vision, and strategic objectives. Cybersecurity strategies will be developed to support and align with these objectives, ensuring they contribute positively to the organization's overall goals.

Recognizing the Business Environment

A thorough assessment of the organization's role within its industry, including its position in supply chains and critical infrastructure, will be conducted. The organization will maintain an up-to-date understanding of the broader business environment, including market trends, competition, and regulatory landscape.

Stakeholder Engagement

The organization will identify and engage with both internal and external stakeholders, including customers, partners, and regulatory bodies. Cybersecurity strategies will be developed in consideration of these stakeholders' expectations and requirements.

Alignment with Organizational Goals

Cybersecurity policies and practices will be aligned with business development strategies and operational objectives. The organization will ensure that cybersecurity decisions and initiatives are reflective of and contribute to achieving broader organizational goals.

Risk Management Integration

Cybersecurity risk management will be integrated into the overall enterprise risk management framework. Decisions regarding cybersecurity risks will be made in context with organizational objectives and risk tolerance.

Legal and Regulatory Compliance

The organization commits to compliance with all relevant laws, regulations, and standards. Regular updates and training will be provided to ensure that all staff are aware of these legal and regulatory requirements.

Adaptability to Change
The cybersecurity strategy will be regularly reviewed and adapted to reflect changes in the business environment, such as new technologies, emerging threats, and evolving industry standards.

Resource Allocation
Appropriate resources, including budget and personnel, will be allocated to support cybersecurity initiatives that align with the organizational context.

Continuous Improvement
Processes for continual learning and improvement will be established, based on feedback, audits, and assessments. This will include regular updates to the cybersecurity strategy and practices to ensure they remain effective and relevant.

Responsibilities

In addition to the responsibilities identified on page four (4), the ISO is responsible for conducting at least an annual review of the Organizational Context Policy, making any appropriate changes, and disseminating the updated policy to workforce members.

Related Form(s) and Evidence

- None

References

- NIST Cybersecurity Framework v2.0: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf