Cybersecurity Policy Framework Project – NovaSphere Technologies

By David Akinlalu

Overview

NovaSphere Technologies began modernizing its digital ecosystem by expanding cloud services, automating workflows, and increasing online offerings. These improvements brought gains in efficiency, but they also opened new exposure points. Internal reviews revealed inconsistent security practices and the absence of formal policies for access control, data protection, incident response, and vendor oversight.

NovaSphere created the role of Cybersecurity Risk Manager and tasked me with developing the company's first cybersecurity policy framework. This initiative aims to reduce operational risk, strengthen accountability, and align with standards such as NIST CSF, ISO 27001, and CIS controls.

Project Goals

1. Establish a clear cybersecurity governance structure.

2. Introduce enforceable security policies aligned with industry standards.

3. Create repeatable processes for protecting data and managing risk.

4. Strengthen organizational resilience and reduce exposure to common threats.

Solution Approach

1. Baseline Security Assessment

I evaluated NovaSphere's environment by reviewing cloud infrastructure, data flows, user access, monitoring capabilities, and third■party integrations. The assessment highlighted gaps such as inconsistent access approvals, lack of data classification, and ad■hoc incident handling.

2. Mapping Requirements to Industry Standards

I referenced NIST CSF, ISO 27001, and CIS Controls to shape the structure and expectations of the policy framework.

3. Four Foundational Policies

A. Data Protection & Classification Policy

- Data classification levels

- Handling and storage requirements

- Encryption standards

- Backup, retention, and disposal rules

B. Access Control Policy

- Role-based access control

- Multi-factor authentication

- Least-privilege enforcement

- Provisioning and deprovisioning workflows

- Quarterly access reviews

C. Incident Response Policy

- Incident severity levels

- Reporting and response steps

- Defined response roles

- Evidence handling

- Post-incident review process

D. Acceptable Use & Digital Behavior Policy

- Safe use of email, cloud apps, and messaging tools

- Restrictions on unauthorized software

- Phishing awareness expectations

- Device security for on-site and remote work

4. Governance & Accountability Structure

I introduced a Security Steering Committee, annual policy reviews, and clearly assigned responsibilities for monitoring, auditing, and enforcement.

Outcome

This policy framework gives NovaSphere a structured foundation for cybersecurity, improves visibility into risks, strengthens defenses against common threats, and prepares the company for future compliance obligations. These policies now support further initiatives such as vulnerability management, vendor risk reviews, and security awareness training.