Business Case: Establishing a Cybersecurity Policy Framework at NovaSphere Technologies

NovaSphere Technologies is in the middle of a company-wide effort to modernize its digital ecosystem. Over the past year, the organization has expanded its catalog of online services, automated several internal processes, and moved a significant portion of its infrastructure to the cloud. These changes have improved productivity, but they have also introduced new points of exposure that the company wasn't fully prepared to manage.

Recent internal assessments revealed gaps in how NovaSphere approaches cybersecurity. Daily operations rely on inconsistent security practices, and there are no formal policies to guide system access, data protection, incident handling, or expectations for third-party vendors. As NovaSphere continues to scale its digital operations, these gaps increase the risk of data loss, service disruption, regulatory complications, and reputational harm.

Leadership has agreed that a structured, enforceable security framework is essential to support the company's growth. Without it, NovaSphere faces a rising likelihood of threats such as phishing, unauthorized system access, and potential data breaches involving sensitive client information.

To tackle this, NovaSphere created the position of Cybersecurity Risk Manager and brought you onboard to lead the initiative. Your role is to design the company's first set of foundational security policies and ensure they align with recognized industry standards. These policies will form the backbone of a broader security program and help establish accountability, reduce operational risk, and prepare the organization for evolving compliance needs.

The first phase of this initiative focuses on developing four core policy documents. Together, they will define how NovaSphere protects its data, manages access, handles security incidents, and promotes safe use of digital technologies throughout the company.