**Purpose: To Develop and Implement a Comprehensive Cyber Strategy for Ensuring Robust Defense Against Cyber Threats**

In a digital era marked by continuous evolution and growing complexity, the necessity for an agile and robust cyber strategy transcends traditional security measures. The purpose of devising a cyber strategy and defense framework is multifaceted and includes:

1. **Understanding the Cyber Environment**: Mapping the organization's digital assets, technologies, and processes to understand what is at risk and where protection is needed.
2. **Assessing Threats and Vulnerabilities**: Conducting regular assessments to identify potential weaknesses and stay abreast of the ever-changing threat landscape.
3. **Designing a Layered Defense Approach**: Creating a multi-layered defense structure using firewalls, intrusion detection systems, encryption, and other security measures to provide a comprehensive protection net.
4. **Integrating Security Across the Organization**: Ensuring that cyber defense is not isolated but integrated into every aspect of the organization, from strategic planning to daily operations.
5. **Promoting a Security-Centric Culture**: Fostering a culture where security is everyone's responsibility, providing training, and encouraging vigilance.
6. **Ensuring Compliance with Regulatory Requirements**: Aligning the strategy with local, national, and international laws and standards to ensure legal compliance.
7. **Creating an Adaptive Incident Response Plan**: Crafting a plan that is not only reactive but can adapt to new types of incidents, ensuring a swift and effective response.
8. **Investing in Continuous Improvement and Innovation**: Committing to ongoing investment in security technologies, processes, and expertise, recognizing that cyber defense must evolve with the threat landscape.
9. **Building Trust with Stakeholders**: Demonstrating a strong commitment to cybersecurity, thereby building confidence with customers, suppliers, investors, and regulators.
10. **Supporting Strategic Business Goals**: Recognizing that a solid cyber defense strategy is not only about protection but supports the overall strategic goals and mission of the organization, enabling growth and innovation.

The overarching purpose is to create a resilient, adaptive, and holistic strategy that goes beyond mere defense, weaving cybersecurity into the fabric of the organization's culture, operations, and objectives. It's about leveraging cybersecurity as an enabler for business success, rather than simply a barrier against threats.