INFORMATION SECURITY POLICY

Date of Current Revision: XXXXXX, XXXX
Primary Responsible Officer: XXXXXXXXXXXXXXXXXXXXXX

PURPOSE

This information Security Policy establishes the framework for setting up an effective information security program at [Organization Name]. It defines the program, assigns responsibilities, demonstrates the strategic and tactical value of security, and outlines enforcement procedures to protect the confidentiality, integrity, and availability of our information assets.

SCOPE

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at [Organization Name], including all personnel affiliated with third parties. It covers all information assets, systems, networks, and data owned or managed by [Organization Name].

POLICY

Information Security Program

The organization must establish and maintain a comprehensive information security program, including policies, standards, procedures, and controls to protect the confidentiality, integrity, and availability of organizational assets. The program will be based on the Center for Internet Security (CIS) Controls version 8.1, focusing on Implementation Group (IG) 1 controls. This policy is the program's foundational document and permits the implementation and enforcement of the program based on the established roles and responsibilities.

Roles & Responsibilities

Senior Leadership. The senior leadership is responsible for providing strategic direction and support for the information security program. They must ensure that the necessary resources are allocated for the effective implementation and maintenance of the program. Additionally, they are required to review and approve the information security policy and any major updates.

Information Security Office/Officer (ISO). The responsibilities of the Information Security Officer/Office (ISO) include developing, implementing, and managing the information security program. The ISO conducts regular risk assessments and audits to identify and mitigate security risks, ensuring compliance with legal, regulatory, and contractual obligations. Additionally, The ISO reports on the status of the information security program to senior management.

IT Department. The IT Department is responsible for implementing controls as outlined in the security framework. They also maintain and monitor the security of information systems and networks while responding to security incidents and conducting root cause analysis when necessary.

Employees and Contractors. Employees and contractors must adhere to the information security policy and related procedures. They are also expected to participate in security awareness training programs. Additionally, they must immediately report any observed or suspected security incidents to the IT department.

Monitoring & Incident Response

To enforce this policy, the ISO will conduct regular audits and continuous monitoring to ensure compliance. In the event of a security incident, a structured incident response plan will be implemented promptly to address and mitigate the situation.

NON-COMPLIANCE AND DISCIPLINARY ACTIONS

Non-compliance with this policy will result in disciplinary action, which may include termination of employment, contract termination, and/or legal action, depending on the severity of the breach.

DOCUMENT ADMINISTRATION

Document Owner

This document is owned by the Organization's Information Security Office/Officer (ISO), which is responsible for its content and maintenance. For questions or comments, please email <contact email>.

Document Review

This document is subject to periodic review to validate the content remains relevant and up-to-date. Significant or material changes to this document must be submitted to the ISO for review and comment prior to adoption.

Change History

Version	Description	Author	Date
1.0	Initial publication		

Approval History

Version	Name	Title	Date
1.0			