Version: [01.00] Document No-IE/IEC/OC/0001
Reference Date-11/01/2024

SOA – 5.1

Information Security Policy

INNER EYE CONSULTANCY SERVICES LLP.

1. **Purpose:**
   The Management of information Security is the reasonable selection and effective implementation of appropriate controls to protect critical organizational information assets. Control and management process, coupled with the subsequent monitoring of their appropriateness, form the two primary elements of the Information Security program. The three goals of Information security includes:
   - Confidentiality
   - Integrity
   - Availability

   This Policy sets out the basis for the protection of information, facilitating security management decisions, and directing those objectives that establish, promote, and ensure the best Information Security controls and management within the Inner Eye Consultancy Services LLP working environment.

2. Scope:
   This Policy states broad management principles guiding the Information Security program in place within Inner Eye Consultancy Services LLP. This Policy applies to all physical areas under the control of the Organization. Where other specific functional policies set more stringent requirements, they take precedence in those functional areas. This Information Security Policy shall be reviewed by the System Officer at regular intervals to ensure its continuing suitability, adequacy, and effectiveness.

3. **Policy Framework:**

   3.1. Policy Ownership:
   The System Officer is responsible for the ownership and oversight of the Information Security Policy.

   3.2. Policy Development:
   The Information Security team, in collaboration with relevant stakeholders, is responsible for developing and updating the Information Security Policy.

   3.3. Approval Authority:
   The Information Security Policy requires initial approval from Manager System IT before Development.
   The Information Security Policy requires initial approval from the Managing Director before Deployment.

   3.4. Policy Distribution:

The IT team will ensure that the latest version of the Information Security Policy is accessible to all relevant personnel.

4. **Roles and Responsibilities:**
   Information security roles and responsibilities are defined in document no **IE/IEC/OC/002.**
5. **Policy Details:**
   5.1. Threat Intelligence:
   Threat intelligence is a proactive approach to cybersecurity that involves the collection, analysis, and dissemination of information about potential and current cyber threats. It provides organizations with insights into the tactics, techniques, and procedures (TTPs) employed by malicious actors, helping them anticipate and respond to cyber threats effectively.
   5.2. Network Security Management:
   Network security management refers to the process of implementing, monitoring, and maintaining security measures within a computer network to protect against unauthorized access, misuse, modification, or denial of network resources and data. It involves various practices, technologies, and policies aimed at safeguarding the integrity, confidentiality, and availability of network assets. This includes activities such as risk assessment, security policy development, access control, intrusion detection and prevention, encryption, regular audits, and incident response. Effective network security management is essential for organizations to mitigate cybersecurity threats and ensure the overall safety and reliability of their network infrastructure.
   5.3. Project Management:
   Project management is a systematic approach to planning, executing, monitoring, and closing projects efficiently and effectively. It involves coordinating resources, tasks, and timelines to achieve specific objectives within defined constraints such as time, budget, and scope.
   5.4. Asset Management:
   In Inner Eye Consultancy Services LLP, a comprehensive approach to information governance is established through several key policies. The Inventory of Information and Associated Assets Policy acts as the cornerstone, meticulously documenting and tracking valuable information and resources within the organization. This inventory forms the basis of Information Asset Management, aiding in an organization, protection, and strategic utilization of critical assets.
   Furthermore, the Acceptable Use of Information and Associated Assets Policy sets clear guidelines for the ethical and proper utilization of the organization's information resources. This policy ensures that employees, contractors, and stakeholders adhere to expectations that uphold the confidentiality, integrity, and availability of information assets.

Additionally, the organization enforces a Return of Assets Policy dictating procedures and expectations for the proper return of company-owned assets when an individual's association concludes. This policy facilitates the efficient recovery and safeguarding of valuable resources.

Safeguarding sensitive information is extended through the Protection of Records Policy, which establishes guidelines for securing the organization's records. This policy is vital for compliance with privacy regulations, effective risk management, and maintaining stakeholder trust.

Furthermore, the organization upholds responsible practices in Media Handling as outlined in the respective policy. This includes guidelines for secure management of storage media, both physical (such as USB drives, external hard disks) and digital platforms. The policy ensures the confidentiality, integrity, and availability of information stored on various media.

Finally, the organization maintains environmental responsibility in its Disposal and Reuse of Equipment Policy, setting guidelines for the secure handling of electronic equipment no longer in use. This policy ensures proper disposal of outdated equipment and outlines protocols for securely managing data on these devices.

Together, these policies create a robust framework for information management and security within Inner Eye Consultancy Services LLP.

5.5. Classification of information:

In Inner Eye Consultancy Services LLP, a comprehensive approach to information security is ensured through several key policies. The Classification of Information Policy serves as the foundation, outlining procedures and criteria for categorizing and safeguarding information based on its sensitivity, criticality, and confidentiality. This policy ensures that appropriate security measures are systematically applied, aligning with the importance of information assets to the organization.

Supplementing this is the Information Labeling Policy, providing guidelines for labeling and marking information assets to convey their classification, sensitivity, and handling requirements. By facilitating easy identification of confidentiality levels, this policy ensures that individuals handling information can apply the appropriate security measures.

Further reinforcing the organization's commitment to secure information management is the Information Transfer Policy. This policy establishes guidelines for the secure and controlled transfer of information within and outside the organization. It ensures efficient information exchange while prioritizing confidentiality, integrity, and compliance with relevant regulations.

Together, these policies create a robust framework that not only classifies and safeguards information based on its significance but also ensures clear

communication of its sensitivity and enables secure and controlled information transfer within Inner Eye Consultancy Services LLP.

5.6. Access Management:

At Inner Eye Consultancy Services LLP, a comprehensive information security framework is established through key policies. The Access Control Policy forms the bedrock, outlining procedures and principles governing access to systems, data, and facilities, ensuring a secure and controlled environment. Complementing this is the practice of Identity Management, a crucial aspect ensuring secure and efficient operations. This involves the management of digital identities, encompassing user authentication, authorization, and access control, ensuring only authorized individuals have access to specific resources.

In conjunction, the Authentication Information Policy plays a pivotal role, defining guidelines and procedures for user authentication, emphasizing the protection of sensitive data and the prevention of unauthorized access. This is reinforced by the Access Rights Policy, a fundamental component of information security, dictating principles and procedures for granting and managing access to various systems, data, and resources within the organization.

Together, these policies create a cohesive and robust information security framework, promoting a controlled and secure environment at Inner Eye Consultancy Services LLP.

5.7. Third Party Management:

To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

This document outlines the due diligence journey a third-party has to complete at Sourcegraph, including a baseline of security controls that Sourcegraph expects partners and other third-party companies to meet when interacting with Sourcegraph data.

5.10. Physical Information Management:

The purpose of this policy is to establish guidelines, procedures, and responsibilities for maintaining effective physical security measures to protect INNER EYE CONSULTANCY SERVICES LLP.'s assets, facilities, and personnel.This policy aims to mitigate risks associated with off-site work, business travel, and remote work arrangements.

5.11. **People Control Management:**

Addressing the 'human factor' in information security compliance requires action at two critical levels. Firstly, non-technical staff must understand their role in

preventing and mitigating cyber threats. A successful staff awareness program can help companies identify potential security vulnerabilities, increase employee awareness of the repercussions of inadequate information security, promote the uniform implementation of procedures, and foster better communication between different teams and levels of the organization. Secondly, every organisation requires skilled professionals with up-to-date technical expertise, competence, and qualifications to deliver an effective information security strategy. These experts must plan and execute more complex information and cyber security activities and ensure the continuous improvement of these protections. Inadequate skilled people resources can result in poor risk management and the implementation of ineffective cybersecurity controls. Additionally, an organisation's ability to respond to and recover from data breaches depends on the effective deployment of technical staff.

6. **Policy Development and Review Process:**

6.1. Policy Development:

The Information Security team will collaborate with relevant stakeholders to develop and update the Information Security Policy based on changes in technology, regulations, or business processes. SOA;- 5.35

6.2. Review Frequency:

The Information Security Policy will be reviewed at least annually or more frequently if significant changes in the organizational environment occur.

6.3. Approval Process:

Any proposed changes to the Information Security Policy will undergo review, approval, and formal authorization by [Executive Leadership/Board of Directors/Other Appropriate Authority].

7. **Communication and Training:**

7.1. Policy Communication:

The Information Security team is responsible for ensuring the timely and effective communication of the Information Security Policy to all employees.

7.2. Training Programs:

Regular training programs will be conducted to educate employees about the Information Security Policy, its importance, and the role each individual plays in its implementation.

8. **Compliance Monitoring:**

8.1. Monitoring and Reporting:

The Information Security team will conduct regular assessments to monitor compliance with the Information Security Policy and report findings to relevant stakeholders.

8.2. Non-Compliance Consequences:

Non-compliance with the Information Security Policy may result in disciplinary action, including but not limited to warnings, suspension, or termination.

9. **Review and Revision of Policy**:
   This policy will be reviewed annually and updated as necessary to reflect changes in technology, business processes, or regulatory requirements.

10. **Acknowledgment:**
    All employees, contractors, and relevant stakeholders are required to acknowledge receipt and understanding of this Organizational Control Policy for Information Security Policy.