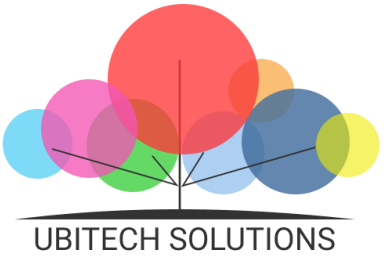

Ubitech

Information Security Roles and Responsibilities

Version 1.0

PURPOSE

This document defines and establishes the information security roles and responsibilities within the Information Security Management System (ISMS) of Ubitech Solutions Pvt. Ltd. (hereby referred to as the organization). This ensures a clear understanding of each role's duties in maintaining the confidentiality, integrity, and availability of the Organization's information assets.

SCOPE

This document applies to the organization's Information Security Management System (ISMS). It encompasses all roles and responsibilities related to information security across the organization, including employees, contractors, and third-party partners involved in handling the Organization's information assets.

DEFINITION

1. ISMS: Information Security Management System Information Security: Confidentiality, Integrity, Availability of the information
2. ISMS: Information Security Management System
3. ISG: Information Security Group
4. LT: Leadership Team
5. CEO: Chief Executive Officer
6. CTO: Chief Technology Officer
7. CFO: Chief Financial Officer
8. C IS O: Chief Information Security Officer
9. IT: Information Technology

INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Top Management

Leadership Team (LT), comprising the CEO, CTO, CFO, and CISO, serves as the organization's top management for the ISMS. The Leadership Team is responsible for:

1. **Approval and Authorization:**
    a. Approving and authorizing the implementation and operation of the ISMS program.
    b. Establishing and approving ISMS policies.
    c. Approving the ISMS scope and boundaries.
2. **Strategic Oversight:**
    a. Ensuring that ISMS objectives and plans are established and aligned with the organization's strategic direction.
    b. Translating the business's strategic direction into specific information security directives for the ISG.

c. Ensuring that ISMS requirements are integrated into organizational processes.

3. **Risk Management:**
    a. Defining the risk assessment methodology.
    b. Approving criteria for accepting risks and determining acceptable risk levels.
    c. Approving residual risks, risk assessment reports, and risk treatment plans.
4. **Resource Allocation:**
    a. Providing sufficient resources to establish, implement, operate, monitor, review, maintain, and improve the ISMS program.
5. **Compliance and Improvement:**
    a. Ensuring compliance with internal ISMS audits.
    b. Presiding over management reviews of the ISMS.
    c. Promoting continual improvement within the ISMS framework.
6. **Advocacy:**
    a. Championing the cause of information security and its objectives within the organization.

Chief Information Security Officer (CISO)

The **Chief Information Security Officer (CISO)** is responsible for:

1. **ISMS Implementation:**
    a. Ensuring the implementation and integration of ISMS program requirements into the organization’s processes.
    b. Overseeing the effectiveness of the ISMS to achieve its intended outcomes.
2. **Leadership and Support:**
    a. Directing and supporting personnel to contribute to the effectiveness of the ISMS.
    b. Overseeing the Information Security Group (ISG).
    c. Supporting other management roles to demonstrate leadership in information security within their areas of responsibility.
3. **Policy and Risk Management:**
    a. Approving all information security policies, procedures, and plans.
    b. Identifying potential and actual information security risks.
    c. Establishing risk acceptance criteria and criteria for performing information security risk assessments.
    d. Ensuring consistent, valid, and comparable results from repeated information security risk assessments.
    e. Analyzing and evaluating information security risks concerning confidentiality, integrity, availability, and data privacy.
    f. Selecting appropriate risk treatment options based on assessment results.
    g. Determining necessary controls to implement chosen risk treatment options.
    h. Comparing requirements with ISO 27001 and verifying that no necessary controls are omitted.
    i. Identifying risk owners and obtaining their approval of risk treatment plans.

j. Ensuring compliance with all applicable legal requirements and information security standards (e.g., ISO 27001, SOC 2, GDPR).
k. Ensuring compliance with the vendor management process.

DevOps Head/CTO

The **DevOps Head/CTO** is responsible for:

1. **Policy Adherence:**
    a. Ensuring all personnel in the guild adhere to ISMS policies and procedures.
2. **Resource Provision:**
    a. Providing guild resources to assist with ISMS risk assessments.
3. **Risk Management:**
    a. Reviewing and approving guild-level risks and activities.
    b. Assigning responsibilities for implementing actions and setting timelines for completion.
4. **Coordination and Compliance:**
    a. Coordinating with the CISO to understand requirements for implementing technical and organizational measures or controls.
    b. Conducting periodic access control reviews for all information assets and systems owned by the guild.
    c. Ensure the timely reporting of information security events or incidents to the CISO and cooperate with the ISG to mitigate and resolve such events or incidents.
    d. Monitoring and measuring the effectiveness of guild-related ISMS requirements.
    e. Evaluating information security controls and their effectiveness within the guild.

ISG

The **Information Security Group (ISG)** comprises an Information Security Manager, IT Head, HR Head, DevOps Head/CTO, and Admin Head. The ISG is responsible for:

1. **Asset Management:**
    a. Monitoring and collecting necessary inputs from asset owners to build an asset inventory.
2. **Risk Assessment and Treatment:**
    a. Conducting risk assessments for information security and personal data protection.
    b. Formulating risk treatment plans.
3. **Policy Development:**
    a. Drafting information security policies, procedures, and plans.
4. **Support and Coordination:**
    a. Assisting various process owners across the organization in implementing controls.
    b. Coordinating with the CISO to implement technical and organizational measures and controls.
5. **Monitoring and Reporting:**
    a. Monitoring the effectiveness of implemented measures and controls.

b. Reporting to the CISO on the efficacy of the ISMS program.

6. **Access Control and Security:**
    a. Ensuring minimum security requirements are implemented in all ISMS policies and procedures.
    b. Determining access control processes for applications and data.
    c. Ensuring the secure administration and operation of the organization's applications and data.

Internal Auditors

Internal Auditors trained in ISO 27001:2022 are responsible for:

1. **Audit Planning and Execution:**
    a. Planning internal audits based on the ISMS program, including scope and boundaries.
    b. Conducting internal audits and finalizing audit plans.
    c. Conducting opening meetings before audit initiation.
2. **Reporting and Remediation:**
    a. Reporting audit findings to the CISO and Top Management.
    b. Reviewing remediation efforts by guilds and process owners in response to audit findings.
    c. Verifying the implementation and effectiveness of corrective actions.
3. **Audit Management:**
    a. Monitoring and managing the internal audit plan.
    b. Discuss findings and observations to reach a consensus.
    c. Collating and finalizing the internal audit report.
    d. Submitting reports to the CISO and Top Management.

Employees, Contractors, and Third Parties
All **employees, contractors, and third parties** of the Organization are responsible for:

1. **ISMS Participation:**
    a. Effectively implement the ISMS program and ensure compliance with it.
    b. Contributing to risk assessments, where applicable.
    c. Understanding their roles and responsibilities in the ISMS program through training.
2. **Policy Adherence:**
    a. Adhering to and following ISMS policies and procedures enacted by the Organization.
3. **Security Measures:**
    a. Participating in and contributing to implementing technical and organizational measures required for information security.
4. **Reporting:**
    a. Reporting risks and weaknesses to guild leaders, the CISO, or the ISG.
    b. Reporting any information security events or incidents to the relevant guild leader, the CISO, or the ISG.

5. **Objective Achievement:**
    a. Contributing towards the achievement of information security objectives and goals.
    b. Assisting in remediating issues arising from audits.

Chief Financial Officer (CFO)

The **Chief Financial Officer (CFO)** manages the organization's financial actions, including budgeting, forecasting, and planning. The CFO also has specific responsibilities related to information security.
Responsibilities:

1. **Financial Oversight:**
    a. Allocate and manage budgets for information security initiatives and the ISMS program.
    b. Ensure financial resources are available for implementing and maintaining security controls.
2. **Risk Management:**
    a. Collaborate with the CISO and ISG to understand financial risks associated with information security breaches.
    b. Approve financial risk treatment plans related to information security.
3. **Compliance and Reporting:**
    a. Ensure compliance with financial regulations that intersect with information security requirements (e.g., Sarbanes-Oxley Act).
    b. Oversee financial reporting related to information security investments and incidents.
4. **Cost-Benefit Analysis:**
    a. Conduct cost-benefit analyses for proposed information security measures to ensure financial viability and effectiveness.

Chief Human Resources Officer (CHRO)
The **Chief Human Resources Officer (CHRO)** is responsible for managing the organization's human resources functions, ensuring that employees and contractors are qualified, competent, and well-informed about their roles in information security.
Responsibilities:

1. **Employee Qualification and Competence:**
    a. Ensure all employees and contractors are qualified and competent for their respective organizational roles.
2. **Testing and Background Checks:**
    a. Oversee the completion of appropriate testing and background checks for all personnel to verify their suitability and reliability.
3. **Policy and Code of Conduct:**
    a. Ensure all personnel and relevant contractors have company policies and the Code of Conduct (CoC).
    b. Facilitate the dissemination and understanding of these policies to all employees and contractors.
4. **Performance and Compliance Evaluation:**

a. Periodically evaluate employee performance and adherence to the CoC to ensure ongoing compliance with information security standards.

5. **Security Training:**
    a. Ensure all personnel receive appropriate security training tailored to their roles and responsibilities.
    b. Coordinate with the ISG to develop and implement training programs that address current and emerging information security threats.
6. **Employee Onboarding and Offboarding:**
    a. Manage secure onboarding and offboarding processes to ensure access to information assets is appropriately granted and revoked.
7. **Incident Response Support:**
    a. Collaborate with the ISG and CISO to address human-related aspects of information security incidents, including employee involvement and compliance.
8. **Cultivating Security Culture:**
    a. Promote a culture of security awareness and responsibility throughout the organization.
    b. Encourage employees to report security concerns and participate in maintaining the organization’s security posture.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 26 2025	Initial Release	Scrut Team	Parth Bhansali	Aditya Goyal