**ISMS COMMITTEE CHARTER**

**Document Control**

|  |  |
| --- | --- |
| **Title** | **ISMS Committee Charter** |
| **Author** |  |
| **Date Reviewed** |  |
| **Date Approved** |  |
| **Approved By** |  |
| **Classification** | Internal |
| **Version** | 1.0 |

**Record of Change**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Name** | **Date** | **Reviewed by** | **Changes** |
|  |  |  |  |

**Approval List**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Signature | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

Contents

[1. CHARTER 4](#_Toc169651576)

[2. MANDATE 4](#_Toc169651577)

[3. PURPOSE 4](#_Toc169651578)

[4. MEMBERSHIP STRUCTURE 4](#_Toc169651579)

[4.1. MEMBERSHIP 4](#_Toc169651580)

[5.1. RESPONSIBILITIES 5](#_Toc169651581)

[6. GOVERNANCE INVOLVEMENT 5](#_Toc169651582)

[7. COMMUNICATION 5](#_Toc169651583)

[8.1 MEETING SCHEDULE 6](#_Toc169651584)

[8.2 DECISION MODEL 6](#_Toc169651585)

[8.3 MEETING AGENDA 6](#_Toc169651586)

[8.4 ATTENDANCE 6](#_Toc169651587)

[8.5 WORK GROUPS AND AD HOC TEAMS – ISMS WORKING GROUP 7](#_Toc169651588)

1. CHARTER

The Information Security Management System Committee is a formal ISMS (Information Security Management System) Committee of [XXXX] Company. This charter describes its operations.

1. MANDATE

The Information Security Management Team will lead the creation of the security framework with review, maintenance, education, and awareness of information security policy, procedures, and standards based on the principles of ISO 27001. The efforts of the ISMS Team will work to address security governance, security risk management, exception management, data classification, technical security standards, and a strategy for certification to security frameworks within the Organization.

1. PURPOSE

The purpose of the Information Security Management System Committee is to help establish, coordinate and communicate an Information Security Framework for the Organization with review, maintenance and awareness of information security policy, procedures, and standards based on the principles of the ISO 27001.

1. MEMBERSHIP STRUCTURE
2. CEO
3. COO
4. Head of Technology
5. Chief Information Security Officer
6. The ISMS Manager

4.1. MEMBERSHIP

Members should strongly represent their respective interests resulting in helping shape and define security practices within the Organization. Members are encouraged to attend quarterly Information Security Committee Meetings and be willing to fully participate possible.

1. **RESPONSIBILITY AND INDIVIDUAL ACCOUNTABILITY**

The committee will strive to foster openness, active discussions, and willingness to share information. While members are expected to represent the viewpoints and the goals of their respective jurisdictions, they will be expected to take a broader view towards the entire needs of the Organization, not just their own departments, units or jurisdictions. It is essential that the committee work closely with the rest of the [XXXX- Company] community to ensure that all policies and objectives reflect the priorities of the Organization as an institution and are consistent with [XXXX] Company’s organizational or enterprise culture.

Most discussions will be facilitated by appropriate roles to ensure directed conversations and that all members can participate and be heard. The planning of meetings (time, location, agenda, format, etc) are determined by the committee. The participation in the Information Security Management System Committee is mandatory for various affected stakeholders representing their respective interests.

5.1. RESPONSIBILITIES

1. Ratify goals for [XXXX] Company’s enterprise-wide information security program
2. Facilitate the development and review of system-wide information security policies, procedures and guidelines
3. Recommend, review and prioritize information security projects and initiatives in alignment with IT (Information Technology) Governance Review Board or other High-Level Board playing this role.
4. Communicate and facilitate information security needs and sound practices among [XXXX] Company’s departments, IT Steering Committee and other IT initiatives and projects.

5. Review the performance and effectiveness of the information security program.

1. GOVERNANCE INVOLVEMENT

The Information Security Management System Committee will report results to the CEO/Executive Management members of [XXXX] Company.

1. COMMUNICATION

Primary communication for the Information Security Management System Committee will be through internal emails and memos.

Meeting notes and action items will be documented at each committee meeting. Following each meeting, the *administrative support* staff will electronically distribute the documents to the co‐chairs for review. The resulting document, and other materials, will be electronically distributed to the committee members prior to the next meeting.

During the next meeting, the documents will be approved. Once approved, the documents will be posted to the committee website or portal (*if any – not compulsory*).

The committee charter, meeting schedules, membership roster, and other documents will also be posted to the committee website (*if any – not compulsory*).

1. **MEETINGS**
   1. MEETING SCHEDULE

Meetings will be held once every quarter

* 1. DECISION MODEL

Decisions will be generally made through member consensus. Disputes will be resolved by the Executive Director of Risk and Control.

* 1. MEETING AGENDA

An agenda will be drafted by the committee co‐chairs with consultation from committee members, staff, and other stakeholders. The draft agenda will be distributed to committee members on the Friday preceding the meeting. Feedback will be incorporated into the final draft agenda which will be presented for adoption at the committee meeting.

* 1. ATTENDANCE

All members of this committee are expected to actively participate. Regular attendance for meetings as well as involvement in special activities is important to satisfy the many responsibilities of this committee. Members are expected to RSVP to meeting notices.

Due to the nature of the committee work, member consistency is critical. If members are unable to attend, a proxy must be assigned.

Committee members may invite additional attendees to participate as appropriate.

* 1. WORK GROUPS AND AD HOC TEAMS – ISMS WORKING GROUP

From time to time the committee may need to involve additional expert resources beyond the committee membership. The co‐chairs may designate ad hoc teams to conduct specific work and report back to the committee. Ad hoc teams may include non‐committee members that are subject matter experts.

The ad hoc teams will be resourced under the platform of the ISMS Working Group. The ISMS Working Group will be formed of individuals with expert working knowledge who execute tactical IT and information security related activities.

One committee co‐chair will be selected to provide leadership and direction to the ad hoc team(s) – that is the ISMS Working Group – while performing normal ISMS Committee assignment(s)