|  |
| --- |
| INTERNATIONAL SOCIETY FOR KRISHNA CONSCIOUSNESS, BANGALORE  ISKCON Bangalore |
| ISMS Policy |
| **POLICY / IT-001** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | **Document Reference** | **POLICY / IT-001** | **Version No.** | **1.0** | | **Document Title** | **Information Security Management System (ISMS) Policy** | | | | **Effective Date** | **January 1, 2014** | | | | **Next Review Date** |  | | |  |  |  |  |  | | --- | --- | --- | --- | |  | **Prepared By** | **Reviewed By** | **Approved By** | | **Name** | **Janaki Vallabha Dasa** | **Amitasana Dasa** | **Amitasana Dasa** | | **Designation** | **Service Line Head - IT** | **Vice President** | **Vice President** | | **Date** |  |  |  | | **Signature** |  |  |  | |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Released On** | **Revision Details** | **Approved By** |
| 1.0 | January 1, 2013 | Initial Version | Amitasana Dasa,  Vice President, ISKCON |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

## Purpose

The purpose of the Information Security Management System Policy is to ensure adequate and proportionate security controls that protect the information assets of the organization and give confidence to the interested parties.

The ISMS policy is a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security of the organization. The policy adopts the ISO/IEC 27001:2005 standard and the guidelines as set forth in ISO/IEC 27002:2005.

## Objectives

The objectives of the information security policy are:

1. To protect the information assets of the organization
2. To protect the personal and sensitive information of donors and business partners
3. To ensure compliance with all legislative, regulatory and contractual requirements connected to information security at all times
4. To maintain consistency in the protection of the confidentiality, integrity and availability of information across the organization.

## Scope

The scope of the ISMS covers the following:

* IT Infrastructure
* Information Security
* Physical Security
* Personnel (how it is related to ISMS)

The IT team will have the total ownership of all the IT assets and the information contained in them.

## Interpretation

Any matter not specifically covered under this policy shall be referred to Division Head - IT for necessary clarification. The interpretation of this policy rests exclusively with the Management. The decision of the Management shall be final and binding.

## Effective Date

The policy & procedures outlined in this document shall supersede all other earlier guidelines / rules / policies / procedures on this subject matter & shall come into force with effect from January 01, 2014.

## References

ISO/IEC 27001:2005 Information Security Management Systems - Requirements

ISO/IEC 27002:2005 Code of Practice for Information Security Management

# Terms and Definitions

**asset:** anything that has value to the organization

**availability:** the property of being accessible and usable upon demand by authorized entity

**confidentiality:** the property that information is not made available or disclosed to unauthorized individuals, entities or processes

**integrity:** the property of safeguarding the accuracy and completeness of assets

**information security:** preservation of confidentiality, integrity and availability of information; other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

**information security event:** an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

**information security incident:** a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

**threat:** a potential cause of an unwanted incident, which may result in harm to a system or organization

**vulnerability:** a weakness of an asset or group of assets that can be exploited by one or more threats

**risk:** effect of uncertainty on objectives; combination of the probability of an event and its consequence

**risk analysis:** systematic use of information to identify sources and to estimate the risk

**risk evaluation:** process of comparing the estimate risk against given risk criteria to determine the significance of the risk

**risk assessment:** overall process of risk analysis and risk evaluation

**risk management:** coordinated activities to direct and control an organization with regard to risk

**risk treatment:** process of selection and implementation of measures to modify risk

**residual risk:** the risk remaining after risk treatment

**statement of applicability:** documented statement describing the control objectives and control that are relevant and applicable to the organization’s ISMS

# Management Framework for ISMS

The ISMS Policy of ISKCON is approved by the management, and published and communicated to all the employees and related parties. It is the responsibility of Information Security Committee of ISKCON to establish, implement, operate, monitor, review, maintain and improve the documented ISMS within the context of the organization’s overall business activities and the risks faced by the organization.

## Information Security Committee & ISMS Org Chart

The Information Security Committee of ISKCON is headed by Sri Amitasana Dasa, Vice President and assisted by Janaki Vallabha Dasa, Division Head – IT and Ayyappa Dasika, Manager – IT. The committee shall also have nominated department heads who have been assigned the responsibility of (a) managing the information security of their departments (b) escalate any security incidents and (c) suggest improvements during the monthly review meetings.

## Monthly Review Meetings

Define the objective, primary agenda, frequency of above committees in a structured format.

The Information Security Committee shall conduct monthly review meetings in order to

* Assess the effectiveness of the ISMS
* Review of ISMS policy, objectives and security controls
* Measure the effectiveness of the controls to verify that security requirements have been met
* Review the risk assessments, the identified risks and acceptable level of risks at planned intervals in the light of change in organization structure, business objectives or processes
* Review the internal audit reports and findings
* Identify and approve corrective and preventive actions to improve the ISMS
* Follow up the corrective and preventive actions taken
* Discuss any major security incident that has happened in the earlier period and take appropriate measures

## Disciplinary Action

Escalation mechanism and reference to disciplinary procedure.

In extraordinary circumstances, if any employee is found to be compromising the information security of the organization, he/she shall face strict action as per the disciplinary procedure of the organization, and can even be terminated.

# Requirements

## Risk Assessment

A well-defined risk assessment methodology shall be developed based on the information security requirements of the organization, legal and regulatory requirements and contractual obligations. The criteria for accepting risks and identify the acceptable levels of risk shall be developed.

All information assets of the organization shall be identified and classified based on a documented procedure for asset classification based on their criticality and sensitivity. A master list of the information asset shall be documented with its location and designated owner. For easier identification and manageability all the assets shall be labeled.

The risk assessment shall identify a) the threats to these information assets b) the vulnerabilities that might be exploited by the threats c) the impact created by failure. The risk assessment shall also analyze and evaluate the risks based on the probability (likelihood of security failures) and the consequences (impact upon the organization that might result from security failures)

A risk treatment plan shall be prepared to identify and evaluate the possible options to mitigate, transfer, avoid or manage the risks. For example, the risk can be mitigated by reducing the impact by applying appropriate controls; or can be transferred to other parties (ex: insurers)

A statement of applicability of relevant control objectives and controls shall be documented and the various technical and procedural controls shall be implemented to control the risks.

**Related Documents:** Procedure for Asset Classification, Risk Assessment Methodology, Risk Assessment Report, Risk Treatment Plan, Statement of Applicability

## **Control of Documents**

A document control procedure shall be established to

* approve documents for adequacy prior to issue
* review and update documents as necessary and re-approve documents
* ensure that changes and the current revision status of documents are identified
* ensure that relevant versions of applicable documents are available at points of use
* ensure that documents remain legible and readily identifiable
* ensure that documents are available to those who need them, and are transferred, stored, and ultimately disposed of in accordance with the procedures applicable to their classification
* ensure that documents of external origin are identified
* ensure that distribution of documents is controlled
* prevent the unintended use of obsolete documents and
* apply suitable identification to them if they are retained for any purpose

## Control of **Records**

A documented procedure for control of records shall be established to

* ensure that records are maintained to provide evidence of conformity to requirements and the effective operation of the ISMS.
* ensure that records are protected and controlled
* ensure that the records remain legible, readily identifiable and retrievable
* define the retention period for the records and procedure for disposition of the records

## Management Responsibility

The management of ISKCON is committed to establishing, maintaining and improving the information security of the organization and in order to do so, agrees to provide sufficient resources in the form of skilled personnel, financial budget and management involvement needed to establish, implement, operate, monitor, review, maintain and improve the ISMS. The management will continually assess the competence of the personnel deployed in order to manage the ISMS effectively and provide required training to achieve the ISMS objectives.

## Internal ISMS Audits

The management shall ensure that internal ISMS audits are conducted once in 6 months to determine whether the control objectives, controls, processes and procedures of its ISMS are performing as expected and conform to the identified information security requirements. A documented procedure shall be prepared to define the responsibilities and requirements for planning and conducting audits and for reporting results and maintaining records.

## Management Review of the ISMS

The management will review the ISMS once in 3 months to

1. ensure its continuing suitability, adequacy and effectiveness and
2. assess opportunities for improvement and the need for changes to the ISMS

The results of the reviews shall be clearly documented and records shall be maintained as per the record control procedure.

|  |  |
| --- | --- |
| **Inputs for Management Review** | **Outputs of Management Review** |
| Results of ISMS audits and reviews  Feedback from interested parties  Status of Preventive and Corrective Actions  Results from effectiveness measurements  Follow up actions from previous reviews  Recommendations for Improvement  Any changes that could affect ISMS  Risk Assessment and Risk Treatment Plan | Improvement of the effectiveness of ISMS  Updates to risk assessment and risk treatment  Modification of procedures and controls  Resource needs  Improvements to control measures |

## Continual Improvement

The management of ISKCON is committed to continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

A documented procedure shall be prepared to define the procedure for determining and implementing the corrective actions required to eliminate the cause of any nonconformities identified by audits and for recording the results of the action taken.

A documented procedure shall be prepared to define the requirements for identifying potential nonconformities and take preventive action. The procedure shall define the requirements for recording the results of the action taken and reviewing of the preventive action taken.

**List of Documented Procedures:** Procedure for Control of Documents, Procedure for Control of Records, Procedure for ISMS Audit, Procedure for Corrective Action, Procedure for Preventive Action

# Information Security Policy

## Asset Identification and Classification Policy

## Acceptable Usage Policy

## Password Management Policy

## Email Security Policy

## Internet Usage Policy

## Information Backup Policy

## User Access Management Policy

## Information Exchange Policy (to exchange information with external parties)

## Clear Desk Clear Screen Policy

## Physical and Environmental Security Policy

## Network Access Control Policy

* I don’t think this set is complete. What about policy like “information category policy”, “Outsourcing Security Policy”, “Change Management and Control Policy”
* Information assets inventory
* JD of Chief Information Security Officer
* Information classification matrix and handling guidelines

Assign number for each policy document, as above. It is easy to refer them using number.