Punjab State Power Corporation Limited (PSPCL)

Information Security Management System

Manual

DOCUMENT CONTROL

Document Name: ISMS Manual

ID Reference: PSPCL/IT/ISMS/ISMS Manual

Prepared by	First Level Reviewed by	Second Level Reviewed by	Authorized by
Information Security Management Team (ISMT)	**Information Security Manager**	**Management Representative**	**Information Security Council (ISC)**
Signature:	Signature:	Signature:	Signature:
Version: 1.3	Version: 1.3	Version: 1.3	Version: 1.3
Date : 22.06.2022	Date : 22.06.2022	Date : 22.06.2022	Date : 22.06.2022

Security Classification: Internal Use

Table of Contents

INTRODUCTION 4
CONTEXT OF THE ORGANIZATION 4
LEADERSHIP 9
PLANNING 14
SUPPORT 15
PERFORMANCE EVALUATION 18
IMPROVEMENTS 19
ANNEXURES 20

INTRODUCTION

Erstwhile PSEB was a statutory body formed on February 1, 1959 under the Electricity Supply Act, 1948. Unbundling or restructuring of state electricity utility became necessary after the Electricity Supply Act, 1948 was replaced by the Electricity Act, 2003 based on which PSEB unbundled into 2 corporations; Punjab State Power Corporation Limited (PSPCL) and Punjab State Transmission Corporation Limited (PSTCL). PSPCL came into force on 16-4-2010 and was entrusted with the responsibility of generation and distribution of power.

PSPCL also implemented R-APDRP project which has been initialized in 2008. The project covers 47 no. towns across Punjab under Part-A scheme. Data Center (DC) and Data Recovery Center (DRC) have been maintained to centrally control all the key features of project. ISMS activities shall cover the DC, DRC site and Head Office IT department.

▪ Abbreviations

PSPCL	Punjab State Power Corporation Limited
CISO	Chief Information Security Officer
DC	Data Center
DR	Data Recovery
MR	Management Representative
ISC	Information Security Council
ISMT	Information Security Management Team

▪ Document Distribution and Review

This ISMS Manual shall be reviewed once in every year and in case of any major changes in the organization or its processes as and when necessary.

This document shall be accessible to all employees of PSPCL, and shall be shared with external stakeholders as and when necessary with post approval.

CONTEXT OF THE ORGANIZATION

PSPCL firmly believes that technology is one of the key enablers for enabling power distribution. For PSPCL, technology is an investment that is adding value to what and how we offer power distribution solutions to our members. The systems designed and deployed at PSPCL have enabled the business to grow rapidly as it's to use, saves time, is accurate and allows for data highlights to be transferred to head office when needed.

Information and communication technologies are an important part of daily routine for production and support staff. It oversees the functioning of a robust IT infrastructure and other services. The department's main task is to maintain and take care of the constantly developing information technologies, follow modern trends and respond to current challenges, so it can provide quality support for organization processes. In a relatively small team of people, and in close cooperation with the various departments, our IT team is trying to ensure that everything runs smoothly without any problems.

The **Restructured Accelerated Power Development and Reforms Programme (R-APDRP)** started in 2008 is a revised version of the Accelerated Power Development Reforms Programme (APDRP). The APDRP scheme was initiated in 2002-03 as Additional Central Assistance to States for reducing the Aggregate Technical and Commercial (AT&C) losses in the power sector *[Aggregate Technical and Commercial Loss captures the total loss in the distribution network. Technical loss may be due to ill maintained equipment, substations and inadequate investment in infrastructure while commercial loss may be due to low metering efficiency, faulty meter reading, theft and pilferages]* and improving the quality and reliability of power supply. This was to be achieved by strengthening and upgrading the sub-transmission and distribution system of high density load centers like towns and industrial centers.

R-APDRP is for urban areas- towns and cities with population of more than 30,000 (10,000 in case of special category states). The focus of R-APDRP is on actual, demonstrable performance in terms of sustained loss reduction. This is proposed to be achieved in two parts - Part A of the scheme envisages establishment of base line data which includes consumer indexing, GIS mapping and metering of distribution transformers and feeders and SCADA/DMS (Supervisory Control and Data Acquisition System/Data Management System) in project areas having a population of 4 lakh and annual input energy of 350 MU. This part of the scheme also includes IT applications for energy accounting/auditing and IT based consumer service. Part B of the scheme is for renovation, modernization and strengthening of distribution systems.

The IT Department is thus committed to the successful implementation of the R-APDRP project for PSPCL and is vital to the organization context towards the external world.

▪ Understanding the Organization and its context

PSPCL shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

Refer Annexure A for Organizational Context

Uncertainty Factors

With respect to PSPCL, there are several internal and external factors that are reverent to the purpose and may create uncertainty leading to risk.

Internal Uncertainty factors:

- Capital investments
- Delay in operationalization of production facilities
- Skill Shortage Risk
- Financial Condition of the organization
- Risks related to information technology (e.g. unauthorized access, malicious code, Unavailability of systems etc.)
- Employee relationship
- Change in Organization structure
- Change in location (Office relocation from one place to another)
- Connectivity issues

External Uncertainty factors:

- Changes in Applicable legal and Regulatory for Power Distribution Companies.
- Variations in Customer demand (With respect to Demand and Supply requirements of customer)
- Performance of the competitor
- Industry specific issues
- Supplier Services Delivery, Political unrest in locations where the business unit operates
- Community relations

In addition to the above uncertainty factors, the various ISMS related Risks (both Internal and External) have been identified in the Risk Assessment as threats and vulnerabilities and a Risk Treatment Plan is prepared.

Refer PSPCL Risk Assessment

▪ Understanding the needs and expectations of interested parties

Interested Parties

Interested parties can be “a person/s or organization/s that can affect the information security, or person/s or organization/s that can be affected by the information security activities or decisions”.

Interested parties that are relevant to PSPCL ISMS:
Shareholders (State Govt. of Punjab)
Employees
Board of directors
Customers
Suppliers
MoP, Govt. of India
PFC
NTPC
CEA (Central Electricity Authority)

NHPC
NCIIPC
Media
Local Government

Refer Annexure B for Interested Parties

Stakeholders can further be classified as ***Internal Stakeholders*** and ***External Stakeholders***.

Internal Stakeholders

Internal stakeholders are people, already committed to serve the organization as board members, employees, Shareholders/ Investors of the business.

External Stakeholders

External stakeholders are individuals, groups, and organizations that are not directly affected by the business's performance. These parties are not directly involved in decision making and other business affairs and, therefore, may or may not be affected by the company's decisions or operations. External stakeholders include government entities, media, NGO.

▪ Purpose & Scope of the Information Security Management System

Purpose of ISMS

The purpose of the ISMS is to:

1. Understand the organization's need and necessity of establishing the Information Security Management System
2. Implement and operate controls and measures for managing the organization's overall capability to manage information security incidents
3. Monitor and measure the effectiveness of the ISMS
4. Continually improve the organizations information security based on objective measurement

Scope of ISMS

ISMS at PSPCL applies to development of in house software applications, IT Hardware procurement, IT support to Data Center operations at Patiala and DR Site at Jalandhar.
This is in accordance with the Statement of Applicability Version 1.3 dated <22-June-2022>

Refer Annexure C PSPCL_ISMS Scope for detailed scope statement

Information Security Management System

Requirement of an Information Security Management System (ISMS)

Information along with the processing systems associated with it is called information assets which add value to the organization and therefore, needs to be suitably protected. Information security protects information from a wide range of threats and vulnerabilities to ensure business continuity minimize business damage and maximize return on investments and business opportunities.

PSPCL has planned an Information Security Management System (ISMS) for its IT department in conjunction with other departments to accomplish its business objectives in a secure and timely manner. Introducing ISMS, demonstrates the commitment that PSPCL shall do its best efforts to safeguard information assets. The commitment must extend from each employee involved in the business operations to other stake holders like suppliers using organization's information systems for business purposes.

Overview of ISMS

Information can exist either in printed or electronic form, transmitted by post or using electronic means, shown on films, or spoken in conversation. However, it is mandatory that whatever form the information takes, or means by which it is shared, transmitted or stored, it should always be appropriately protected.

The ISMS is a part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security in an organization. The ISO27001:2013 standard provides a guideline to develop a framework or a system to initiate, implement, maintain and manage information security within the organization. This framework would help the organization to determine the status of their information security programs and, where necessary, establish a target for improvement.

The benefits of ISMS envisaged by PSPCL will be achieved by establishing organizational structures, implementing suitable set of controls which consists of policies, standards, procedures, and guidelines. These controls have been established to ensure that the specific security objectives of the organization are met. The Information Security Framework and security policies at PSPCL are driven by the following fundamental pillars of information security:

- **Confidentiality** relates to the protection of sensitive information from unauthorized disclosure.
- **Integrity** relates to the prevention of accidental or unauthorized alteration of information and safeguarding the accuracy of information.
- **Availability** relates to safeguarding necessary resources and associated capabilities and ensuring availability of information when it is required by the business process.

PSPCL's ISMS reflects the management's commitment towards protection of confidentiality, integrity and availability of all information assets, as per the Information Security Framework and security policies of the Organization.

PSPCL's Information Security Framework and policies shall be applicable and binding to all employees, third party vendors using organization's information systems for business purposes.

Information Security Framework

The Information Security Framework is essentially based on the key factors of People, Processes and Technology. It is also dependent on a sound foundation of an Information Security Management Structure, supported by the pillars of Senior Management Commitment in the form of an Information Security Council and a thrust on ensuring security awareness within the organization, by setting up an Information Security Management Team.

The Information Security framework would involve the development and deployment of policies and procedures across the organization, monitoring their implementation on a continuous basis and ensuring a sound response and recovery mechanism to ensure continual improvement.

Strategy for Management of Information Security

The information security policies will be implemented and control objectives achieved through the following:

- Periodically assessing risks and planning their mitigation
- Creating awareness of security policies and objectives among employees through security training and on the job training
- Ensuring implementation of the security framework in accordance with the policies and processes laid down
- Having an information security organization that owns, and monitors the effectiveness of the ISMS and takes suitable corrective actions
- Provide necessary resources, infrastructure and funds for implementing the security system
- Security processes and procedures shall be audited periodically as part of the internal audit process and by external agencies
- The leading practices in information security management shall be adopted by taking inputs from global security standards followed worldwide, existing policies and procedures, stakeholders within the organization and external consultants if required.

LEADERSHIP

PSPCL management is committed towards implementing strong and robust Information Security Management System (ISMS). The ISMS shall be based on the requirements of organization and the ISMS objectives shall be framed that are based on the business objectives.

▪ Leadership and Commitment

One of the key factors in the successful implementation of information security in any organization is the visible support and commitment from management. Top management shall make sure that information security is taken seriously across the organization.

An Information Security Council (ISC) shall be constituted as an apex body within PSPCL to give a clear direction with management and financial support for information security initiatives. The ISC will be headed by Chief Engineer (IT) whose members shall be nominated by the competent authority.

ISC of PSPCL shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

- Establishing an ISMS policy;
- Ensuring that information security objectives and plans are established;
- Establishing roles and responsibilities for information security;
- Communicating to the organization the importance of meeting information security objectives and conforming to the ISMS Policy, its responsibilities under the law and the need for continual improvement;
- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS;
- Deciding the criteria for accepting the risk and acceptable levels of risk;
- Ensuring that internal ISMS audits are conducted; and
- Conducting timely management reviews of the ISMS

ISMS Policy

The organization is committed to provide comprehensive protection to its information assets against the consequences of breaches of confidentiality, failures of integrity and/ or interruptions to their availability. The ISMS Policy provides management direction and support to implement information security controls across PSPCL as an organization.

Safeguarding the information assets is of paramount importance to PSPCL. In this effort, PSPCL is committed to maintain and improve information security across the organization. ISMS Policy establishes the policies that institute the standards and procedures, to be followed to

- Maintain Confidentiality, Integrity and Availability of information assets, and, ensure Business Continuity Plans are developed, maintained and tested.
- Comply with Legal, Regulatory and contractual requirements including protection of personally identifiable information.
- Impart Information Security awareness to all employees, and, ensure Information Security Incidents are reported, recorded and responded.

The security policies are applicable to all business units, which are using PSPCL information's assets for carrying out their operations, all information processing facilities of PSPCL, all employees, contractors, supplier and their employees and individuals with access to information asset at any operational location of PSPCL.

All employees and supplier staff using PSPCL's information assets shall comply with the ISMS Policy. Non-compliance or any violation to the ISMS Policy could be subject to disciplinary action(s) as per PSPCL Employee Punishment & Appeal regulations or the contract.

Refer PSPCL Information Security Management System Policy

Information Security Roles and Responsibilities

To manage information security within PSPCL, a formal information security organization structure has been defined with agreed responsibilities, authority and relationships to manage information security within organization.

The following diagram represents a generic structure of Information Security Organization defined for PSPCL. The list of members is listed below. PSPCL Senior Management has made clear assignments of Information roles, responsibilities and objectives throughout the Information Security Organization

(Refer below Figure)

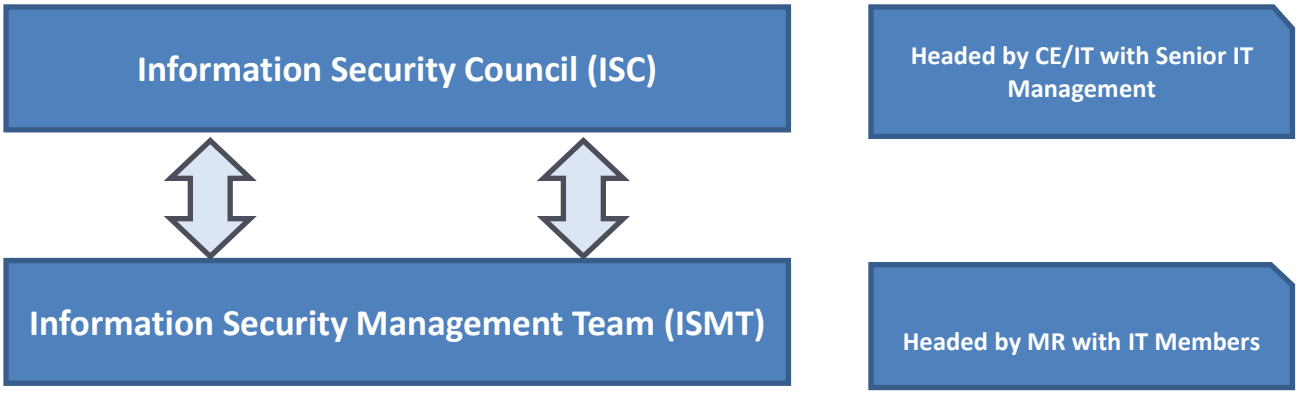

Figure 1- Information Security Organization

▪ Information Security Council (ISC)

An Information Security Council (ISC) shall be constituted as an apex body within PSPCL to give a clear direction with management and financial support for information security initiatives. The ISC will be headed by Chief Engineer (IT) whose members shall be nominated by the competent authority. The members may be as follows:

EIC– IT	Chairperson
SE-IT (O&S)	CISO/Member
SE-IT (A&PM)	Alternate CISO/Member
DGM-IT(SD&I)	Member
SE-Tech to Director/Distribution	Member
CAO to Director/Finance	Member
Sr. Xen/ISM (Information Security Manager)	Member cum Convener for maintaining the policy and providing support and advice during implementation

Information Security Council shall have the following responsibilities:

Position: Member of Information Security Council

Chaired by: CE – IT

Responsibilities of Information Security Council:

The chairperson of Information Security Council shall take overall responsibility for Information Security, including

I. Define and provide guidance for the Information security goals & objectives
   A. Ensure that information security goals are identified.
   B. Provide support to information security initiatives to enhance overall information security posture of the organization;
   C. Drive and initiate information security awareness programs for all the employees in the organization;
   D. Decide on future security solutions to be implemented in organization based on recommendations from IS Lead and audit team;
   E. Perform any other high-level information security management activities as deemed fit by the Council.

II. Identify roles and assign Information Security responsibilities

III. Monitor effectiveness and track improvement in Information Security Posture through activities like review of audit reports &technical assessment, monitoring KPI presented by MR, suggestions received from interested parties.

IV. These activities can be shared to Information Security Council as and when required.

Authority of Chairperson of Information Security Council

I. Approve Information Security Policies

II. Approve information security initiatives to enhance overall information security posture of the organization

Responsibilities of Management Representative (MR)

MR shall have following responsibilities:

I. Organize and facilitate security discussion in IT Information Security Council meetings

II. Review implementation of information security policies

III. Ensuring security goals should meets legal compliance requirements

IV. Ensure if any critical incidents experienced by organization is well addressed and approve the corrective and preventive actions to prevent any recurrence of such incidents;

V. Seek legal guidance in case information assets are hacked or there is compromise of sensitive customer or company data;

VI. Review any remedial work / punitive action related to security incidents. For this purpose, the Legal and Human Resource department's consent shall have to be obtained on any punitive action to be taken against an employee because non-compliance

VII. Initiate and monitor risk assessment activities including taking decisions on Risk Treatment Plan

VIII. Assess information security initiatives and provide recommendations
   A. Review new requirements for information security based on business

requirements or regulatory requirements B. Discuss with Information Security Council about the plan of implementation and benefits IX. Review information security audits and technical assessment reports, risk assessment A. Provide necessary resources and support for audit
Authority of Management Representative (MR) I. Authorize need for implementation of new information security tools and products across the organization; II. Approve the audit and technical assessment scheduling

▪ Information Security Management Team (ISMT)

ISMT shall include representatives identified from IT Department, responsible for leading and approving security related activities as per the ISMS Policy. ISMT shall include the following:

1. ASE/Sr. Xen-IT,DCM
2. System Software Manager-IT
3. ASE/Sr. Xen-IT, GUPM
4. ASE/Sr.Xen-NSP
5. ASE/Sr. Xen-IT/ Imp. DRC Jalandhar

MR would chair the ISMT meetings.
ISMT will ensure all initiatives / activities / requirements related to information security at PSPCL are completed. ISMT will meet once a month.

Position: Member of Information Security Management Team
Chaired by: Management Representative (MR)
Responsibilities of Information Security Management Team: I. Review of ISMS Policy A. Review ISMS Policy& procedures; B. Facilitate completion of action items from ISMS Policy C. Align policies and procedures with ISO 27001 requirements; D. Analyze resources required to implement various information security requirements from policies and procedures; E. Collate feedbacks from business representative &Information Security Council and append ISMS Policy; F. Supervise Vulnerability assessment and penetration testing activities; G. Ensure implementation of corrective actions for non-compliance observed during audits; II. Provide authorization for the identified corrective actions

III.	Review Information security audits and technical assessment reports, Risk assessment
IV.	Ensure appropriate measures are implemented or initiated for sustaining business continuity of all business processes and systems;
V.	Ensure security requirements are addressed in all third-party agreements with the vendors and contractors;
VI.	Periodic Monitoring and reviews
VII.	Business Continuity Management A. Review of critical systems and process to be covered under business continuity procedures; B. Review of business continuity procedures for all critical systems and processes of IT Department. C. Review of business impact analysis for critical business applications D. Review of test business continuity plan on periodic basis
VIII.	Tracking of approved mitigation actions and corrective and preventive actions as an outcome of audits of various functions.
IX.	Monitoring the organization-wide information security education and its effectiveness.
X.	Oversee the implementation of the information security policies;
XI.	Interfacing with auditors during information security audits;
XII.	Maintaining and tracking the risk treatment plan and audit closure sheets
XIII.	Managing the security training and awareness programs
Authority of Member of Information Security Management Team	
I.	Authorize the identified corrective actions

PLANNING

Actions to address risks and opportunities

To achieve the Information Security objectives while managing the risk effectively and efficiently, organization shall have comprehensive understanding of their risks and opportunities to ensure that Information Security Management System achieves its defined Information Security objectives.

Information security risk assessment

PSPCL has a developed a risk based approach for its ISMS program. The ISMS approach for Information Security Risk assessment includes the following elements:

- Identifying and ranking the sensitivity and criticality of information assets that could be affected in case a threat materializes. This is carried out to identify the information assets that are the most important to business;
- Identifying threats and vulnerabilities that could harm and thus adversely affect critical operations and assets. Potential threats to the business may be malicious software, intruders, disgruntled employees, natural and manmade disasters;
- Estimating the likelihood of occurrence of such threat based on historical information and judgment of knowledgeable individuals;
- Estimating potential loss or damage (in qualitative terms) that could occur, if a threat materializes;

- Evaluating existing controls;
- Identifying actions to mitigate or reduce the risk. These actions include implementing new organizational policies and procedures as well as technical or physical controls;
- Documenting the results and developing an action plan

Refer SOP 16 Risk Assessment Procedure document for details on ISMS Risk Management approach

Information security risk treatment

For each of the identified information security risks, identify if organization is ready to accept the risks or they would treat the risk or transfer the risk. Obtain the risk treatment plan to effectively implement the control for risks that needs treatment.

Refer SOP 16 Risk Assessment Procedure document for details on ISMS Risk Management approach

ISMS Objectives

To protect critical information from unauthorized access, use, disclosure, modification and disposal, whether intentional or unintentional, internal or external, deliberate or accidental.

- To identify the information assets, to understand their vulnerabilities and the threats that may expose them to risk, through appropriate risk assessment;

To manage the identified risks to an acceptable level through the design, implementation, monitoring and maintenance of a formal Information Security Management System (ISMS);
To ensure confidentiality, integrity and availability of information acquired permanently, or in transit, provided or created.
To ensure breaches of information security, actual or suspected, are reported, investigated and appropriate corrective and preventive actions shall be initiated.
To ensure awareness programs on information security are available to all employees and wherever applicable to third parties and regular training shall be imparted.

- Review of information security audit activities

The above objectives will be measured as part of KPIs and will be monitored on a continual basis.

Refer KPI Sheet for ISMS Effectiveness Measurement

SUPPORT

Resources

The Information Security Council of PSPCL shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

Competency

PSPCLISC has defined ISMS Governance Structure and has determined ISMS roles needed to establish, implement, operate and maintain Information Security Management Systems as per the scope. ISC has provided the nominations for the identified ISMS roles w.r.t each Operation as per the required competency.

Refer Annexure D for Competency Matrix

Training and Awareness

PSPCL is determined to embed Information security training, awareness and competency into its routine operations and management processes. This includes communicating ISMS Policy to all employees and the importance of meeting information security objectives. This will ensure that all employees are aware of how they contribute to the achievement of the ISMS objectives. To achieve this, the organization will raise, enhance and maintain awareness through an ongoing ISMS education and information program for all associates.
All the personnel who are covered in the scope of ISMS shall be aware of the ISMS policy, wherever relevant, followed by the organization. They should be aware of their roles and responsibilities towards successful achievement of ISMS objectives as well as conscious about the implications of not conforming to the requirements of information security management system.

Communication

ISMS is a dynamic framework which incorporates changes which occur within the organization. To keep stakeholders and interested parties up to date with the changes and developments in the ISMS, a communication plan is established. This plan defines the procedure and guidelines to establish effective communication with stakeholders and interested parties and keep them informed about ISMS improvements or events of a disaster leading to business disruption at the locations within the scope of ISMS.
The primary objective of the communication plan is:

- to identify the key internal and external parties for establishing communication
- to define the criteria for communication with interested parties
- establish controlled communication structure
- utilize the pre-defined templates for communication
- identify accountability, roles and responsibilities for communications personnel, as well as capture individuals and contact information for each role

Refer Annexure-EPSPCL_ISMS Communications Management Plan V 1.3

Documented Information

General

PSPCL shall document the requirements for implementing the ISMS based on ISO 27001:2013 and shall continuously review and update at least once in a year or whenever there is any significant changes

Creating and Updating

PSPCL shall create, maintain and update the necessary ISMS documentation and related records. All documents shall have unique identification, shall be duly reviewed and approved for suitability and adequacy, periodically.

Control of Documented Information

PSPCL shall control the documentation for its ISMS annually.

Refer PSPCL_ISMS Documented Information Procedure V 1.3

Operational Planning and Control

PSPCL shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in section 4.1. The organization shall also implement plan to achieve information security objectives determined in section 4.2.

Information Security Risk Assessment

Risk Assessment in information security identifies and assesses risks related to information assets. The risk assessment is the determination of risk associated with PSPCL's information assets and analyzing the likelihood of occurrence and consequences of these risks. PSPCL will perform the Risk Assessment in line with the defined and documented Risk Assessment Methodology.

Risk Assessment is applicable to Operations as per the defined scope and the underlying infrastructure / support processes.

Risk Assessment shall be performed annually or in case of any significant changes in the information security structure of the organization.

Information Security Risk Treatment

Risk Treatment Plan involves prioritizing, evaluating and implementing appropriate controls to mitigate identified information security risks.

ISC members would work along with process owners to develop mitigation plan for each of the information security risks. The mitigation plan also elaborates the actions to be taken to reduce the residual risk to an acceptable level based on organization's agreed risk appetite.

ISC members should decide what action needs to be taken to reduce the residual risk to an acceptable level.

PERFORMANCE EVALUATION

Monitoring, measurement, analysis and evaluation

It is a self-evaluation process for the maintenance of ISMS which focuses on the measurement of the ISMS implementation effectiveness based on pre-defined KPI parameters. Information Security team shall monitor the effectiveness of ISMS on a regular basis and report the results to the MR. Further, the MR communicates the results to the ISC bi-annually. Following activities are performed to assess the effectiveness of ISMS:

- internal audits performed annually by internal auditors
- risk assessment activity performed annually or in case of any significant changes along with ISC members from respective Operations

Internal audit

The ISC/CISO shall appoint the Internal Audit Team and its Lead Auditor. The MR shall plan for and schedule internal ISMS audits annually to determine whether the control objectives, controls, processes and procedures of its ISMS

- conform to the requirements of ISO27001 standard and relevant legislation or regulations
- conform to the identified information security requirements
- are effectively implemented and maintained
- perform as expected

An audit activity shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.
The responsibilities and requirements for planning, conducting, reporting results, maintaining audit records shall be defined in a documented procedure.
The respective business owner, responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected non-conformities and their causes. Improvement activities shall include the verification of the actions taken and the reporting of verification results.

Refer PSPCLISMS Policy PO 17 and SOP 17 Internal Audit Procedure

Management Review

Management review for ISMS shall be conducted bi-annually. The Information Security Council and ISMT shall respectively meet and review the overall ISMS.

The input to ISMS review shall include information on:

- results of ISMS audits and reviews
- feedback from interested parties
- techniques, products or procedures, which could be used to improve the ISMS performance and effectiveness
- status of Non-Conformity and corrective actions

- vulnerabilities or threats not adequately addressed in the previous risk assessment
- follow-up actions from previous ISMS reviews
- any changes that could affect the ISMS
- results of risk assessment and status of risk treatment
- Opportunities for continual improvement.

The output of the management review shall include any decisions and actions related to the following:

- improvement of the effectiveness of the ISMS;
- modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:
    - business requirements
    - security requirements
    - business processes effecting the existing business requirements
    - regulatory or legal environment
    - levels of risk and/or levels of risk acceptance

The minutes for management reviews shall be documented and retained.

IMPROVEMENTS

Nonconformity and corrective action

ISMS shall be reviewed and necessary actions to ensure the system is up to date shall be taken. The nonconformities arising out of internal audits and external audits shall be documented and necessary action items shall be taken.
A list of corrective actions shall be maintained with actions to be taken duly reviewed and the results of action taken shall be assessed.

Continual Improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.
PSPCL will continually improve the efficiency of its ISMS by making use of the ISMS Policy, security objectives, audit results, analysis of monitored events, corrective actions as well as the management review or whenever there is:

- a revision in the PSPCL's ISMS Policy or ISO 27001 standard
- a change in the Risk Assessment process
- a change in the legal and/or regulatory requirements
- emerging information security risks that are not addressed adequately in the current ISMS
- a new security incident that warrants changes or improvements in the ISMS framework
- a significant technological change is planned for the existing infrastructure

PSPCL will act accordingly to protect against future non-compliance and its re-occurrence.

ANNEXURES

Annexure Name	Document
Annexure A- Organizational Context	Organizational Context v1.3.xlsx
Annexure B- Requirements of Interested Parties	PSPCL_Interested Parties List_v1.3.xlsx
Annexure C-ISMS Scope Document	PSPCL ISMS Scope Document_V1.3.docx
Annexure D -Competency Matrix	Competency Matrix V1.3.xlsx
Annexure E–Communications Plan	ISMS Communication Plan.xlsx