Information Security Manual.

For

Promoto Software Pvt Ltd

91springboard, Plot 23,

Maruti Industrial Area, Sector 18,

Gurugram, Haryana 122015

INDIA

Document Control

Document Reference No.	CSB/POL/2018/12/003
Document Name	Information Security Manual 1.0
Version No.	1.0
Document Status	Released
Issue Date	16th Dec 2018
Compliance Status	Mandatory
Distribution	Management/Employees/Business Associates (on Demand)
Revision Cycle	

Review and Approval

Sr. No:	Date	Name	Position
1	16th Dec 2018	Puneet Kataria	CEO
2			

Sr. No:	Change Description	Change Date	Change Approval
1			
2			

Contents

1. Introduction and Scope

Information is a valuable asset that needs to be protected from unauthorized disclosure, modification, use, or destruction. Promoto Software Pvt Ltd (PSPL) shall ensure that its Information Asset's confidentiality, integrity, and availability are not compromised.

This document is an ISMF directives manual, which are to be promulgated to each employee under the ISMF scope in PSPL, for safeguarding the Information Assets of the company. All departments under the ISMS scope are required to follow this Information Security Policies hereby established. All users (employees, contractors, vendors, and other parties) are expected to understand and abide by them.

In addition to defining roles and responsibilities, these policies raise awareness of users regarding potential risks associated with information assets.

PSPL perceives to mitigate security incidents, decrease loss of productivity due to security breaches, and assure the implementation and conformance of controls for information security throughout the organization.

These policies have been designed to implement an Information security Management System conforming to ISO 27001:2013. The policies are designed to comply with applicable laws and regulations. However, if there is a conflict, applicable laws and regulations will take precedence.

These policy statements seek to provide a baseline secure environment for day to day operations at PSPL. Contractual obligations may require implementation of additional processes for which necessary policies and procedures will need to be developed.

2. Common Policy Elements

2.1 Enforcement

The CEO and the ISF(Information Security Forum) shall be responsible ensuring implementation of security policies and corresponding processes. Regular audits are to be undertaken to ensure compliance with these policies and processes. Periodic reviews will be undertaken of the policies and processes to ensure that they remain current, relevant, efficient and effective Violators of these policies shall be subject to employee disciplinary proceedings as per HR Policies.

2.2 Exceptions

Exceptions to a policy will be promulgated by the CEO consequent upon formal review by the ISF. In each case the request for exception shall be made in writing, and include such details as the need for the exception, the scope and extent of the exception and duration for which the

exception is sought.

2.3 Version History

As policies are revised, a summary of the changes made shall be listed at the beginning of this and each policy, procedure and guidelines.

2.4 Information Security Policy Manual Owner

The ownership of Information Security Policy Manual of PSPL lies with the Information Security Forum (ISF). Any changes or updates to this document will be drafted by ISF and thereafter reviewed by the CISO for approving the change. A policy change shall be implemented only post approval by the CEO.

3. Terms and Definitions

This section includes some of the important terms referenced in the various enterprise information security policies. Additional terms may be defined within each individual policy.

Term	Definition
Change Management	A business process that ensures that only authorized changes take place and that all changes are authorized after having gone through a process which is designed to ensure that the change will perform as expected with no unexpected outcomes.
Information Processing Facilities or Information Processing and Communication Facilities	A facility that contains a data center, network operations center, or other similar information system command or monitoring center with computer systems that store production information or house network services or user workstations.

Term	Definition
Information Security	Preservation of *confidentiality, integrity, and availability* of information. *Confidentiality* - Ensuring that information is accessible only to authorized users *Integrity* - Safeguarding the accuracy and completeness of information and processing methods *Availability* - Ensuring that authorized users have access to information and associated assets when required
Information Security Incident or Breach	An event that results in unauthorized access, loss, disclosure, modification, non-availability or destruction of information resources whether accidental or deliberate.
Information System	The network or combination of all computing equipment, telecommunication or other communication or information processing devices and channels used within an organization.
Risk Assessment	Assessment of vulnerabilities and threats and their impact on information and information processing facilities.
Risk Management	Process of identifying, controlling, and minimizing or eliminating security risks that may affect information systems
SLA - Service Level Agreement	A detailed subsection of a contract that specifies the expectations of the contracting parties regarding services, procedures and responses.
Teleworking/Telecommuting	The practice of working from a site that is remote from the user's normal base office but still within a more controlled environment than a typical remote dial-in or internet connection. Teleworking allows staff to work from a fixed location that is remote from the organization's base operation.

Term	Definition
Trojan Code	Software that is written to allow access to a computer via some method not intended by the owner of the system. Typically embedded in some other form of software Trojan code attempts to camouflage its presence to avoid detection. Trojan code operates by either announcing itself to the writer of the code when installed or by responding to a special form of prompting. The intent of the code is to allow access to a computer without the knowledge of the computer owner.
ISF	Information Security Forum
ISM	Information Security Manager, Managing, constructing and administering information security.
CEO	Chief Executive Officer
Users	Employees, contractors, vendors, or any other parties who are granted access to PSPL Development system, support systems and application

4. Organizational Security

4.1 Information Security Infrastructure

4.1.1 Information Security Infrastructure

Purpose

To establish an Information security infrastructure for PSPL.

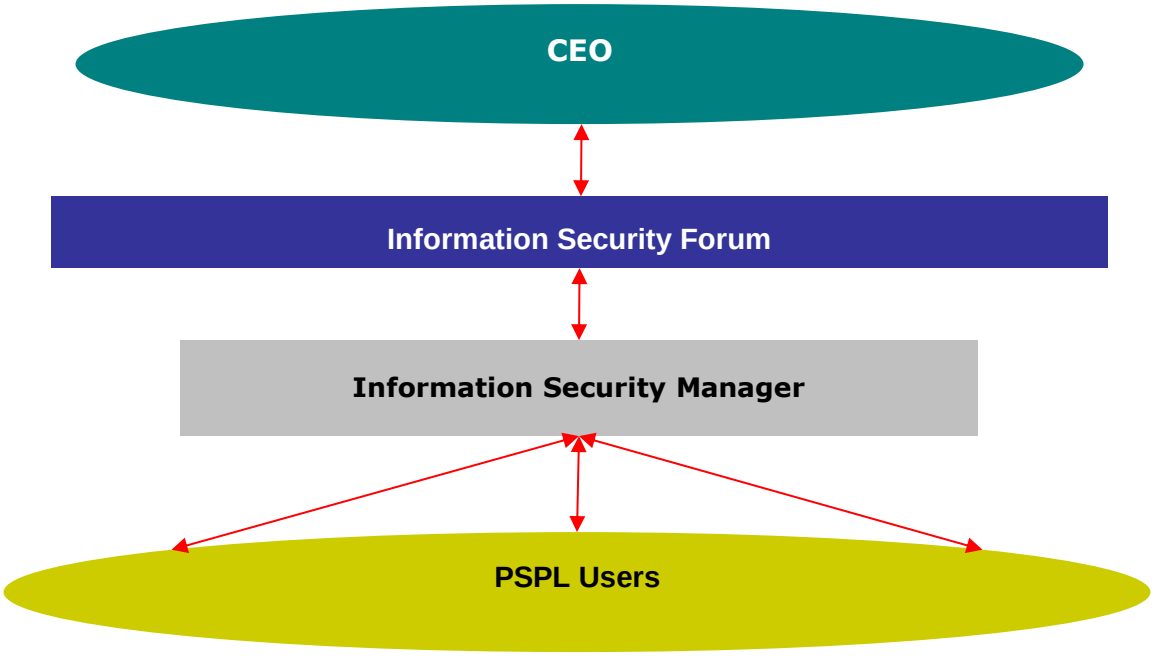
Scope

All operations of PSPL.

Policy

PSPL shall identify appropriate resources to create an Information Security Organization Structure that will manage and implement the Information security policies and processes at PSPL.

4.2 Information Security Organizational Structure



4.3 Security of Third Party Access

4.3.1 Security Requirements in Third Party Contracts

Purpose

To provide guidance on the information security issues that should be considered when using third party resources to accomplish business objectives.

Scope

All processes that use external resources to perform work within the business functions.

Policy

Any contract with a third party involving access to PSPL information assets will outline information security issues (based on risk identification) relevant to that access and require the third party to adhere to PSPL's information security policies and processes.

4.4 Outsourcing

4.4.1 Security Requirements in Outsourcing Contracts

Purpose

To provide guidance when using outsourced service providers to manage and maintain information resources.

Scope

All processes that use outsourced services, through a formal contract.

Policy

All outsourcing contracts will contain provisions to ensure adherence to PSPL's Information Security Policy Manual.

5. Asset Classification and Control

5.1 Accountability for Assets

5.1.1 Inventory of Assets

Purpose

Provide guidance in creating accountability, for PSPL's information assets.

Scope

Hardware, communications devices, software packages, documents and other information assets in use at PSPL operations.

Policy

All information assets used by PSPL will be documented and the list periodically reviewed. The periodicity of review shall be decided by the respective Departmental Heads and shall not exceed twelve months.

5.2 Information Classification

Purpose

Establishing policies for the classification of all information used by PSPL for its operations.

Scope

All information residing within resources operated by PSPL.

Policy

PSPL will adhere to an information classification system, which includes the extent to which information should be disclosed to specified users.

5.2.1 Information Labeling and Handling

Purpose

To address the issue of how all the information that has been classified should be labeled and

handled.

Scope

Information that has been classified by PSPL.

Policy

Each department shall adopt and use information labeling and handling procedures in accordance with the information classification scheme adopted by PSPL.

6. Personnel Security

6.1 Security in Job Definition and Resourcing

6.1.1 Inclusion of Security in Job Responsibilities

Purpose

To minimize the risks of human errors, fraud, misuse of information systems and to ensure awareness and responsibility towards information security from all employees.

Scope

All full time employees, contract employees and third party contractor's employees working for PSPL.

Policy

The job responsibilities of all employees shall include adherence to laid down information security polices as per the company security policy.

6.1.2 Personnel Security Screening

Purpose

To address information security concerns at the recruitment stage of employment for all employees, and prior to the engagement of contractors.

Scope

All full time employees, contract employees and third party contractor's employees working for PSPL.

Policy

Appropriate screenings of prospective employees and contractors shall be carried out.

6.1.3 Confidentiality Agreements, Security Terms and Conditions

Purpose

To ensure that all users are aware of their security responsibilities and do not compromise information security inadvertently.

Scope

All full time employees, contract employees and third party contractor's employees working for PSPL.

Policy

All employees shall sign a confidentiality or non-disclosure agreement with PSPL as part of their induction into the organization.

6.2 User Training

6.2.1 Information Security Education and Training

Purpose

To ensure that users are security conscious and aware of the different security threats, concerns, and the procedures for reporting security incidents.

Scope

All full time employees, contract employees and third party contractor's employees working for PSPL.

Policy

All employees shall undergo appropriate security awareness training.

6.3 Responding to Security Incidents

6.3.1 Reporting Security Incidents

Purpose

To ensure that PSPL has a defined process to report security incidents so that they can be dealt with quickly to minimize the overall risk to the organization.

Scope

All full time employees, contract employees and third party contractor's employees working for PSPL.

Policy

PSPL shall implement a security incident reporting process and ensure employees are aware of this process and are encouraged to use it.

6.3.2 Reporting Security Weaknesses

Purpose

To improve security awareness among the employees of PSPL.

Scope

All full time employees, contract employees and third party contractor's employees working for PSPL.

Policy

PSPL shall have a process for users to report any perceived information security threats and vulnerabilities.

6.3.3 Reporting Software Malfunction

Purpose

To monitor all malfunctions and to look for security related problems

Scope

All full time employees, contract employees and third party contractor's employees working for PSPL.

Policy

PSPL shall have a process for users to report software malfunctions on information systems.

6.3.4 Learning from Incidents

Purpose

To all ensure security related incidents are documented and appropriate corrective and preventive action is undertaken.

Scope

All identified security incidents.

Policy

PSPL shall develop a process to quantify all reported incidents, and implement appropriate corrective and preventive action plan.

6.3.5 Disciplinary Process

Purpose

To ensure that a process is in place to deter employees from violating PSPL's information security policies.

Scope

All full time employees, contract employees and third party contractor's employees working for PSPL.

Policy

Employees in violation of PSPL's information security policies shall be subject to disciplinary action.

7. Physical and Environmental Security

7.1 Secure Areas

7.1.1 Physical Security Perimeter

Purpose

To ensure that PSPL takes appropriate measures designed to safeguard the physical perimeter of the facility that houses its information systems.

Scope

PSPL facility and data center.

Policy

PSPL will ensure appropriate measures and procedures are in place to prevent, detect and mitigate the impact of unauthorized access or damage to its facility.

7.2 Equipment Security

7.2.1 Equipment Siting and Protection

Purpose

To reduce the risk to all business critical equipment from environmental threats and hazards and deter unauthorized access.

Scope

All the business critical equipment's owned or managed by PSPL.

Policy

All the business critical equipment shall be secured from physical and environmental threats.

7.2.2 Power Supplies

Purpose

To protect business critical equipment and information systems from power anomalies.

Scope

PSPL information systems that are deemed sufficiently critical to warrant power protection.

Policy

All PSPL information systems that are deemed sufficiently critical to warrant power protection shall be provided with uninterruptible power supply.

7.2.3 Cabling Security

Purpose

To protect telecommunications and power cabling.

Scope

All critical power and telecommunications cabling.

Policy

Appropriate protective measures shall be undertaken to ensure that all critical cabling pertaining to power and telecommunication networks is protected.

7.2.4 Equipment maintenance

Purpose

To ensure maintenance of equipment.

Scope

All information systems and related equipment at PSPL.

Policy

Appropriate maintenance procedures shall be implemented for all critical equipment.

7.2.5 Secure Disposal or Re-Use of Equipment

Purpose

To prevent exposure of sensitive information assets from improper data cleansing of equipment.

Scope

PSPL computing or communications equipment that is disposed or re-used.

Policy

Proper disposal of equipment shall be done to ensure that there is no unauthorized exposure of information.

7.3 General Controls

7.3.1 Clear Desk and Clear Screen

Purpose

To ensure that information or information processing systems are not left unattended at any given point of Time.

Scope

All personnel working on critical PSPL systems.

Policy

All PSPL personnel (employees and third party) working on critical systems or sensitive information are expected to maintain clear desk and clear screen when leaving their respective seats.

7.3.2 Removal of Property

Purpose

To monitor removal of any property from PSPL.

Scope

PSPL operations.

Policy

Equipment, information or software belonging to the organization shall only be removed upon authorization of the management.

8. Communications and Operations Management

8.1 Operational Procedures and Responsibilities

8.1.1 Documentation of Operating Procedures

Purpose

To ensure the secure operation of information processing facilities of PSPL through the documentation and maintenance of operating procedures.

Scope

This policy addresses the definition, documentation, and maintenance of the operating procedures for PSPL systems.

Policy

Operating procedures and responsibilities for all PSPL information processing facilities will be formally authorized, documented, and maintained.

8.1.2 Operational Change Control

Purpose

To implement formal change management control procedures to protect PSPL information systems and services.

Scope

This policy addresses the definition and documentation of information assets change management control procedures.

Policy

Changes to all information processing facilities, systems, software, or procedures will be strictly controlled, documented and authorized according to formal change management procedures.

8.1.3 Incident Management Procedures

Purpose

To establish response procedures to ensure the quick, orderly, and effective handling of security incidents.

Scope

This policy addresses the definition and documentation of security incident management procedures for information systems and services.

Policy

Security incident management procedures will be established to ensure quick, orderly, and effective responses to security incidents.

8.1.4 Segregation of Duties

Purpose

Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.

Scope

PSPL Operations.

Policy

The organization shall ensure clear documented segregation of duties, roles and responsibilities.

8.1.5 Separation of Development and Operational Facilities

Purpose

To require the separation of operational, development, and test computing environments to reduce the risk of unauthorized access or accidental changes to operational software or data.

Scope

The system development Operations at PSPL.

Policy

Operational computing environments will be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.

8.1.6 External Facilities Management

Purpose

To reduce security exposure and prevent compromise, damage, or loss of data when external contractors provide information processing facilities for systems or services.

Scope

Contracted services for information-processing facilities that are entrusted with PSPL's information assets.

Policy

Contractual controls consistent with PSPL's Information Security Policy will be established to reduce security risks created when external contractors are utilized to provide information processing facilities.

8.2 System Planning and Acceptance

8.2.1 Capacity Planning

Purpose

To ensure the proper management of capacity planning to meet current and future information system requirements so as to minimize the risk of failure due to inadequate system resources.

Scope

The Operations at PSPL.

Policy

System capacity requirements will be monitored and usage projected to ensure the continual availability of adequate processing power, bandwidth, storage and necessary manpower.

8.2.2 System Acceptance

Purpose

To reduce the risk of system failure due to inadequate testing and validation acceptance of new or upgraded information systems.

Scope

All Information systems at PSPL.

Policy

System acceptance criteria for all new information systems and system upgrades shall be defined, documented and utilized to minimize risk of system failure.

8.3 Protection against Malicious Software

8.3.1 Controls Against Malicious Software

Purpose

To protect the integrity of information systems and software by detecting and removing malicious software.

Scope

All Information systems at PSPL.

Policy

Security awareness, prevention and detection tools will be utilized to protect information systems and services against malicious software.

8.4 Housekeeping

8.4.1 Information Back-Up

Purpose

To ensure that back-up copies of essential electronically-stored business data are routinely created and properly stored.

Scope

All Information systems of PSPL.

Policy

Back-ups of all essential electronically stored business data of PSPL shall be routinely created, properly stored and routinely tested to ensure prompt restoration.

8.4.2 Operator Logs

Purpose

To require the maintenance of activity logs for PSPL's information systems by all the operational staff.

Scope

All critical Information systems of PSPL.

Policy

Appropriate log(s) of activities involving PSPL's critical information systems and services will be maintained and reviewed periodically.

8.4.3 Fault Logging

Purpose

To require that all faults involving PSPL's information systems and services be properly logged and reported and that appropriate action is taken to correct them.

Scope

All Information systems of PSPL.

Policy

All faults involving PSPL's information systems and services will be logged, reported and appropriate corrective action taken.

8.5 Network Management

8.5.1 Network Controls

Purpose

- To require controls for the security of data on networks.
- To protect connected services from unauthorized access.

Scope

All information residing on the network of PSPL.

Policy

PSPL shall establish operational controls and safeguards to ensure the security of its information systems and the protection of the supporting network infrastructure.

8.6 Media Handling and Security

8.6.1 Management of Removable Computer Media

Purpose

To ensure the proper management of PSPL's removable computer media. (e.g., disks, cassettes, CDs, printed reports and operational logs).

Scope

All removable computer media (e.g., disks, cassettes, CDs, printed reports and operational logs) in PSPL.

Policy

All removable computer media shall be managed securely to ensure proper and controlled

use.

8.6.2 Disposal of Media

Purpose

To ensure the safe disposal of PSPL's computer media

Scope

PSPL's removable and non-removable computer media.

Policy

When no longer required, the contents of all computer media will be disposed of permanently, destroyed or rendered unrecoverable.

8.6.3 Security of Operational System Documentation

Purpose

To require the implementation of security controls to protect all operational system documentation of PSPL from unauthorized access.

Scope

Operational system documentation for PSPL's information systems or services (e.g. **Network diagrams, router configuration, firewall rule sets**, etc.).

Policy

Operational system documentation of PSPL's information systems shall be protected from unauthorized access.

8.7 Exchanges of Information and Software

8.7.1 Information and Software Exchange Agreements

Purpose

To provide guidance in creating software exchange agreements. Such agreements are

intended to prevent loss, modification or misuse of information shared between organizations.

Scope

This policy covers agreements for the sharing of information between PSPL and external (i.e. third party) organizations.

Policy

Agreements shall be developed and implemented for the exchange of information between PSPL and other external entities to extend appropriate security controls. This shall happen on a case to case basis.

8.7.2 Security of Media in Transit

Purpose

To secure media in transit.

Scope

Any transfer of information from PSPL to external or internal entities.

Policy

All information during transit shall be protected by implementing necessary security controls.

8.7.3 Security of Electronic Mail

Purpose

To provide coordination and guidance on the establishment, administration and use of email systems, to ensure the effective and safe use of email services at PSPL.

Scope

All employees authorized to use corporate email.

Policy

PSPL will establish acceptable use policies for the use of electronic mail, which will include

inspection or review by the management.

8.7.4 Publicly Available Systems

Purpose

Give guidance for the usage of PSPL Information made publicly available on a publicly available system, e.g. information on a Web server accessible via the Internet, may need to comply with laws, rules and regulations in the jurisdiction in which the system is located or where trade is taking place.

Scope

All publicly available systems of PSPL.

Policy

There should be a formal authorization process before information is made publicly available, care should be taken to protect the integrity of published PSPL information to prevent unauthorized modification which could harm the reputation of PSPL.

9. Access Control

9.1 Business Requirement for Access Control

9.1.1 Access Control Policy

Purpose

To define access controls to information systems and resources for PSPL.

Scope

PSPL operations.

Policy

Access to PSPL information systems and computing resources will be based on each user's

access privileges. Access privileges shall be granted on the basis of specific business need (i.e. a “need to know” basis). Access Controls shall ensure that even legitimate users cannot access stored information unless they are authorized to do so.

9.2 User Access Management

9.2.1 User Registration and Password Management

Purpose

To manage the allocation of user access rights in accessing multi-user Information Systems and Resources at PSPL.

Scope

All stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to PSPL’s information systems and resources.

Policy

User access to all systems will be managed by a formal authorization process.

9.2.2 Privilege Management

Purpose

To ensure management of user access privileges for information systems and resources.

Scope

All users of PSPL information systems.

Policy

All privileges granted to users shall be granted and managed through a formal authorization process.

9.2.3 Review of User Access Rights

Purpose

To maintain effective control over access to data and information services to ensure that unauthorized privileges have not been obtained.

Scope

All users of PSPL information systems.

Policy

User access shall be periodically reviewed to monitor access to sensitive information.

9.3 User Responsibilities

9.3.1 Password Use

Purpose

To establish a standard for creation and use of passwords, the protection of those passwords, and the frequency of change for such passwords to prevent compromise of confidential information.

Scope

All personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that stores PSPL's Information.

Policy

All critical systems shall employ passwords to protect against unauthorized discovery or usage of information. Users shall be responsible for keeping their passwords confidential.

9.4 Network Access Control

9.4.1 Use of Network Services

Purpose

To establish guidelines for access and use of networks and network services at PSPL.

Scope

All users in PSPL who access PSPL's computer networks.

Policy

Access to PSPL's network and its resources shall be strictly controlled, managed, and reviewed to ensure that only authorized users gain access based on the privileges granted.

9.5 Operating System Access Control

9.5.1 Use of System Utilities

Purpose

Restrict access to local system utilities.

Scope

Types of system utilities and applications that are considered typical for administration use by privileged users but not by average users.

Policy

Access to system utilities on critical systems will be available only to those users who have a business case for accessing the specific utility.

9.5.2 User Identification and Authentication

Purpose

To ensure an audit trail.

Scope

All users accessing the information systems at PSPL.

Policy

All users accessing PSPL's critical information systems shall have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual.

9.5.3 Password Management System

Purpose

To ensure proper management of passwords used for authentication and log on to PSPL's information systems.

Scope

All passwords used for authentication on PSPL's network.

Policy

A Password management system shall be used to provide an effective, interactive facility which aims to ensure quality passwords.

9.6 Application Access Control

9.6.1 Information Access Restriction

Purpose

To prevent unauthorized access to information held in PSPL's computing resources.

Scope

All applications running on PSPL's systems and network.

Policy

Applications shall be installed on users' machines only if explicitly required to execute their specified business function.

9.6.2 Sensitive System Isolation

Purpose

To enhance the security of sensitive information.

Scope

Systems that involve sensitive information

Policy

All sensitive information shall have a dedicated and isolated systems.

9.7 Monitoring System Access and Use

9.7.1 Event Logging

Purpose

To provide for the tracking of computing resource activity that will benefit the disclosure of unauthorized activity.

Scope

The tracking of security related events and the data logs produced by the tracking mechanisms for all critical information systems at PSPL.

Policy

Log of activities shall be maintained for all PSPL's computing resources and these logs shall be stored offsite for a minimum of one year unless otherwise specified.

9.7.2 Monitoring System Use

Purpose

To ensure that there are adequate procedures in place to monitor the use of PSPL's computing resources.

Scope

All information processing facilities of PSPL.

Policy

Appropriate procedures shall be used to monitor the events and activities of users accessing resources and these shall be reviewed regularly for any discrepancies.

9.7.3 Clock Synchronization

Purpose

To assist the creation of an audit trail for any investigation

Scope

Any computing and networking resources on PSPL's Network

Policy

The system clocks of all information systems shall be synchronized.

9.8 Mobile Computing and Teleworking

9.8.1 Mobile Computing and Teleworking

Purpose

To ensure information security when utilizing mobile computing and Teleworking facilities.

Scope

All information systems being used for mobile computing and Teleworking as well as the users using them.

Policy

All mobile computing and Teleworking shall be secured by implementing appropriate controls to protect the information they carry.

10. Systems Development and Maintenance

10.1 Security Requirements of Systems

10.1.1 Security Requirements Analysis and Specification

Purpose

To ensure security is built in to information systems.

Scope

New information systems or revisions to existing information systems at PSPL

Policy

The business requirements definition phase of system development shall include a review to ensure that the system adheres to applicable security policies and standards.

10.2 Security in Application Systems

10.2.1 Data Validation

Purpose

To ensure correctness and appropriateness of input and output data in meeting the information security requirements of application design.

Scope

New information systems or revisions to existing information systems at PSPL

Policy

Data in application systems (input and output) shall be validated to ensure that it is correct and appropriate at different stages of processing.

10.3 Cryptographic Controls

10.3.1 Cryptographic Controls

Purpose

To protect the confidentiality, authenticity, and integrity of information

Scope

All information systems of PSPL

Policy

Transfer and storage of all sensitive and confidential information shall use adequate cryptographic controls.

10.4 Security of System Files

10.4.1 Control of Operational Software

Purpose

To minimize the risk of corruption of operational systems

Scope

New information systems or modifications to existing systems at PSPL

Policy

The operating system files and application software shall be secured from unauthorized use or access.

10.4.2 Protection of System Test Data

Purpose

To minimize exposure of information

Scope

PSPL information systems and/or making modifications to existing systems

Policy

Data that is to be used for testing shall not be obtained from production data.

10.4.3 Access Control to Program Source Libraries

Purpose

To minimize the potential for, accidental or intentional, corruption of application software

Scope

Systems that use program source libraries as an operational component of the operating system on PSPL computing resources.

Policy

Access to program source libraries shall be protected to ensure access by only authorized users.

10.5 Security in Development and Support Process

10.5.1 Change Control Procedures

Purpose

To minimize the corruption of information systems due to adhoc changes to information systems.

Scope

New information systems and modifications to existing systems at PSPL

Policy

All information systems shall have documented change control procedures to ensure proper versioning and implementation.

10.5.2 Review of Operating System Changes

Purpose

To ensure that operating system changes do not adversely affect the security of information systems.

Scope

New information systems and modifications to existing systems at PSPL

Policy

Before implementing changes in applications on a production computing resource, the changes shall be tested and approved to minimize security risks and disruption to the production environment.

10.5.3 Restrictions On Changes to Software Packages

Purpose

To minimize the corruption of information systems.

Scope

All software packages purchased by PSPL.

Policy

All software provided by third party vendors, and related customization, shall not be modified unless absolutely authorised. The modification shall only be performed after they have been authorized by concerned Department Head.

10.5.4 Covert Channels and Trojan Code

Purpose

To avoid compromise due to malicious software

Scope

All Information Systems at PSPL

Policy

All software packages installed on information systems shall be tested to ensure that they are not introducing covert channels and Trojan codes.

11. Disaster Recovery and Business Continuity

11.1 Aspects of Disaster Recovery and Business Continuity

11.1.1 Disaster Recovery and Business Continuity Planning

Purpose

To ensure that PSPL develops and maintains disaster recovery and business continuity plans and has processes in place to allow them to continue to deliver their essential business functions despite damage, loss, or disruption due to the unexpected occurrence of a natural or man-made emergency or disaster.

Scope

PSPL operations.

Policy

PSPL shall have a documented Business Continuity Plan in place for the entire enterprise. The development of this plan shall be a continuously managed process and it shall be periodically tested to ensure concurrence to any changes in the organization with respect to internal operations or other external factors.

12. Compliance

12.1 Compliance with Legal Requirements

12.1.1 Compliance with Legal Requirements

Purpose

To ensure that the organization does not violate any criminal and civil law, statutory, regulatory or contractual obligations and any other security requirements.

Scope

All departments of PSPL.

Policy

PSPL's information systems and operations shall comply with all applicable laws and other regulations including customer requirements.

12.1.2 Intellectual Property Rights (IPR)

Purpose

To ensure protection of intellectual property of product, services and systems handled by PSPL.

Scope

All operations of PSPL.

Policy

Appropriate policies and procedures shall be implemented to ensure protection of all IPR handled by the organization. This shall include own, customer and all third party IPR

12.1.3 Safeguarding of Organizational Records, Data and Personal Information

Purpose

Protection of all organizational information against loss, falsification or destruction.

Scope

All information handled by PSPL, including own, customers, third party and employees.

Policy

All organizational records, data and personal information with PSPL are an important asset and shall be suitably protected. Procedures shall be developed for safeguarding critical organizational records, data and personal information.

12.1.4 Prevention of Misuse of Information Processing Facilities

Purpose

To prevent misuse and unauthorized use of information processing facilities at PSPL.

Scope

All information processing facilities of PSPL .

Policy

All users shall be allowed to use PSPL's information systems only for their defined scope of work.

12.1.5 Regulation of Cryptographic Controls

Purpose

To ensure compliance to agreements and other requirements pertaining to cryptographic controls

Scope

All information assets of PSPL.

Policy

Cryptographic controls shall be implemented as per internal or customer requirements, and shall comply to legal and regulatory requirements as applicable.

12.2 System Audit Considerations

12.2.1 System Audit Controls

Purpose

To minimize the risk of disruptions to business processes due to the audit process.

Scope

PSPL operations.

Policy

All audits of operational systems shall be planned in advance and conducted on a mutually agreed date between the auditor and the auditee.

12.2.2 Protection of System Audit Tools

Purpose

To prevent the misuse of system audit tools.

Scope

PSPL operations.

Policy

All system audits tools shall be stored securely and available only to the internal audit team.

EOD.