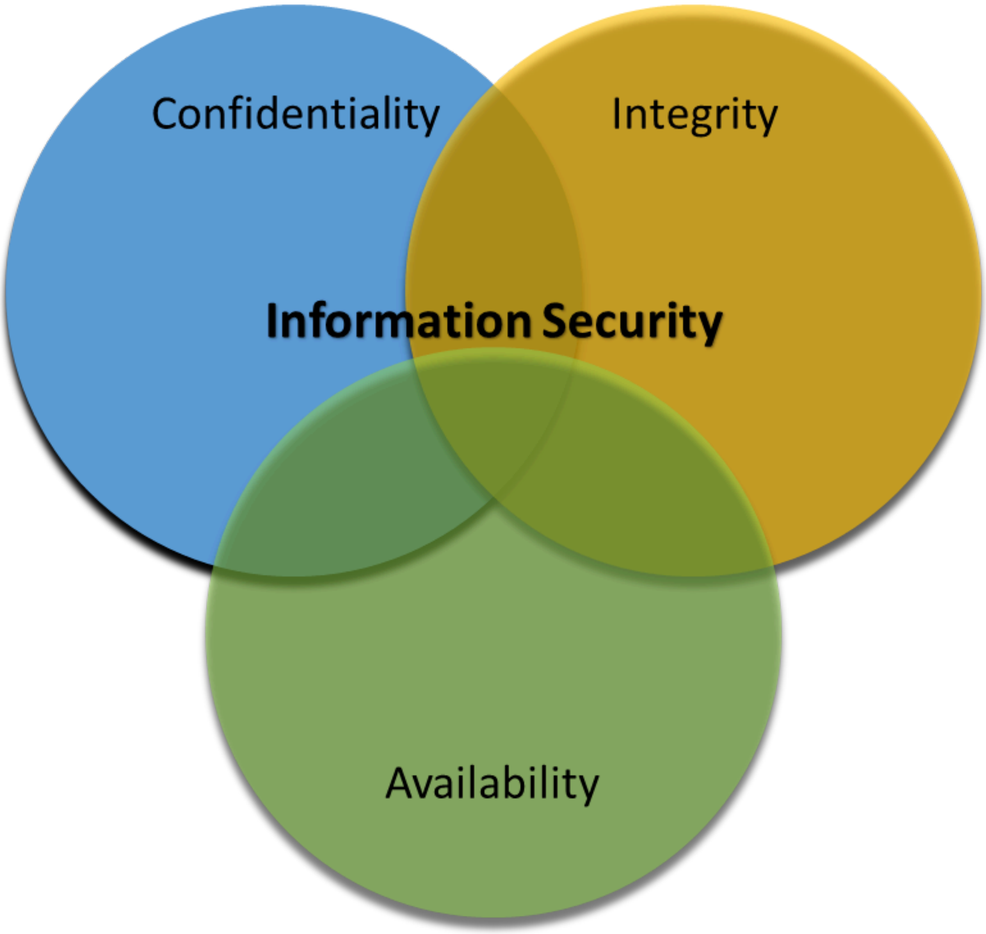
# Information Security Policy



## Document Statistics

| Type Of Information | Document Data |
|---|---|
| Document Title | Information Security Policy |
| Date of Release | 15 November 2022 |
| Document Version No | 1.0 |
| Security Classification | Internal |
| Document Status | Final |

## Document Revision History

| Ver. No. | Date | Change Description | Author | Approved By |
|---|---|---|---|---|
| 01 | 15/11/2022 | Official release | Sanjay Sharma | CDO |
| 02 | | | | - |
| 03 | | | | - |
| 04 | | | | - |
| 05 | | | | - |
| 06 | | | | - |
| 07 | | | | - |
| 08 | | | | - |
| 09 | | | | - |
| 10 | | | | - |
| 11 | | | | - |
| 12 | | | | - |
| 13 | | | | - |
| 14 | | | | - |

**Contents**

## 1. Introduction

Shriram Pistons & Rings LTD(SPRL) has an exceptional lineage of Shriram Group, one of the reputed Industrial houses. Driven by advance technology, the company has the capability to provide end-to-end solutions which include Design, Develop, Validate and Manufacture products for its customers as its Tech Centre with highly talented Design and Engineering Professionals in Concept Design, FEA, Simulation, Rig Testing, Prototype Development, and Engine Testing & Analysis. This is supplemented with continuous Technology and Application Engineering support from the technology partners including in Advanced Engineering and manufacturing processes.

SPRL strives for achieving and maintaining the industry best practices for assuring the following Information Security goals:

- **Confidentiality:** Assurance that Information is accessible only to those authorized to have access.
- **Integrity:** Assurance of the completeness and accuracy of Information and its processing methods; and
- **Availability:** Assurance that authorized user has access to Information and associated assets when required.

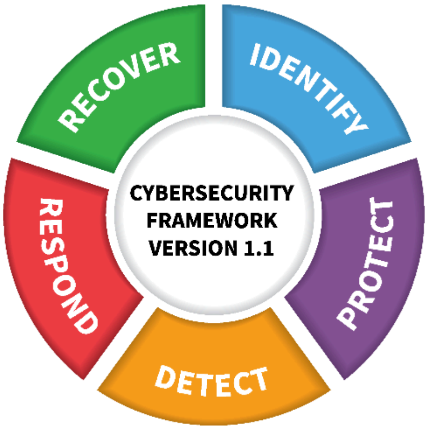
## 2. Objective

The objective of this Policy is to achieve and maintain confidentiality, integrity and availability of Information and Information Processing Facilities.

## 3. Scope

SPRL Information Security Policy is designed to provide a risk-based framework for protecting Information Assets of SPRL.

## 4. Information Security Framework



### 4.1 Structure of this policy

- Chapters 5 through Chapter 18 of this policy address the domains and controls mentioned in the standard under the following:
  - A.5 Information security policies
  - A.6 Organization of information security
  - A.7 Human resources security
  - A.8 Asset management
  - A.9 Access control
  - A.10 Cryptography
  - A.11 Physical and environmental security
  - A.12 Operational security
  - A.13 Communications security
  - A.14 System acquisition, development and maintenance
  - A.15 Supplier relationships
  - A.16 Information security incident management
  - A.17 Information security aspects of business continuity management
  - A.18 Compliance

### 4.2 Ownership and Management

The information security policy shall be reviewed on an annual basis by the head of information security to ensure that it is updated in-line with any major changes within the operating environment or on recommendations provided by internal/ external auditors and/or legal counsel.

In cases where non-compliance with the policy is identified, the head of information security shall issue either general or specific notifications to relevant staff regarding the policy established. In instances of persistent violation of established information security policies, the violator(s) shall be subject to disciplinary action in accordance with the ***SPRL Handbook.***

## 4.3 Exception Management

Compliance to the requirements outlined in this document is mandatory and deviations, if any, shall be treated as exceptions. An Exception Management process shall be defined for handling short term and long term / recurring deviations to this policy. All exceptions shall be validated by **SPRL Information Security Team** and shall be approved **by SPRL Senior Management (Function Head or delegated authority)**. All Exceptions:

- Shall be granted for a limited period post which the exception requirement shall be reconsidered. Time period granted to any approved exception shall not exceed 30 days and can be renewed maximum up to 90 days (three cycles);
- Any long term / recurring deviations due to technical / operational limitations, shall be:
  - Communicated to the exception management team for review and tracking.
  - Validated by SPRL Information Security team and shall be approved by SPRL Senior Management (Function Head level or delegated authority); and
  - Shall be reviewed annually.
- Shall be accompanied with a valid business justification and recorded. The record shall capture exception details, business justification, exception validity, supporting documents and associated approvals; and
- Shall be assessed for associated risks. Based on the risks identified through risk assessment the exception should be assigned an overall risk rating. For example, the exception risk rating can be High, Medium, and Low. Compensatory controls shall be considered to reduce the impact of identified risks.

# 5. Information Security Policies

## 5.1 Management Direction for Information Security

### 5.1.1 Policies for Information Security

- This policy highlights SPRL senior management’s intention to identify and secure organization’s valuable assets in a manner which complies with legislations, meets leading practices and business needs, protecting it from unauthorized use, disclosure, or destruction.
- The Information Security Management System Policy Statement at SPRL states:

  **“SPRL commits to protect its information assets from all identified threats, whether internal or external, deliberate or accidental, such that the confidentiality of information is maintained; integrity of information can be relied upon; availability of information is ensured; legal, regulatory, statutory and contractual obligations are met and ensure continual improvement towards organization wide Information Security Management System.”**

### 5.1.2 Review of the Policies for Information Security

- To ensure continuing suitability, adequacy, and effectiveness, the Information Security policy and supporting documents shall be reviewed at least annually or earlier if any significant changes occur. (e.g., technology level changes in the organization and business level changes in the organization);
- The input to the review should include information from but not limited to:
  - Feedback from business users
  - Change in the business

  - Change in the IT environment
  - Trends related to threat and vulnerabilities and
  - Reported security incidents and audit findings
- Records for the management review and approval shall be maintained by the Information System team.
- Recommendations provided by relevant authorities and/or other associated entities, both within and outside the organization, shall be part of the security policy review agenda.

# 6. Organization of Information Security

## 6.1 Internal Organization

### 6.1.1 Information Security Roles and Responsibilities

- All Information Security responsibilities, with regards to the protection of SPRL's information, Information Systems and information processing facilities shall be clearly defined through job descriptions, work allocation and delegation of tasks.
- The Information security policy, standards and procedures shall be approved by Chief Information Officer (CIO).
- The defined Information Security responsibilities shall be formally allocated and accepted across the organization. Such responsibilities shall include: -
  - Identifying the information assets and the security processes associated with each individual asset
  - Defining and documenting the asset ownership, the level of responsibility and authorization levels
  - Classification, labelling and handling of information assets in accordance with the established procedure;
  - Identification and implementation of controls that shall be termed necessary to adequately protect assets; and
  - Reviewing and approving user access privileges in accordance with the Access Control Policies & Procedures.

### 6.1.2 Segregation of Duties

- Roles defined to carry out business activities shall consider Segregation of Duties to reduce opportunities for deliberate or accidental misuse of infrastructure elements and/or software. E.g., ability to initiate, authorize, execute, and verify requests should be split so that no one person completes the entire request.
- Wherever Segregation of Duties is not possible, appropriate compensatory controls such as activity monitoring, audit trails and management supervision shall be developed to detect misuse of access rights.
- When primary personnel are not available (e.g., vacations, illness and leave of absence) and the role is filled in by another person with a different role, appropriate segregation and/or compensatory controls shall be considered; and
- Conflicting functions (e.g., functions with ability to initiate, authorize, execute and verify transactions) shall be identified and formally documented.

### 6.1.3 Contact with Authorities

- Appropriate contacts shall be established by the Information System and Legal & Regulatory Team respectively with law enforcement authorities, regulatory bodies, Internet Service provider (ISP), third party vendors, hardware vendors, software vendors, and office security providers.

### 6.1.4 Contact with Special Interest Groups

- Appropriate contacts shall be established by the Information Security Management Representative (ISMR) with special interest groups, forums, and professional associations related to Information Security to:

- o Improve knowledge about best practices and keep up to date with latest developments; and
- ○ Gain access to specialist Information Security advice.

### 6.1.5 Information Security in project management

- Information security shall be integrated into SPRL's project management methods to ensure that information security risks are identified and addressed as part of projects. The project management methods in use shall require that:
  - ○ Information security objectives are included in project objectives and overall organizations objectives.
  - ○ A project risk assessment is conducted at an early stage of the project to identify project risks; and
  - ○ Information security is part of all phases of the applied project methodology.
- Information security implications shall be addressed and reviewed regularly in all projects.

## 6.2 Mobile devices and Teleworking

### 6.2.1 Mobile device policy

- SPRL shall provision remote access for its employees to facilitate connection to network/application using mobile devices. Employees shall be given access to business information, only after successful identification and authentication.
- A secure communication channel between the remote user and the networks/Application of SPRL shall be provided.
- SPRL will ensure that the following steps are taken, basis the risk and asset value, to ensure business information on mobile equipment (e.g., laptops) is not compromised:
  - ○ Mobile phones used for sending / receiving SPRL mails shall have appropriate security controls in place
  - ○ Backup of emails solution shall be made available to the end users to ensure data availability
  - ○ Users shall be educated on risk of overlooking by unauthorized persons and how to mitigate them, and
  - ○ Users shall be educated about usage of mobile devices.

# 7. Human Resources Security

## 7.1 Prior to Employment

### 7.1.1 Screening

- Background verification checks shall be performed for all candidates considered for employment, in accordance with relevant laws, regulations and ethics.
  - o SPRL HR shall ensure that identified third party carries out all background verification checks in accordance with relevant laws, regulations, and ethics
  - o The checks shall include
    - Identity Check
    - Satisfactory character references
    - Previous employment check
    - Academic and professional qualification
    - Credit check, and
    - Criminal record check for sensitive positions for prospective SPRL employees.
  - o The background verification check process should ensure that all personal information is kept confidential, and the privacy of the prospective employee data is maintained in line with the Section18.1.4 “Privacy and Protection of Personally Identifiable Information”.

### 7.1.2 Terms and Conditions of Employment

- The terms and conditions of employment, signed by SPRL employees and third party, shall include their respective responsibilities for information security and related obligations, both during and after employment.
- All employees and third party who are given access to confidential information shall sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities.
- All SPRL employees and third party employees processing, storing or handling SPRL Information Assets shall be liable for any unauthorized disclosure, modification and/ or destruction of information.

## 7.2 During Employment

### 7.2.1 Management Responsibilities

The management will ensure that all employees and third party apply information security in accordance with the established policies and procedures of the organization. All employees and third party shall be properly briefed about their roles and responsibilities with respect to information security and the acceptable usage of SPRL information assets and processing facilities.

### 7.2.2 Information Security Awareness, Education and Training

- All employees shall be provided appropriate and relevant information security awareness training, regular updates on organizational policies, procedures and breaches.
- The HR department shall maintain records for the information security training and awareness session conducted for its employees. These records shall be stored in a safe place and be readily available for audit purpose.
- The HR team and Information Security Department work in conjunction for disseminating security awareness information to system users.
- The initial security training and awareness program shall be conducted as part of the induction process.
- The third party shall provide appropriate security awareness training to their employees and sub-contractors in line with SPRL Information Security Policy.

### 7.2.3 Disciplinary Process

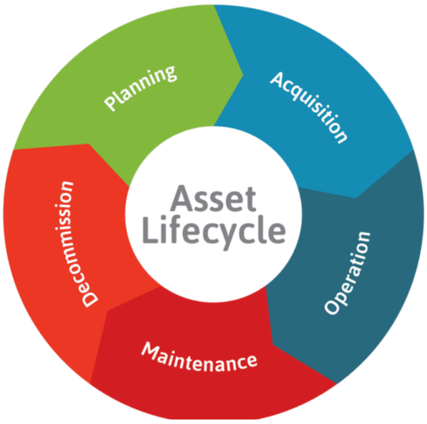
- SPRL shall ensure a comprehensive disciplinary process is in place for handling all kind of security breaches and cases of misconduct.
- The documented disciplinary procedure shall be applicable to all employees and third party in the event of an information security breach.

## 7.3 Termination and Change of Employment

### 7.3.1 Termination or change of employment responsibilities

- The responsibilities for performing employment termination and/or change of employment shall be defined, documented, and clearly communicated by the HR Head.
- Employment contracts / vendor agreements shall include the duties and responsibilities that shall be valid after the termination of such contract or agreement.
- Upon termination of duty/employment, all employees shall return / hand-over all information assets issued by the organization against their names.
- Information Security function shall ensure that, in case of any change in the responsibilities of the user, the access rights are revoked or modified as required. If the account is required to remain active, for any business reason, Information Security function shall obtain appropriate approvals from the Functional Head and ensure that passwords for such active accounts of a user are changed immediately on the departure of the user.
- The Information Security function shall ensure that the access rights of the users to information assets are revoked within twenty-four hours of separation of their employment, contract, or agreement; and
- In the case of change of employment, the access rights and/or privileges granted to employees and third party shall be formally reviewed and accordingly adjusted.

# 8. Asset Management



## 8.1 Responsibility of Assets

### 8.1.1 Inventory of Assets

- Each business function and third party shall be responsible for identification of Information Assets used for processing and storing information and they shall maintain an inventory of such assets; and
- For each of the identified assets, ownership of the asset should be assigned, and the classification should be identified
- All SPRL assets will be inventoried and tagged with a barcode. All SPRL user assets will be inventoried in Sapphire tool and all other corporate assets such as production servers, routers, and appliance hardware will be inventoried. Each asset will have a primary and secondary owner or point of contact in case of anything that happens to the device.
- All assets will be built and configured according to industry build standards such as CIS and will be scanned for vulnerabilities on a weekly basis by the Information Security department.

### 8.1.2 Ownership of Assets

- Asset Owner shall be identified for each asset within the asset inventory
- The owner shall be responsible for:
  - Ensuring that information and assets associated with information processing facilities are appropriately classified
  - Defining and periodically reviewing access restrictions and classifications, considering applicable access control policies
  - Information asset owners or their delegates shall be responsible for the following activities:
    - Approving information-oriented access control privileges for specific job profiles
    - Approving information-oriented access control requests that do not fall within the scope of existing job profiles
    - Selecting special controls needed to protect information, such as additional input validation checks or more frequent backup procedures
    - Defining acceptable limits on the quality of their information, such as accuracy, timeliness, and time from capture to usage
    - Approving all new or substantially enhanced application systems that use their information before these systems are moved into production operational status
    - Reviewing reports about system intrusions and other events that could lead to compromise of information; and
    - Selecting a security classification category relevant to their information and review this classification for possible downgrading or upgrading.
- Information owners shall not delegate ownership responsibilities to third-party organizations such as outsourcing organizations, or to any individual who is not a full-time employee of the company
- **Software Asset Management:** Software Asset management includes maintaining software license compliance; tracking the inventory and usage of software assets; and maintaining control over the deployment, and use of software assets. These include:
  - Procurement details, such as number of licenses acquired/purchased, expiry date of licenses, etc. The details shall be maintained, as a record, by the Information Systems team

- Data in the software inventory shall be synchronized with software purchase data e.g., date of purchase, expiry date of the license and number of licenses etc. Original physical or soft copy of the license received from the vendor, if any, on purchase shall be filed appropriately and stored securely
- Software usage and deployment shall be tracked and reconciled against purchase data every six months/annually
- Discrepancies, if any observed, shall be reported to the asset owner/team and the Information Systems team
- In case software license agreements are found to be violated, Information systems team shall initiate immediate actions to resolve/rectify the same
- Data relating to purchase of software shall be tracked and regularly monitored. Information Systems Head, along with respective asset/business owner of the applications, shall be responsible for conducting a review every six months/annually to determine, but not limited to, the following:
  - If licenses being used are more than purchased; and
  - If new software or more number of licenses are required to be procured for meeting future business requirements; and
  - Use of any unauthorized and unlicensed software. The unauthorized software shall be uninstalled, or a licensed version be procured.

### 8.1.3 Acceptable Use of Assets

- Acceptable use of assets associated with information processing facilities shall be clearly defined; and
- All users (employees and third party) who use or interface with assets associated with information processing facilities shall acknowledge their awareness of acceptable use of assets.

### 8.1.4 Return of Asset

- The Information Systems and HR function shall ensure that at the time of termination/ change of employment or change in the responsibilities or transfer of employee, all the assets belonging to SPRL are returned by the employee
- All employees shall return information assets that were issued to them during their tenure in SPRL; and
- Relevant Functional Heads dealing with the third-party employees shall ensure that at the completion of the assignment in SPRL or change in the responsibilities, third party employees return assets allocated to them such as corporate documents, equipment, mobile devices, software, access cards and/ or any other asset that is the property of SPRL.

## 8.2 Information Classification

### 8.2.1 Classification of information

- Information Assets and information processing systems shall be classified based on their business value, legal requirements, sensitivity and criticality to the organization
- Information Assets shall be classified as per established standard.

| Classification | Definition | Examples / comments |
|---|---|---|
| Public | Information/ assets (including information deemed public by legislation or through a policy of routine disclosure), available to the Public, all employees, contractors, sub-contractors and agents | There are no limitations on public information regarding creation, distribution, storing, disposal etc. It will therefore not be further covered in this guideline.<br>*Examples*: content on SPRL web site, advertisements, press releases and other informative material. |
| Internal | Information/assets that is sensitive outside the Company/Business and needs to be protected. Authorized Access to employees, contractors, sub-contractors, and agents on a "Need to Know Basis" for Business related Purposes. | Information that can be freely shared within the SPRL.<br>*Examples*: Local procedure and standards, technical and business experience/ knowledge, most projects, most meeting minutes etc. |
| Confidential | Information that is highly sensitive within the Company/Business and available only to a specific named individual (or specific positions), function, group or role | Information that should only be available to a limited number of people.<br>*Examples*: strategies, marketing and sales plans, technical information about networks, personal data for both customers and employees, encryption keys, traffic information etc. |

### 8.2.2 Labelling of Information

- All information shall be labelled as per the category it falls into
- If information is not marked with one of these categories, namely public, internal, or confidential it shall be taken, by default, to be classified as “Internal”
- The level of security provided to the information asset and information processing system shall be in accordance with the labelled category
- All storage media such as hard disks, CD/DVD etc. containing confidential information shall be labelled from the outside, in writing or through sticker, to indicate the category the asset falls into. If a storage volume such as a hard disk contains information with multiple classifications, the most sensitive category (Confidential) shall appear on the outside label

- Making additional photocopies or printing extra copies of information classified as confidential information will not take place without the prior permission of the information owner; and
- Confidential information on paper such as print outs, writing, fax etc. shall be personally delivered to the designated recipients. Such information shall not be delivered to an unattended desk or left in open or in an unoccupied office.
-

### 8.2.3 Handling of assets

- Asset owners shall ensure that information assets shall be appropriately handled.
- Handling and storage of information assets to protect this information from unauthorized disclosure or misuse shall be in accordance with the established standard.

## 8.3 Media Handling

### 8.3.1 Management of Removable Media

- If removable media is used (tapes, removable HDD, CDs, DVDs, USB, SD cards) to store SPRL information, adequate protection should be used by the Backup Admin to protect content on the media against unauthorized access, misuse, and corruption.
- Backup Admin shall be responsible for protection of Removable Media being used by them and shall ensure its storage under locked storeroom in their absence
- Back up Media/Tapes shall be disposed of securely and safely when no longer required.

### 8.3.2 Disposal of Media

- Media containing critical and sensitive information shall be disposed of securely when no longer required, using formal procedures.
- All shredder bins must always remain locked. Employees should make every effort to cross-cut printed material containing confidential or internal information before shredding it. If a shred bin is utilized, removal by an organization that specializes in document shredding must occur on a regular basis. In the event the shred bin reaches capacity prior to the next regularly scheduled pick-up, the shredding service must be contacted to schedule an emergency pick-up.
- Backup tapes will be destroyed after 12 months by a third-party service.

***Section 11.2.7 "Secure Disposal or Re-use of Equipment*" for details**

### 8.3.3 Physical Media Transfer

- Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond the organization's physical boundaries
- Logs shall be maintained, to track dispatch and receipt, for physical media transferred; and
- Authorized personnel and third-party agencies shall be identified for movement of electronic media and software applications from onsite location to offsite location.

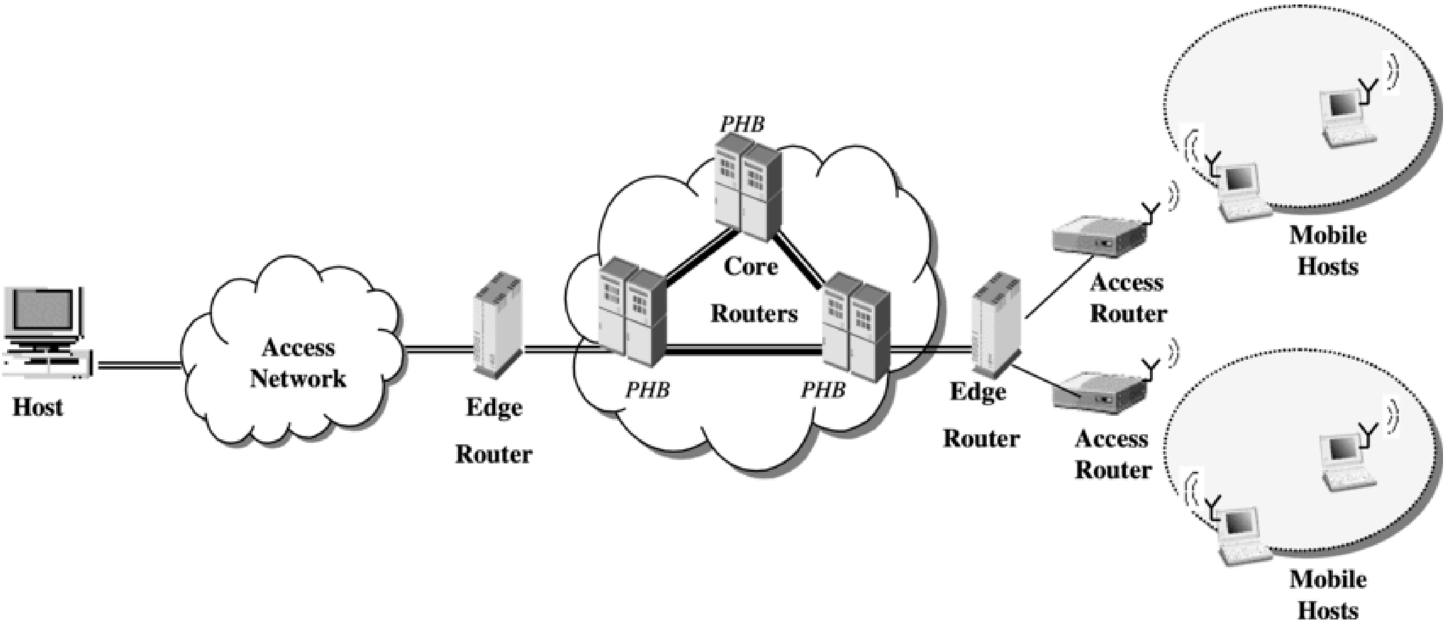
# 9. Access Control

## 9.1 Business Requirements of Access Control

### 9.1.1 Access Control Policy

- Access to any information processing assets and facility, operated or controlled by SPRL, shall be by authorization only. The IT HEAD shall be the highest authority in the company. SPRL employees can only authorize access to an information processing facility if the authority can be linked back to the IT HEAD in an unbroken chain;
- Physical and logical access to SPRL information processing facilities/ information assets shall be based on authorization against business & information security requirements
- Access requests should have at least two levels of verification and authorization. Requests for access shall be initiated by the individual and the rationale behind the request shall be documented
- Authorized person from SPRL hall monitor and grant the access requested. Access shall be restricted to the minimum resources or systems needed to accomplish the assigned work (least privilege);
- No single individual should have control over multiple steps in the access control process (Segregation of Duties). Whenever segregation of duties is not possible, appropriate compensatory controls like active monitoring, audit trail and management supervision shall be developed to detect misuse of access rights. Allocation of multiple roles with ability to initiate, authorize, execute, and verify transactions, all by the same person, if required for business reasons, shall be formally documented and approved
- A matrix mapping various roles and associated rights shall be maintained by owner of each access-controlled resource
- A valid audit trail shall be enabled for access control processes to ensure accountability for Users and Authorizers
- When the cost of administrating access is high and the associated risk is low, then group or default access can be applied even though not all member of the group need the level of access in their daily work. Group or default access can only be given after proper authorization by the resource owner
- Access to confidential information shall be granted only when a legitimate business need has been demonstrated and access has been approved by the information owner
- File access control permissions for all company networked systems shall be set to a default setting that blocks access; and
- User accounts which have data attached to them shall initially be disabled, not deleted, for employees/third party no longer working for SPRL. A mapping of User ID and associated access rights shall be maintained for all Users across all information processing facilities.

### 9.1.2 Access to Network and Network Services



- User access to applications / services (intranet, email, applications etc.) either remotely or locally shall be provided after authentication
- Users shall only have direct access to the services that they have been specifically authorized to use. Users shall not establish any external network connections that could permit third party users to gain access to company systems and information, unless prior approval though exception management process has been obtained; and
- When using company information systems, or when conducting company business, users shall not deliberately conceal or misrepresent their network identity.

## 9.2 User Access Management

### 9.2.1 User Registration and De-registration

- There shall be a formal and documented user registration and de-registration procedure in place for granting and revoking access to all infrastructure elements and software(s);
- Access control for application, servers, network, and tools in SPRL shall be based on the established access control procedure
  - o All regular and privileged accounts within SPRL domain shall be controlled and monitored centrally through means such as Active Directory
- Employees shall be distinguished from third party users in user directory and email systems
- All users shall have a unique identifier (user ID) for their own use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user
- Users shall be responsible for all activities that take place with their user ID and password or other authentication mechanism
- Any deviation from the mandatory User ID format must be approved as per defined exception management process
- For any third party, updated list mapping User IDs to individuals shall be maintained

- In exceptional circumstances, where there is a clear business benefit, the use of shared user ID for a group of users or a specific job can be used. However, such an arrangement shall have to be approved by an authorized individual and be recorded. Additional controls required to maintain accountability shall be assessed and implemented
- User creation/ modification request shall be authorized by the respective manager and submitted to Information Systems
- As part of de-registration process, user accounts which have data attached (e.g., email accounts) to them shall be initially disabled. The disabled accounts shall be deleted after a period of 30 days wherever applicable
- Authentication is mandatory for access to all infrastructure elements and software(s). Sites meant for public (e.g., SPRL Internet website) is exempted from this requirement.
- Strong authentication such as two factor authentication shall be considered wherever applicable
- Access credentials for employees and third party shall be handled by authorized personnel and transferred to the user only after proper identification; and
- Employment termination or change of roles shall trigger relevant processes for revoking or amending access rights. The defined processes shall outline steps to be taken in case of management-initiated termination based on disciplinary grounds. For third party it is the responsibility of the SPRL staff/team to trigger the relevant processes, not the concerned Service Provider employee.

### 9.2.2 User Access Provisioning

- The employees shall raise a request for accessing SPRL managed application, servers, and tools. The request for third party shall be raised by the respective point of contact, from different teams, handling them.
- The request shall then be sent to the Manager (of respective department to which the employee/ contract staff belongs) for approval. The Information security management representative may also approve the request, when needed.
- Based on the approval, from the Manager (of respective department to which the employee/ contract staff belongs) the Information Systems team shall grant access on the specified role(s).

### 9.2.3 Management of Privileged Access Rights

- Access to infrastructure elements, software(s), and data shall be given:
  - As per a defined process comprising of verification of the request and appropriate authorization. Multiple levels of authorizations (authorizations by multiple individuals or entities) should be considered for access to critical infrastructure elements and software(s); and
  - On a need to know, least privilege basis, and on the condition that it does not violate requirements of segregation of duties outlined in **Section 12.1.3 "Segregation of Duties".**
- A matrix mapping various roles and associated rights shall be maintained
- Employment termination or change of roles must appropriately trigger relevant processes for revoking or change of access rights. Also refer to ***Section 7.37.3 "Termination or Change of Employment";***
- Regular user activities shall not be performed using privileged user accounts; and
- Administrative / Super user privileges shall be limited to a limited number of users.

### 9.2.4 Management of secret authentication information of users

- Password management standard shall be defined and documented

- Passwords used by the employees and those set/provisioned on application and network devices must meet complexity requirements
- Users shall be educated to keep the passwords allocated to them confidential
- When granting access to infrastructure elements or software(s), users shall be provided with a temporary password that meets the password complexity requirements. Users shall be forced to change this password at first login and shall be unique for each user
- Temporary passwords should be given to users in a secure manner
- Procedure shall be defined to process password reset requests. The procedure shall ensure that the identity of the user is verified prior to processing the request. The new password shall be securely delivered to the users
- Default vendor passwords shall be changed; and
- For additional requirements refer to ***Section 99.4.3 "Password Management System".***

### 9.2.5 Review of User Access Rights

- There should be a periodic reconciliation of user accounts and the associated rights. The periodicity of the reconciliation must be at least quarterly. The period of reconciliation may be less than once a quarter depending on the criticality of the infrastructure element or software; and
- A review to identify the inactive or dormant user IDs shall be conducted at regular intervals (at least once every quarter). Dormant or inactive user IDs that are no longer required shall be removed / disabled as appropriate.

### 9.2.6 Removal or adjustment of Access Rights

- Process shall be defined to ensure that access rights associated with the employees, and third-party personnel are revoked upon termination of their employment, contract, or agreement;
- The defined processes must also outline steps to be taken in case of management-initiated terminations based on disciplinary grounds; and
- If there is a change of role, necessary changes/adjustments shall be made so that the user does not have more rights than required to carry out the new job function.
- The removal or modification of access rights for terminated SPRL employees or contract staff shall be carried out by the relevant team.

## 9.3 User Responsibilities

### 9.3.1 Use of secret authentication information

- Users shall be made aware to follow good security practices in the selection and use of passwords
- This shall also be covered through Security Awareness Sessions as per ***Section 7.2.2"Information Security Awareness, Education and Training"***; and
- Wherever possible the strong password policy shall be enforced at the system or application level.

## 9.4 System and Application Access Control

### 9.4.1 Information Access Restriction

- Access to information and application system functions by users and support personnel shall be restricted in accordance with principles outlined in ***Section 9.1.1 "Access Control Policy"*** and ***Section 6.1.2 "Segregation of Duties".***

### 9.4.2 Secure Log-on Procedures

- All users shall be authenticated before they are granted access to application and operating system;
- The log-on procedure should disclose minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance. Following should be considered while defining the log-on procedures:
  - If the login is unsuccessful, the error message should not display which part of the login information was incorrect
  - Limit the number of unsuccessful log-on attempts
  - Password should not be displayed while it is being entered; and as far as possible login information shall not be sent in clear text over the internal SPRL network.

### Session Time-out

- Inactive sessions (Application sessions, VPN sessions, Administration Sessions etc.) shall be shut down where feasible after a defined period of inactivity Intranet site may be exempted from requirement of session time out and Limitation of Connection-time

- Depending on the risk, restrictions on connection times to infrastructure elements and software(s) may be considered to reduce the opportunity of unauthorized access; and
- Re-authentication may be considered at timed intervals.

### 9.4.3 Password Management System

- Systems for managing passwords shall:
  - Force users to change temporary passwords at first log-on
  - Allow user to change the password
  - Enforce strong passwords
  - Enforcement of password history to prevent re-use; and
  - Store passwords in a protected form (e.g. encrypted or hashed).

### 9.4.4 Use of Privileged Utility programs

- The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

### 9.4.5 Access Control to Program Source Code

- SPRL has decided to exclude the applicability of this clause for its assessment in 2016. The statement of applicability states this clause is not applicable to the current scope.

# 10. Cryptographic Controls

## 10.1 Policy on the Use of Cryptographic Controls

### 10.1.1 Policy on the Use of Cryptographic Controls

- Cryptographic algorithms used should not have any known weaknesses
- Key strength used should be sufficient to prevent attacks targeted to breaking the cryptographic key (e.g. brute force attack on the cryptographic key);

- Third party commercial CA’s shall be considered for Internet facing applications that are accessed by non-SPRL community (e.g. customers) or from non- SPRL systems; and
- Legal & regulatory requirements (as applicable) of cryptography controls shall be complied with.

### 10.1.2 Key Management

- To ensure that the confidentiality of the secret key is protected, it shall be secured by logically and physically securing the device on which the key is stored
- The shared secret key shall be accessible only by authorized personnel on a need-to-know basis
- Keys shall be revoked and generated afresh in case of suspected compromise
- Audit trails of key management activities shall be stored and protected
- Internal CA systems shall be managed securely with appropriate physical and logical controls
- Secure backup of internal CA private keys shall be maintained on an independent secure media which provides a source for key recovery. Backed up keys shall be protected from physical and environmental threats.
- Cryptographic keys shall be destroyed in a secure manner when they are no longer required
- No copy of user’s private key shall be retained by the internal CA to avoid risk of repudiation
- Users shall keep their private keys strictly confidential and shall be responsible for the safety of their private keys.

# 11. Physical and Environmental Security

## 11.1 Secure Areas

### 11.1.1 Physical Security Perimeter

- Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities; and
- A manned reception area to control physical access to the site or building shall be in place.

### 11.1.2 Physical Entry Controls

- Appropriate entry controls shall be implemented to ensure that only authorized personnel are allowed access to locations storing and processing SPRL information.
- Physical access control shall be supported by an electronic access control system
- User identification and authentication shall be based on User ID access cards (with or without photo). ID access cards without photograph shall only be issued to visitors. Employees, third party staff, and visitors must display User ID access cards given to them;

***Section 9.1.1 “Access Control Policy”***

### 11.1.3 Securing Office, Room, and Facilities

SPRL shall ensure that

- key facilities are sited to avoid access by the public
- The buildings occupied by its employees or information processing assets should be unobtrusive and give minimum indication of their purpose with no obvious signs, outside or inside the building, identifying the presence of information processing activities
- Facilities are configured to prevent confidential information or activities from being visible and audible from the outside

- Directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.

### 11.1.4 Protecting Against External and Environmental Threats

- SPRL shall ensure that critical information processing facilities are appropriately equipped and maintained with security controls to safeguard against external and environmental threats

### 11.1.5 Working in Secure Areas

SPRL shall ensure that  Employees and third-party resources are aware of the existence of, or activities within, a secure area on a need to- know basis All areas within its facilities are supervised to avoid safety breaches and to prevent opportunities for malicious activities Vacant secure areas should be physically locked and periodically reviewed Only authorized video, audio, or other recording equipment (such as camera or camcorders) devices, are allowed inside the facility with proper monitoring of their movement.

### 11.1.6 Delivery and Loading Areas

- Delivery and loading areas, as well as other publicly accessible areas shall be appropriately isolated from information assets and information processing facilities.

## 11.2 Equipment

### 11.2.1 Equipment Sitting and Protection

- Equipment’s shall be protected from security threats and environmental threats in line with its criticality and classification defined.
- Adequate air conditioning equipment shall be installed to ensure the information assets are protected from environment threats
- Supporting equipment such as photocopiers, printing devices and fax machines shall be protected from unauthorized physical access
- Consumption of eatables and beverages inside all areas containing information processing equipment shall be prohibited; and
- Storing of flammable objects within all areas containing information processing equipment is also prohibited.

### 11.2.2 Supporting Utilities

- Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities Air-conditioning and humidity control systems to support information systems and equipment shall be deployed  Flood protection or water detection measures shall be implemented
- Appropriate fire protection measures shall be implemented, including installation of fire-suppression systems in areas such as data centers; and Adequate power supply controls shall be implemented to ensure continuous power supply.

### 11.2.3 Cabling Security

- SPRL shall define and implement appropriate cabling standards for data networking, electric power and telecommunications cables, Network cables, power cords, patch cables, shall be uniformly marked, color coded and labelled in accordance with the cabling standards Network cabling shall be appropriately protected from unauthorized access, interception, damage and/or interference Power and telecommunications cabling shall be appropriately protected from damage and/or disruption; and Access to patch panels and cabling rooms (if separate) / cabinets shall be controlled.

### 11.2.4 Equipment Maintenance

- To ensure continued availability and integrity maintenance activity shall be carried out at regular intervals by trained and authorized personnel All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning, shall be in appropriate condition for the information systems and/ or facilities that they are supporting Uninterruptible power supply (UPS) systems and generators shall be installed to support controlled shutdown or continued functioning of equipment supporting critical business operations.

- An alarm system to highlight the malfunctions in the supporting utilities shall be installed A preventive maintenance exercise for the utility equipment shall be carried out at scheduled intervals ensuring their continued availability and integrity A review of preventive maintenance shall be conducted All equipment shall receive appropriate level of protection against environmental threats; and A record shall be kept for all faults (suspected or actual). The record shall also capture corrective and preventive actions along with root cause analysis.

### 11.2.5 Removal of assets

- Equipment, information containers or software (such as DVD/CD/HDD etc.) shall not be taken off-site without prior authorization The removal of equipment, information assets, software, materials or supplies from SPRL information processing facilities shall be inspected and recorded.
- Such removal records shall be maintained and periodically reviewed Removal records shall include items removed on a temporary basis and items removed for repairs Physical asset verification checks shall be periodically performed, to detect unauthorized removal of property from SPRL premises.
- Process shall be defined to ensure equipment being taken off-site for maintenance is approved by authorized personnel and track return of temporary outward movement of equipment (returnable equipment); and
- Mobile devices specifically issued to authorized users are exempted from this requirement.

### 11.2.6 Security of Equipment and assets Off-premises

- Any equipment taken off from premises storing and processing SPRL information for maintenance purposes shall be adequately protected
- Suitable logical access and/or physical access controls shall be identified and implemented to protect the information asset; and Insurance cover may be considered for equipment off-site.

### 11.2.7 Secure Disposal or Re-use of Equipment

- Back up/storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal
- Processes shall be defined to ensure that all information is wiped off the storage media / systems before it is disposed or re-used; and
- Controls implemented to wipe information shall be commensurate with the classification of information on the storage media / systems.
- A programmatic (automatic) process shall be executed on database systems to remove all sensitive and confidential data that exceeds business retention requirements.
- Other applicable data stored in files and directories, where the containing media will be re-used, shall be deleted securely by a “wiping” utility approved by the Information Security Department.
- Media containing confidential or sensitive data that should no longer be retained must be disposed of in a secure and safe manner as noted below:
  - Hard disks: sanitize (7-pass binary wipe), degauss or shred platter.
  - Floppy disks: disintegrate, incinerate, pulverize, shred or melt.

  - Tape media: degauss, shred, incinerate, pulverize, or melt.
  - USB “thumb” drives, smart cards, digital media: incinerate, pulverize, or melt.
  - Optical disks (CDs and DVDs): destroy optical surface, incinerate, pulverize, shred or melt.
- SPRL shall ensure that before information system/device such as computer or communications equipment are sent to a vendor for trade-in, servicing, or disposal; all confidential information shall be destroyed or concealed.
- Outsourced destruction of media containing confidential information must use a bonded Disposal Vendor that provides a “Certificate of Destruction”.

#### 11.2.8 Unattended User Equipment

- Appropriate security measures such as password protected screen savers or key locks, automated termination of active sessions, etc. shall be adopted by the users to protect the unattended equipment.

#### 11.2.9 Clear Desk and Clear Screen Policy

- A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted
- All confidential information shall be kept in a secure office or other location e.g. storage in a locked drawer, file cabinet etc.;
- All incoming and outgoing mail points and unattended facsimile machines shall be protected from unauthorized physical and logical access
- Personal computers, laptops and printers shall be left logged off or protected by a password, token, or similar user authentication mechanism when unattended
- Password-protected screen savers shall be activated within 15 minutes of user inactivity
- Application sessions shall be locked after 30 minutes of inactivity until a user’s password is re-entered
- Users shall log off or lock their personal computers when leaving it unattended for any period; and
- Users shall turn off personal computers or log off all network resources at the end of each day.

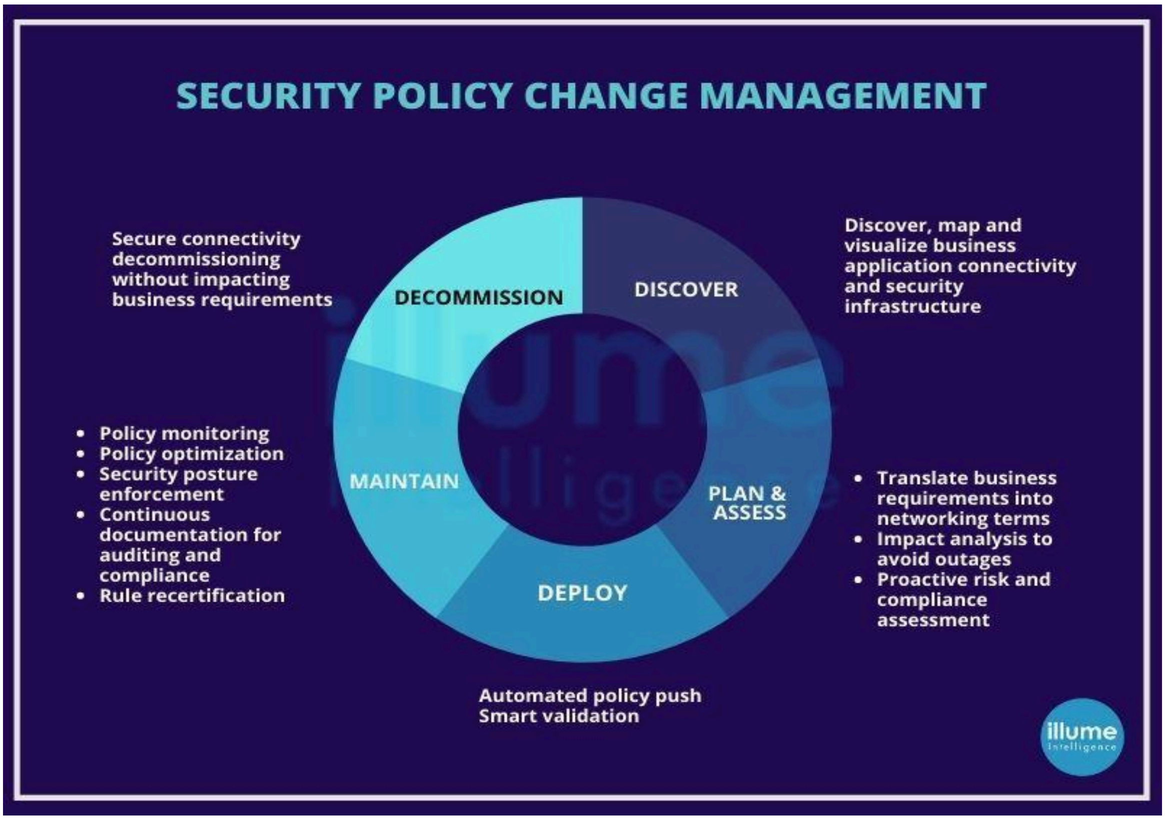
## 12. Operations Security

### 12.1 Operational Procedures and Responsibilities

#### 12.1.1 Documented Operating Procedures

- Respective teams shall ensure that all relevant documentation including software details is obtained from manufacturer/vendor/supplier
- Following documents shall be made available to the relevant people manning the operations:
  - Operations and Maintenance procedure or standard operating procedure (SOP) for all operational activities including security requirements
  - SOP shall be developed by respective teams for operation and maintenance of assets
  - SOP shall be developed to handle supply chain of products (hardware and Software) along with retention schedule for the records
  - Network diagrams and other supporting documents outlining interconnectivity details between various infrastructure elements. E.g., address, device name, neighboring device(s) etc.; and
  - Product and user manuals including recovery documents.

### 12.1.2 Change Management


SECURITY POLICY CHANGE MANAGEMENT
DECOMMISSION
DISCOVER
PLAN & ASSESS
DEPLOY
MAINTAIN
Secure connectivity decommissioning without impacting business requirements
Discover, map and visualize business application connectivity and security infrastructure
Translate business requirements into networking terms
Impact analysis to avoid outages
Proactive risk and compliance assessment
Automated policy push
Smart validation
Policy monitoring
Policy optimization
Security posture enforcement
Continuous documentation for auditing and compliance
Rule recertification
illume intelligence

- Changes to information processing facilities, systems and applications including software updates shall be controlled and recorded
- There shall be a documented Change Management Process to handle scheduled and emergency changes
- The change request shall at least include the following:
  - Affected Asset Name
  - Change Description
  - Reason for Change
  - Business impact of the change
  - Expected date of completion
  - Change Approval Board approval; and
  - Comments (if any).
- Major software updates and changes shall be informed to licensor within stipulated time
- Following steps shall be carried out for changes to information processing facilities, systems and applications:
  - Identification and recording of significant changes
  - Planning of changes
  - Assessment of the potential impacts, including security impacts
  - Testing of changes wherever applicable, testing shall not be performed by the change developer

  - After approval of test reports the changes shall be implemented in production environment by the information systems team
  - Formal approval procedure for proposed changes. All Major/Minor/ Normal changes shall be approved by CAB (Change Advisory Board). Scheduled changes may be pre-authorized
  - Communication of change details to all relevant persons; and
  - Fall-back procedures, including procedure and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events. Administrator shall maintain previous versions of software or configuration files. Backup of the database shall be taken before copying the change to production or live environment.
- In case of emergency changes:
  - The approval may be sought verbally from ECAB (Emergency Change Advisory Board) followed by an e-mail; and
  - The emergency change details shall be recorded post implementation with the relevant approval details.
- The CAB (Change Advisory Board) shall:
  - Review and approve major Change Requests
  - Review all emergency changes which are major or critical implemented since last CAB meeting; and
  - Discuss any unauthorized changes implemented, if any.

### 12.1.3 Capacity Management

- Critical parameters and their thresholds shall be monitored for all critical infrastructure elements and software(s) at periodic intervals to ensure required performance levels and availability
- Capacity planning shall take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.
- The periodicity of capacity review shall be defined taking into consideration the criticality of the infrastructure element, lead time / costs to procure replacement, and the parameter being monitored
- System tuning and monitoring shall be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time.
- Outcome of the monitoring activity shall:
  - Be used to take corrective actions (if required);
  - Help in root cause analysis (if required); and
  - Be used to make projections of future capacity requirements to reduce the risk of system overload.

## 12.2 Protection from Malware

### 12.2.1 Controls against Malware

- Anti-Malware tools, associated procedures, and other relevant controls like user awareness shall be implemented to efficiently detect, prevent, and recover against Malwares
- Appropriate protection shall be enforced so that the users cannot disable the Anti-virus check
- Anti-Virus software and associated signature files shall be kept up to date
- Use of unauthorized software shall be prohibited.
- Controls shall be implemented to prevent malware files from being introduced into the SPRL infrastructure from external networks like Internet; and
- Upon encountering a virus attack, users shall immediately stop using the involved desktop/laptop and/ or any other computer system and report it to Information Security team.

## 12.3 Back-up

### 12.3.1 Information Backup

- Backup solution shall be defined to meet the business requirements and ensure availability of business-critical information, software(s), device configurations in case of emergencies
- Relevant documented processes / procedures shall be created and followed to meet the business requirements. The process / procedures shall define:
  - Frequency for taking backup and testing of backup through a restoration process
  - Data to be backed up
  - Type of backup (incremental, differential, full)
  - Testing procedure for ensuring that the backup media can be relied upon in case of emergency. Backup Data shall be periodically restored for relevant systems wherever possible, Split test should be done and the results be recorded. In case the restoration test fails, the data owner would be notified regarding the same. Root Cause Analysis for such failure would be carried out as per the incident management procedure
  - Instructions to restore in case of an actual disaster; and
  - Retention period for backup.
- Adequate controls shall be put in place to ensure protection of backup media. The environmental conditions for storing the backup media shall be in line with the specifications on environmental conditions for the backup media
- The backup media shall be labelled to a consistent standard
- Adequate controls shall be put in place to protect the information contained on back up media
- Backup results shall be recorded. In case the backup fails, root cause analysis shall be performed as per the incident management procedure; and
- Offsite storage may be considered to meet the business requirements. However, if used, then appropriate controls shall be implemented to protect the backup media and the data contained on it. For additional instructions on physical media in transfer refer to ***Section 8.3.3 "Physical Media in Transfer"***.

## 12.4 Logging and Monitoring

### 12.4.1 Event Logging

- Infrastructure elements and software(s) (applications, databases, operating systems etc.) that are used for SPRL operations shall be configured where feasible to capture security relevant logs (e.g., use of privilege accounts like root and administrator accounts, system failures, policy violations, unauthorized access attempts, logging of firewall traffic etc.).

### 12.4.2 Administrator and Operator Logs

- System administrator and system operator activities shall be logged and protected against unauthorized modification.

### 12.4.3 Protection of Log Information

- Logs shall be securely maintained for a minimum period stipulated as per applicable laws and regulations so as to provide support for investigations of incidents; and
- Logging facilities and log information shall be protected against tampering and unauthorized access.

### 12.4.4 Clock Synchronization

- All infrastructure elements must point to the same Network Time Protocol (NTP) source and the same time zone.

## 12.5 Control of Operational Software

### 12.5.1 Installation of Software on operational systems

- Installation of new software and changes to existing software on production systems shall be in line with
  - Changes are authorized and made by authorized personnel only
  - Production systems hold only approved code and not development code
  - Implementation happens only after required level of testing
  - System documentation is updated; and
  - Roll back plan is available.
- The risks of relying on unsupported software (software for which support has been ceased by the vendor) for business-critical applications shall be considered.

## 12.6 Technical Vulnerability Management

### 12.6.1 Management of Technical Vulnerabilities

- Timely information about technical vulnerabilities in infrastructure elements and software(s) being used shall be obtained from trusted sources (e.g., through subscription to vendor security advisories)
- Timelines shall be defined for responding to identified / reported technical vulnerabilities
- Information obtained regarding vulnerability shall be evaluated to assess risk to SPRL's/Third party infrastructure. The evaluation shall take into consideration:
  - Vendor reported criticality (e.g., high, medium, and low);
  - Likelihood of the vulnerability being exploited (e.g., existence of a known exploit or other malicious code that uses the vulnerability as an attack vector)
  - System criticality (e.g., the relative importance of the applications and data the system supports at SPRL); and
  - System exposure (e.g., proxy server vs. internal file server vs. application servers).
- The identified risk shall be categorized as per the severity of the risk (e.g., High, Medium, and Low);
- Appropriate measures shall be taken to address the associated risks. If the vulnerability cannot be addressed, controls shall be considered to reduce the impact of risk
- If the vulnerability closure requires patch deployment, the patch must be tested in a test environment before deployment to production environment. The test environment should closely simulate the production environment and if possible, the test should verify the patch does not conflict with other software(s). The patch deployment must go through change management process with a rollback plan
- To assist with technical vulnerability management, inventory of Infrastructure elements and software assets shall be maintained
- Tool based vulnerability scans shall be carried out for all critical infrastructure elements
- The system should be checked to verify if the patch has not affected any of the existing functionality; and
- After applying the patch/solution for high-risk vulnerabilities, a check shall be performed to ensure that the vulnerability has been closed.

### 12.6.2 Restrictions on software installation

- SPRL shall ensure that adequate controls are in place to restrict the installation of software on the information processing systems. Only the system administrator/ authorized personnel from Information systems team shall have the access rights to install new software on the system. Approvals shall be taken by the employee for installing software that is needed for work purposes.

## 12.7 Information Systems Audit Considerations

### 12.7.1 Information Systems Audit Controls

- Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes
- Risk based approach shall be adopted to arrive at the scope of the audit
- Where system audits require access to production system or data or includes the use of software tools and utilities, such audits shall be conducted with the knowledge, cooperation, and consent of the owners of the information systems and Relevant precautions shall be taken to protect the Information Systems and data from damage or disruptions as result of the audit.

# 13. Communications Security

## 13.1 Network Security Management

### 13.1.1 Network Controls

- Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit
- Critical infrastructure elements within IT network that support AAA (Authentication, Authorization, and Accounting) integration should be configured for AAA
- Infrastructure elements and software(s) exposed to un-trusted or semi trusted networks/users (e.g. internet facing systems, third party etc.) shall be adequately protected by firewalls and limited connectivity;
- All Internet facing systems shall be treated as semi-trusted systems
- Any server deployed on the internet must go through a thorough vulnerability check. All identified vulnerabilities must be closed or mitigated before the server is deployed on the Internet.
- IT infrastructure elements shall be hardened as per documented and approved hardening procedures before connecting to the SPRL production infrastructure.
    - Administrators / custodians of the infrastructure elements shall be responsible for:
        - Developing documented and approved hardening procedures for all types of infrastructure elements and software versions; and
        - Review of documented hardening procedures at least annually or when there this is a major change in the software versions / models of the infrastructure elements.
    - All configurations must be done by trained and authorized personnel; and
    - Vulnerability Assessment of these infrastructure elements shall be carried out as per “Technical Vulnerability” section of this policy.
- Wireless may be used for SPRL business communications provided it meets the requirements outlined.
- All end user systems connecting to the SPRL infrastructure must be hardened, patched, and installed with updated anti-malware software
- Permission to connect other networks and computer systems in company’s network shall follow exception management process.
    - End user systems used by IT vendors to manage SPRL infrastructure elements and software(s) shall be configured as per SPRL security policies for end user systems.

### 13.1.2 Security of Network Services

- Security features, service levels, and management requirements of all network services shall be identified and included in the form of an agreement as outlined in ***Section 15.1.2 "Addressing security within supplier agreements"***.

### 13.1.3 Segregation in Networks

- Group of users, systems, applications shall be adequately segregated through creation of Virtual LANs, to prevent unauthorized access; and
- Appropriate logical segregation shall be done between and within IT, Network, and Physical Security infrastructures through creation of zones.

## 13.2 Information transfer

### 13.2.1 Information transfer policies and procedure

- Information transfer guidelines shall be captured in Acceptable Usage Standard and users shall be made aware of these guidelines
- Audio conference setup shall support use of PIN/Authentication code to join the conference
- It should not be possible to send mails to non-SPRL domains from multifunction peripheral devices (e.g. faxes, printers etc.);
- PIN protection is recommended to be put in place on printers being used to handle confidential and internal information
- Risks associated with page caching and storage in multifunction peripheral devices shall be addressed through relevant controls; and
- Wherever possible, business functions shall use only officially appointed courier service providers for transmitting physical information.

### 13.2.2 Agreements on information transfer

- Agreements and relevant controls shall be established for the transfer of information and software between SPRL and Third party and shall be included in the formal agreement suggested ***in Section 15.1.2 "Addressing Security within Supplier Agreements"*** of this document.

### 13.2.3 Electronic Messaging

- Information involved in electronic messaging (e.g. emails, instant messengers) shall be appropriately protected from unauthorized access, modification or denial of service;
- Public email accounts and public instant messengers shall not be used for conducting SPRL operations, unless authorized
- Details on acceptable use of email and instant messengers are captured in Acceptable Usage Standard; and
- Forwarding of SPRL mailbox to public or non- SPRL email accounts shall be allowed only after authorization.

### 13.2.4 Confidentiality or non-disclosure Agreements

- Non-disclosure agreements shall be defined, implemented, and maintained to address SPRL's information confidentiality/ non-disclosure requirements.

- All employees shall sign and comply with the non-disclosure agreement maintained by the SPRL's Human Resource Team.
- All third parties shall sign and comply with non-disclosure agreement.

# 14. System Acquisition, Development and Maintenance

## 14.1 Security Requirements of Information Systems

### 14.1.1 Information Security Requirements Analysis and Specification

- Information Security requirements to ensure confidentiality, integrity and availability shall be identified before procuring a new infrastructure element or software or upgrading an existing setup
- SPRL shall ensure that contemporary security features and features related to communication security are included at the time of procurement of equipment and implement the same
- SPRL shall ensure that details of features, equipment, software etc. procured and implemented are maintained till they are in use; and

### 14.1.2 Securing applications services on public networks

- If applicable, information involved in electronic commerce passing over the public network shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. Risk shall be identified for data passing over the internal SPRL network and appropriate controls shall be deployed depending upon the risks
- Customer related data shall be protected in accordance with applicable industry, regulatory and legislative directives
- If applicable, the integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification; and
- All publicly available systems shall be tested against for vulnerabilities, and it shall be ensured that the identified vulnerabilities are fixed prior to publishing any information in such systems.

### 14.1.3 Protecting application services transactions

- If applicable, information involved in application services transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

# 15. Supplier Relationships

## 15.1 Information Security in supplier relationship

### 15.1.1 Information security policy for supplier relationships

- Information security requirements for mitigating the risks associated with supplier's access to SPRL's assets shall be agreed with the supplier and documented in the form of agreements or contracts.

### 15.1.2 Addressing security within supplier agreements

- All agreements with Third party that access, process, communicate or manage SPR information or information processing facilities, or provide products or services shall have relevant security requirements embedded in them

- If any aspect of SPRL operation is further outsourced to a sub-contractor by the Third party, agreement with Third party and sub-contractor shall cover relevant security controls and requirements. Following controls shall be considered:
  - Approval shall be taken from SPRL (if required) Risks to the SPRL operations shall be identified and appropriate steps be taken to mitigate the identified risks Appropriate steps shall be taken to ensure that the sub-contractor complies with security requirements outlined in this document and other relevant security requirements; and Suitable agreements shall be drafted to ensure Information Security requirements are addressed through them.

### 15.1.3 Information and communication technology supply chain

- Agreement with suppliers shall include requirements to address the information security risks associated with information and communication technology services and product supply chain.

## 15.2 Supplier service delivery management

### 15.2.1 Monitoring and Review of supplier Services

- Key Performance Indicator (KPI) framework shall be defined for monitoring effectiveness of Information Security. Depending on the nature of engagement with the Supplier, following shall be agreed with the Supplier to monitor Information Security effectiveness and ensure compliance to Information Security terms and conditions within agreements:
- Reports and Key Performance Indicators (KPIs) to be shared by the Supplier; and Frequency of sharing agreed reports and KPIs. Periodic audits shall be carried out to ensure compliance to Information Security terms and conditions within agreements with the supplier; and Supplier operations shall be monitored through a security governance program including all the above aspects.

### 15.2.2 Managing Changes to supplier Services

- Significant changes to supplier services (e.g. enhancement to networks, new technologies, new products or newer versions, change of vendors, change of physical location etc.) shall be informed to the Information Systems team; Such changes shall:
  - Consider criticality of business systems and processes involved; and Be accompanied by re-assessment of risks.

# 16. Information Security Incident Management

## 16.1 Management of Information Security Incidents and Improvements

### 16.1.1 Responsibilities and Procedures

- Information Security incident management standard for SPRL shall define procedures and responsibilities to ensure quick, effective, consistent, and orderly response to Information Security Incidents reported.
- Information Security team shall appointed a team member for:
  - Investigation / co-ordination of the reported Information Security incidents and Security weaknesses; and
  - Tracking closure of identified corrective and preventive actions.

### 16.1.2 Reporting Information Security Events

- Information Security events shall be reported through email to the IS team. The mails shall be sent to
  - **admin@Shrirampistons.com and Ithelpdesk@Shrirampistons.com**
- All Information Security events shall be recorded in an Information Security incident database Facility for monitoring (like Security Operations Centre) shall be setup for proactive monitoring of intrusions, attacks,

and frauds; and User community shall be educated on how to identify and report Information Security events.

### 16.1.3 Reporting information security weakness

- Information Security weaknesses, both actual and suspected, shall be reported through different channels like email, phone line, and intranet. In addition, users shall not test the existence of vulnerability in any information facility, system or application; and Centralized database shall be maintained of all reported Information Security weakness.

### 16.1.4 Assessment of and decision on information security events

- Information security events shall be assessed, and it should be decided if they are to be classified as information security incidents. If required, the SPRL Information Security department shall have the necessary rights to access the systems and applications for forensic purposes; and All such incidents shall be classified as per the classification criteria mentioned in the incident management standard.

### 16.1.5 Response to information security incidents

- The overall response to reported incidents shall include identification of corrective action(s); Where a follow-up action against a person or organization after an Information Security Incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s); and Existence of information security incident shall be communicated to the internal people, external people and other interested parties related to SPRL.

### 16.1.6 Learning from information security incidents

- Analysis shall be carried out for the Information Security Incidents considering the following factors:
- Type of Information Security Incident Volume of Security Incidents; and Wherever possible, costs incurred due to Information Security Incidents. The output of the analysis shall be used to improve the security posture.

### 16.1.7 Collection of Evidence

- Where a follow-up action against a person or organization after an Information Security Incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s); and Existence of information security incident shall be communicated to the internal people, external people and other interested parties related to SPRL.

**SPRL-ISMS-Std-Incident Management Standard-1.0**

# 17. Information Security Aspects of Business Continuity Management

## 17.1 Information Security Continuity

### 17.1.1 Planning Information Security Continuity

- The organization-wide Information security processes shall include Information Security requirements to help ensure that confidentiality, integrity and availability of critical information assets shall be preserved even in the event of a business disruption or disaster. SPRL A strategy plan, based on appropriate risk assessment, shall be developed for the overall approach to information security.

### 17.1.2 Implementing Information Security Continuity

- SPRL shall ensure that an adequate framework is in place to prepare for, mitigate and respond to a disruptive event using personnel with necessary authority, experience, and competence SPRL shall identify personnel with necessary responsibility, authority, and competence to manage an incident and maintain information security; and SPRL shall ensure that documented plans, response and recovery procedures are developed and approved, describing how SPRL will manage a disruptive event and maintain its information security at a predetermined management approved information security continuity objective.

### 17.1.3 Verify, Review and Evaluate Information Security Continuity

- Information security controls for all business continuity sites and systems shall be reviewed and verified. Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective each calendar quarter, emergency contact information shall be validated and revised; and The roles and responsibilities for both information systems contingency planning and information systems recovery shall be reviewed and updated annually.

## 17.2 Redundancies

### 17.2.1 Availability of Information Processing Facilities

- SPRL shall identify business requirements for availability of information systems
- Redundant components or architectures shall be considered wherever availability cannot be guaranteed using the existing systems architecture; and
- Redundant information systems shall be tested to ensure the successful failover from one component to another.

# 18. Compliance

## 18.1 Compliance with Legal and Contractual Requirements

### 18.1.1 Identification of applicable legislation and contractual requirements

- The legal/regulatory department at SPRL shall be responsible for communicating changes to any of the above areas and additional security requirements
- Necessary measures shall be taken to prevent the following types of content from being carried over the SPRL network in any form:
  - Objectionable, obscene, unauthorized content
  - Content, messages, or communications infringing copyright, intellectual property etc.; and
  - If instances of such infringement are reported by the enforcement agencies, it shall be ensured that transmission of such material on the network is prevented immediately.

### 18.1.2 Intellectual Property Rights (IPR)

- The software used must be acquired from legitimate (known and reputable sources) to ensure copyright is not violated
- Proof and evidence of ownership of licenses, master disks, manuals etc. shall be maintained
- Controls shall be implemented to ensure maximum number of users permitted to use the software is not exceeded
- Only authorized software and licensed products shall be installed; and
- Copying, storage, duplicating, converting to another format, extracting of electronic content (eBooks, media files, articles, reports etc.) must not violate copyright laws.

### 18.1.3 Protection of Record

- Important records required for meeting statutory and regulatory requirements shall be identified and their retention periods defined
- Each department having ownership of such records shall ensure that these records are protected from loss, destruction, unauthorized disclosure, and falsification
- All sensitive and confidential data, regardless of storage location, will be retained only as long as required for legal, regulatory and business requirements

### Data Disposal

All confidential or sensitive electronic data, when no longer needed for legal, regulatory, or business reasons, shall be removed from SPRL systems by using approved methods documented in this policy. This requirement includes all data stored in system and all temporary files, as well as storage media.

### 18.1.4 Privacy and Protection of Personally Identifiable Information

- SPRL shall ensure Privacy and protection of personally identifiable information as required by the relevant legislation and regulations.

### 18.1.5 Regulation of Cryptographic Controls

- Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

## 18.2 Information Security Reviews

### 18.2.1 Independent Review of Information Security

- Audits of operational information systems shall be planned and performed at periodic intervals with the agreement of the information systems' owner so as to minimize the risk of disruption to business processes; and
- Independent audits of information security management system shall be performed as per the planned intervals or when significant changes occur.

### 18.2.2 Compliance with Security Policies and Standards

- Continued compliance with SPRL's Information Security policies and procedures shall be maintained.
- Any detected non-compliances with the Information Security policies shall be investigated and corrective action shall be taken and reviewed.
- Such non-compliances as well as their preventive actions shall be further reported at the time of independent reviews.

### 18.2.3 Technical Compliance Review

- Compliance of SPRL's Information Systems with technical security standards shall be maintained. Security control measures shall be regularly reviewed to ensure continued compliance with ISMS; and
- In case of any non-compliance, a root-cause analysis shall be performed to ascertain the reasons and possible preventive actions for the future.