SystemSpecs

Information Security Policies

P-INFOSP

Version 1.6
21-Nov-2023

Document History

Version	Release Date (DD-MMM-YYYY)	Author	Description of Change	Reviewed By
0.1	24-Aug-2016	Oluwaseyi Ojo	Control level Information Security policies.	PISC
1.0	30-Aug-2016	Ribhu Lavania	Content review	PISC
1.1	12-Dec-2017	Oluwaseyi Ojo	Content review	PISC
1.2	14-Sept-2018	Technology Support and Enterprise Security	Content review	PISC
1.3	29-Jul-2019	Process Development & Improvement	Annual review	PISC
1.4	18-Aug-2020	Process Development & Improvement	Annual review Change of corporate logo	PISC
1.5	23-Aug-2022	Process Development & Improvement	Annual review	PISC
1.6	21-Nov-2023	Process Development & Improvement	Annual review	PISC

Details
This document describes Management directives for various security controls exercised to achieve a wholesome Information Security Management System (ISMS) at SHL. Its content is available to the concerned employees of SHL and relevant interested parties, including suppliers; with Management approval. Mode of distribution will be through the common folder structure owned by the PISC. This document is controlled through its version number.

Approval

Name	Position	Signature	Date
Udy Ngele	Chief Information Security Officer		

Reference Documents

Document ID (if any)	Document Name
ISO/IEC 27001:2013 International Standard	Information Technology - Security Techniques – Information Security Management System (ISMS) – Requirements.
ISO/IEC 27002:2013 International Standard	Information Technology - Security Techniques – Code of Practice for Information Security Controls.

Note of Confidentiality

This documentation is furnished to you solely in your capacity as a client or potential partner of SystemSpecs Holdings Limited (SHL) and participant in one or more of its products and services. By accepting this document, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions which limit your use of the Information.

You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a client or potential partner of SHL or as a participant in one or more of its products and services. The Information may only be disseminated within your organization on a need-to know basis to enable your participation as a user of one or more of SHL products and services.

Please note that reasonable endeavors have been made to ensure that the information in this document is accurate. SHL does not accept any responsibility or liability (whether arising due to breach of contract, negligence or for any other reason) for any incomplete or inaccurate information; or for any loss which may arise from reliance on or use of information contained in this document.

For the avoidance of any doubts, information contained in this document can be disclosed to third parties only upon written consent of SHL.

TABLE OF CONTENTS

1. Purpose

This set of policies is applied to the entire Information Security Management System (ISMS), all employees of SystemSpecs Holdings Limited and selected vendors. The purpose of the Information Security Management is to ensure adequate security for SHL' information and supporting infrastructure (information assets critical to the operation of the business, external information i.e. Information assets belonging to customers, suppliers and business partners in any form of business relationship with SHL).

The implementation of this policy is a testimony of SHL' commitment to continually improve the organization's Information Security initiatives and provide confidence to business partners in the conduct of business with SHL.

It is the policy of SHL:

To preserve Confidentiality	That is to protect Information Assets against unauthorized access and disclosure.
To maintain Integrity	That is to protect Information Assets from unauthorized or accidental modification thereby ensuring the accuracy and completeness of the organization's information assets.
To ensure Availability	That is to, ensure that Information Assets are available as and when required by authorized users while adhering to the organization's business objectives.

2. Scope

The Information Security Management System (ISMS) is applicable to the design, development, maintenance and support of financial services and human capital software solutions, provided from its offices.

3. Objectives of Implementing the ISMS (High Level)

- Preserve confidentiality, integrity and availability of information; in addition to other information properties such as authenticity, accountability, non-repudiation and reliability.
- Provide assurance of business continuity and information systems resilience.
- Protect critical information assets related to SHL' core business by applying physical and logical controls.
- Protect critical business processes.
- Build and continually improve information security awareness culture.

4. Review

These set of policies are reviewed on an annual basis or earlier (as the need arises); however control mechanisms exist to ensure compliance activities are built into the organizational policies and practices.

When evaluating the effectiveness, adequacy and continued suitability of this document, the following criteria albeit not exhaustive need to be considered:

- Number of employees and external parties who have a role in the ISMS, but are not familiar with this document
- Non-compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organization
- Opportunities for improvement in ISMS implementation and maintenance
- Unclear responsibilities for ISMS implementation

5. ISMS Policies

A. ISMS Policy

Being a leading e-payment, financial and human capital management solutions provider, SHL is committed to protecting its information assets and those of its customers against loss of confidentiality, integrity and availability through mitigating any information security risks by applying appropriate controls.

B. Control Level Policies

Control level policies are reviewed for suitability, adequacy and continued effectiveness at yearly intervals or whenever a significant change takes place in our business. The policies stated in this document are applicable to SHL employees and contractors and are enforced through their contracts/agreements. Violation of ISMS policies may attract punitive actions for employees and contractors.

I. Mobile device policy (A.6.2.1):

Mobile phones, laptops, USB cameras are defined as 'mobile devices'. USB port shall be disabled on some user systems in order to meet specific customer's expectation(s).

II. Teleworking Policy (A.6.2.2):

Where deemed necessary for meeting business objectives, teleworking may be allowed by the network administrator after due authorization by concerned Group Head. Teleworking through

private or public networks is allowed only after authenticating user's connecting (source) device by the destination gateway device. The method of authentication shall be decided in such a way as to ensure that connection is initiated and established using very secure protocols.

III. **Information Security Awareness, education and Training Policy (A.7.2.2)** *(embedded in the HR Security Policy):*
All categories of employees and contractors are made aware/trained based on their roles in the organization on physical and information security.

IV. **Access Control Policy (A.9.1.1, A.9.4.1):**
SHL access control follows a policy of 'minimum access rights' to be granted to a user required for his job function. Access rights are granted by System Administrator to user(s), based on their job roles at the time of joining and whenever job responsibilities are changed. Access control rights and restrictions are determined by the system administrator keeping in mind the technical feasibilities and Group Head's recommendations. Working beyond the granted access rights may invite appropriate disciplinary action.

V. **Secure Log-on Policy (A.9.4.2)**:
Suitable authentication techniques shall be deployed by system administration to authenticate the claimed identity of the person who tries to log-on to SHL networks, applications or devices. Access rights are withdrawn after three unsuccessful attempts and can be re-opened by system administration based on the authorization request from concerned Group Head or direct supervisor. Repeated violators are identified at monthly intervals and reported to reporting manager, Group Head and Executive Director.

VI. **Policy on cryptography and key management (A.10.1.1 and A.10.1.2)**:
SHL uses cryptography for protecting selected information while it is transferred from one devices to other, within or outside the organization. Current risks in the organizational risk register are used to decide which information or a computing device like laptop should be selected for encryption. Executive Director may like to provide written waiver from encryption, on the request of an employee.

Cryptographic key generation, storing, retrieving and retiring/ destroying are automated based on industry best practices and available technology in the company. Public and private keys are separately controlled and communicated to user.

VII. **Clear desk and clear screen policy (A.11.2.9):**

SHL culture demands individual work place, cafeteria and conference/ meeting rooms to remain free of papers having even the slightest information about the company. Personal information and information about company's info assets is protected at all costs across the departments and floors of the company. Further, we mandate a clear screen policy wherein screens of all computing devices including servers, laptops, desktops and other electronic displays do not have any icons indicative of company related information.

Any sensitive and critical information on paper is locked in safe cabinets on daily basis, when not required or while vacating the office. Computers and terminals are logged off or protected with a screen and keyboard locking mechanism, controlled by a strong password. Unauthorized use of

photocopiers, scanners, digital cameras is not allowed and media containing sensitive or classified information is removed from such devices.
Paper shredders are made available at strategic places within the office premises to shred paper based sensitive and classified information not required anymore.

VIII. Backup and restoration policy (A.12.3.1):

Based on the business process a system addresses and how frequently data on such systems change, some backups are taken daily at close of business and some others are taken weekly (Saturdays). Backups include all common folders including emails. Backups are taken on hard disk drives and backed up data that may not be required for immediate restore are kept away from the office area. Minimum three months' backups are available at any given time at a location away from the office. Backup tapes can be identified by stickers pasted on them.

Randomly-selected backed up information is restored once every month to verify integrity of data. Any backup information required by user departments is passed on to them, after being tested by network administrator/s.

IX. Information Transfer Policy (A.13.2.1):

Non-sensitive/ non-critical files can be transferred by employees to interested parties using Skype messenger or company provided emails. Use of personal email ids is prohibited for official purposes. Email attachments up to 20 MB in size can be transferred. Use of official mail id for transmitting personal information is prohibited. Paper files are retained for 5 years unless required to be stored for a longer time under legal obligations.

X. Secure Development Policy (A.14.2.1):

SHL software development facility is a secured one. Entry of visitors and employees is controlled using a biometrics machine installed at the door of the development center. Secure coding guidelines and coding standards are used in the development center. All code repositories and data of development and testing tools are kept secure using appropriate password controls, encryption and timely backups.

XI. Supplier Relationship Policy (A.15.1.1, A.15.2.2):

Confidentiality agreements are signed with each supplier of goods and/ or services, thus contractually barring sharing of sensitive information of each other within or outside the company. Suppliers are contractually obliged to follow SHL security precautions while physically being in the company premises or while dealing with the matters related to the company. Information access rights are defined in the supplier agreements. The supplier agreements contain applicable legal, commercial and technical requirement and they are trained on company's info security measures. Changes or renewal of supplier agreements will address changes required in access given to information processing facilities.

XII. Information Security Reviews (A.18.2)

New customer orders are accepted after commercial and legal reviews to ensure compliance to applicable statutory, regulatory, contractual requirements and SHL process requirements. Their impact on information system is identified and implemented. Waivers, if any are recorded and maintained. Intellectual property rights (IPR) of all the entities involved are respected and implementation of contracts is not allowed in a way that it infringes on any IPR/s. Info assets registers are maintained and it is ensured that none of the IPRs involved are violated. Only software

licenses and products/ tools authorized by the management are installed on information processing facilities. Unauthorized or pirated software is not used in SHL computing resources.

Personally identifiable information like name, address, tax identification number, passport details etc are protected and communicated to employees.

Information security controls, their effectiveness and continued suitability is reviewed by the management every six months along with main risks on hand, during planned management reviews.

Independent vulnerability and penetration tests are conducted once in a year on our IP addresses. Alternately, certificates of such tests are obtained from hosted service providers.

XIII. Human Resource Policy (A.7)

Human Resources (HR) shall ensure that employees, vendors and third party users agree formally to terms and conditions concerning information security. When and where appropriate, these responsibilities shall continue for a defined period after the end of the employment.

SHL' Management shall require staff of the SHL to apply security controls in accordance with established policies and procedures.

XIV. Information Asset Management Policy (A.8.1)

Information assets are resources which enables the SHL to carry out her mission. They include data, network links, workstations (laptops, desktops, mobile devices), servers, software, network devices (switches, Wireless routers, wired routers, gateways, bridges), network accessories (cables etc.), software licenses, printers, scanners, contractual agreements, legal documents, regulatory obligations, and human resources.

XV. Configuration & Change Management Policy (A.12.1.2)

SHL configuration and change management process applies to all SHL information resources.

XVI. Acceptable Use of Information Resource Policy (A.8.1.3)

All SHL' information resources will be used in an approved, ethical, and lawful manner to avoid loss or damage to the SHL' operations, image, or financial interests and will be used to comply with official policies and procedures on acceptable use. Personnel must seek the authorization of the Chief Information Security Officer prior to engaging in any activities not explicitly covered by these policies.

XVII. Information Security Management System Roles & Responsibilities Policy (A.6.1.1)

Information security is the individual and collective responsibility of all SHL' Staffs, business partners, and other authorized users. Security-related roles and responsibilities must be identified and separation of duties and responsibilities considered when defining roles. Access to information resources will be based on the individual's roles and responsibilities. Only authorized Staff and business partners such as consultants, vendors, and customers, will be approved for access to the SHL' information resources.

XVIII. Physical & Environment Security Policy (A.11)

Physical locations are protected by a combination of physical building structure, guards, access controls.
Location where SHL' offices are situated should be physical protected by physical barriers not limited to the following important ones: Walls/Fences, gates, guards, access control and Closed Circuit Televisions (CCTVs). Separate physical entry controls exist for employees, visitors, cards and equipment. There is a combination of physical, technical (CCTV), personnel controls, and procedural controls. These are controls employed to protect the organization, people and physical environment from unauthorized access and use.

XIX. Anti-Malware Policy (A.12.2)

The chosen anti-malware software are: Comodo and bit defender. The Head of Technical Support is responsible for ensuring that the software is installed on the entire SHL' workstations, servers and notebook computers, that automatic updates are enabled and that the most current version is actually operating on all devices. Users are responsible for notifying Technology Support in the event that their device(s) do not have the latest version of relevant antimalware software

XX. Incident Management Policy (A.16)

The SHL' information resources must be protected against events that may jeopardize information security by contaminating, damaging, or destroying information resources. All information security incidents must be reported in accordance with the policies and procedures provided below regardless of whether or not damage appears to have taken place.

XXI. Network Security Policy (A.13.1)

This policy outlines rules for computer network access, determines how policy is enforced and lays out some of the basic architecture of the company security/ network security environment.

XXII. Operations Management Policy (A.12)

This domain is concerned with the actual delivery of required services, which range from traditional IT operations over security and continuity aspects to training. In order to deliver these services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls, managing third party services and associated service level agreements. This also addresses the control over the IT process of managing operations that satisfies the business requirement to ensure that important IT support functions are performed regularly and in an orderly fashion.

XXIII. Business Continuity & Disaster Recovery Policy (A.17.1)

SystemSpecs Holdings Limited recognizes the importance of business survival and has developed this Business Continuity Plan (BCP) that outlines the policies and strategies to be implemented in the event of a disaster. The plan ensures an effective, organized response should an emergency situation disrupt normal office operating conditions for an immediate or indefinite period of time.

Without well-rehearsed contingency plans for disasters, SHL employees have little option but to react haphazardly in the event of a disaster. On the other hand, a Business Continuity team that has planned, practiced, and fine-tuned its options can align its actions to meet a problem of any magnitude. Regular drills enable personnel to act instinctively when disaster strikes.

6. Disciplinary Action

Any deliberate attempt to jeopardize the information assets or the supporting infrastructure will be subject to appropriate disciplinary action, including but not limited to immediate termination. The company's employee's Handbook will serve as formal reference for such actions.

----End of Document----