BSV
bringing life to life

Bharat Serums and Vaccines Limited

INFORMATION SECURITY POLICY(SUPPLIERS)

Domain:	Information Security Management System
Document Owner:	Information Security Officer (ISO)
Document Approver:	CQA-Head
Version #:	1.0
Document Number:	BSV-ISMS-PLY-ISPS-008
Effective Date:	02/01/24

	Prepared by (ISO)	Reviewed by (Head - IT)	Approved by (Head-CQA)
Name	Gayatri Poppale	Sharad Tatar	SACHIN D. JOSHI
Sign and Date	28/12/23	29/12/23	02/01/24
Designation	ISO	GM-IT	Head-CQA.

Revision History:

The Revision History table below provides a record of all revisions made to this document throughout its life cycle. Updates are tracked by date the revisions were made, the version number, a brief description of the changes made and reason, as well as the name of the reviser and the approver.

Effective Date	Version #	Change Description/ Reason	Created/Revised by	Approved by
2nd January 2023	1.0	First release	ISO	CQA-Head

Table of Contents

1. Objective:

The Objective of this document is to define and establish the management intent and overall direction for the Information Security Management System based on ISO 27001:2013 standard. The overall objective of BSVL, towards Information Security is:

1.1 Conducting periodical risk assessments to identify possible risks for confidentiality, integrity and availability of data, information assets, information systems as well as information processing facilities etc.

1.2 Employing prudent controls, policies, standards, practices, processes, and procedures to mitigate and minimize the risks.

1.3 Identifying all applicable compliance requirements including legal, statutory, regulatory as well as contractual obligations and ensuring timely and continual compliance of them,

1.4 Involving and engaging employees, non-employees, outsourced resources, independent contractors, clients, business partners, service providers in the process of information security and ensuring that everybody follows policies and contributes in their responsibilities towards effective information security.

1.5 Creating widespread and regular awareness amongst all stakeholders about their responsibilities towards information security.

1.6 Committing continual improvement through effective monitoring, measurement, and analysis of information security performance.

1.7 Implementing effective response and reporting mechanisms for information security violations and breaches as well as by planning causal analysis and corrective actions for reducing the re-occurrence in future.

1.8 Planning effective continuity of people, services, and systems for ensuring continuation, resilience and restoration of client deliveries, trust, satisfaction, and confidence.

1.9 Committing continual improvement through effective monitoring, measurement, and analysis of information security performance.

1.10 Identifying all applicable compliance requirements including legal, statutory, regulatory as well as contractual obligations and ensuring timely and continual compliance of them.

2 Scope:

Information Security Management System Policy applies to Bharat Serum and Vaccine's all suppliers.

3 Responsibility:

The term `Supplier' as mentioned within this document include all types of external providers including suppliers, vendors, service providers, outsourced agencies, consultants, contractors, external resources etc. who work with BSVL and may access the information or information assets or information processing facilities or information systems in due process.

All suppliers, who access BSVL information systems, are responsible for ensuring that they operate systems in such a manner as to ensure its security with relevant controls as per the requirement.

3.1 Suppliers must ensure the confidentiality of all information entrusted to them by BSV.

3.2 BSV's `Confidential' information should not be disclosed, shared, or used for purposes other than the agreed-upon contractual requirements.

3.3 Suppliers should implement appropriate measures to protect personal data belonging to BSV or provided by BSV for processing and comply with applicable data protection laws and regulations.

3.4 Access to BSV's systems, data, and facilities should be strictly controlled. Suppliers must maintain robust authentication mechanisms and limit access to authorized personnel only.

3.5 Suppliers should exercise due diligence in handling, transmitting, and storing information to prevent unauthorized access, alteration, or destruction.

3.6 Suppliers should promptly report any security incidents, breaches, or suspected vulnerabilities to BSV.

3.7 Suppliers should comply with all applicable laws, statutes, regulations as well as contractual requirements related to information security, cyber security and data privacy.

3.8 Suppliers should have a robust business continuity plan to ensure the timely recovery of operations in the event of disruptions or disasters.

3.9 Suppliers should ensure that their subcontractors and third-party vendors comply with the same level of information security requirements specified in this policy.

3.10 Suppliers must adhere to security guidelines while implementing any application for BSV.

3.11 Suppliers remain accountable for the actions of their subcontractors and third parties involved in providing services to BSV.

3.12Suppliers should oblige to all physical security controls set in BSV premises while their visit.

4 Policy:

Bharat Serums and Vaccines Ltd. (BSVL) Information Security Policy is based on the following principles:

1. Confidentiality: Protection of information by ensuring that information is accessible only to those authorized.
2. Integrity: Assuring accuracy and completeness of information and its associated information processing methods.
3. Availability: Ensuring that information and associated assets or systems are available to authorized users when required.

The overall objective of BSVL, towards Information Security is:

a. Conducting periodical risk assessments to identify possible risks for confidentiality, integrity and availability of data, information assets, information systems as well as information processing facilities etc.
b. Employing prudent controls, policies, standards, practices, processes, and procedures to mitigate and minimize the risks.
c. Identifying all applicable compliance requirements including legal, statutory, regulatory as well as contractual obligations and ensuring timely and continual compliance of them,
d. Involving and engaging employees, non-employees, outsourced resources, independent contractors, clients, business partners, service providers in the

process of information security and ensuring that everybody follows policies and contributes in their responsibilities towards effective information security.

e. Creating widespread and regular awareness amongst all stakeholders about their responsibilities towards information security.

f. Committing continual improvement through effective monitoring, measurement, and analysis of information security performance.

g. Implementing effective response and reporting mechanisms for information security violations and breaches as well as by planning causal analysis and corrective actions for reducing the re-occurrence in future.

h. Planning effective continuity of people, services, and systems for ensuring continuation, resilience and restoration of client deliveries, trust, satisfaction, and confidence.

Any major change in policy would be initiated by ISO and incorporated only after approval of the BSVL management committee. The ISO shall be responsible in communicating the same to all service providers and employees or parties who may be directly or indirectly impacted by the change in policy.

This policy must be reviewed at least once a year and changes to policy and standards must be identified. The policy must be updated based on the outcome of this review. Every person in custody of this document has the responsibility for ensuring its confidentiality. The owner of this document is the ISO and shall ensure that the document is continually updated with amendments that may be issued from time to time.

5 Information Security Measures for Suppliers

5.1 Password Policy

Suppliers should adhere to below detailed password policy of BSV while managing information systems or networks of BSV.

Password Specifications	
Password History: the system should recognize the last number of passwords of the user	5
Maximum Password Age: The validity period of the password (in days) after which it should be renewed.	61
Minimum Password Age	60
Minimum Password Length (in characters)	12
Minimum alphabet, a-z, A-Z.	1
Minimum numeral, 0-9.	1
Minimum special character,~,!,@,#,$, %,^,&,*,(,).	1
Password must meet complexity requirements:	Enabled
The maximum number of days that a productive password can be unused (in days).	90
The maximum number of days that an initial password can be unused (in days).	1

Account Lockout Duration (in minutes) (idle time/session time out)	10
Account Lockout Threshold (Invalid login attempts)	5
Reset Account Lockout Counter after (in minutes)	10
Maximum no. of failed login attempts	3

5.2 Software Development related Controls

5.2.1 Supplier, while developing any application or information system for BSV, should adopt industry recommended security practices within their SDLC. Appropriate security measures should be planned so as to comply to information security as well as data privacy requirements laid down by applicable laws and regulations.

5.2.2 Supplier shall develop and follow secure coding guidelines while developing applications or information systems for BSV. Supplier may choose to adopt industry frameworks such as OWASP or NIST or may create their own secure coding guidelines and get them reviewed by BSV before implementing.

5.2.3 Supplier shall incorporate appropriate data privacy principles such as privacy-by-design and privacy-by-default within the applications and information systems being developed for BSV.

5.2.4 Supplier shall conduct appropriate and timely security testing at their end, by themselves or through a competent third party, at every relevant stage of SDLC. Such security testing may include Unit testing, Code reviews, Functional testing, Regression testing, Load testing, Integration testing, Vulnerability assessment, Penetration testing, Acceptance testing etc. Reports of such testing shall be provided by Supplier to BSV on demand.

5.2.5 Supplier shall include information security and data privacy requirements and principles while planning the security testing of the application or information system.

5.2.6 Supplier shall not outsource any development or testing activity to third-party or person without prior knowledge of BSV. In such case where BSV approved outsourcing or sub-contracting of activity happens, the security requirements applicable to Supplier shall also be applicable to such outsourced party or person.

5.2.7 Supplier shall be responsible to comply to intellectual property rights and licensing requirements of tools and software used by Supplier while developing applications or information systems for BSV.

5.3 Non-Compliance

5.3.1 Non-compliance with this Information Security Policy may result in termination of the business relationship and may also lead to legal action.

5.3.2 In case any breach or violation is caused by Supplier personnel, while working with BSV, the actions would be taken as per BSV's Disciplinary policy.