INFORMATION SECURITY MANAGEMENT SYSTEM

Supplier Security Procedure

Version: 2.0

Document No.: PIBL - ISMS - PRO - 018

Internal

TABLE OF CONTENTS

Document Control

Version History:

Date of Approval	Version	Description of change	Owner	Approved by
06-02-2017	1.0	Initial Release	Prudent Insurance Brokers Limited (PIBL)	Information Security Apex Committee (ISAC)
18-02-2019	2.0	5.1.2 Replaced Audit Committee with Apex Committee 3.5 Monitoring of Logical Access rights - removed 3.2.1 Revised Annexure - updated	Chief Information Security Officer (CISO)	Information Security Apex Committee (ISAC)

Authorization:

Prepared by	Reviewed by	Approved by
Acquisory Risk Consulting Pvt. Ltd. (ARCPL)	Mr. Manoj Prakash Kern, Chief Information Security Officer (CISO) Mr. Janmenjoy Banerjee, Compliance Officer	Information Security Apex Committee (ISAC) Mr. Ajit Singh Dhingra Mr. Surjit Singh Dhingra Mr. Pavanjit Singh Dhingra Mr. Gurpal Singh Dhingra

Distribution List:

Sr. No.	Department or Function Name	Distribution Medium
1	All departments of PIBL	Email

Supplier Security Procedure

1. Purpose

1.1 The purpose of this procedure is to reduce the risk of sensitive or critical business information being disclosed, lost or tampered with or by unauthorized personnel and the threat of security breaches.

2. Applicability

2.1. All locations of PIBL in India

2.2. All employees, contract workers and suppliers of PIBL in India

3. Procedure

3.1. Supplier Registration and Selection

3.1.1. Terms and conditions of engagement with third parties:

3.1.1.1. Once the supplier is selected, a formal contract should be signed with the supplier. Contract should include all legalities followed by PIBL. The contract should be bound by a Service Level Agreement (SLA)/SOW to ensure that the supplier provides a defined level of service continuously and efficiently without disrupting the operations at PIBL. It should be ensured that the SLA is clear, complete and documents the 'exit' clauses precisely. PIBL should ensure the following:

3.1.1.1.1. Usage of SLAs with measurable parameters for monitoring and measuring the supplier's performance.

3.1.1.1.2. Based on the criticality of the contract, mutually acceptable punitive clauses shall be included in SLA or purchase order. (E.g. Penalty in case of downtime beyond defined service levels)

3.1.2. Third party access to the confidential information should be restricted to the information they require in completing the contracted work. Non-Disclosure Agreement (NDA) / Confidentiality agreement should be signed by all suppliers, third parties & contractors of the suppliers prior to initiation of the contracted work in order to protect PIBL's information and information assets. The agreement shall also have relevant clauses related to ownership of information, trade secrets, and intellectual property of information assets created in soft/hard form on behalf of PIBL.

3.1.3. The contract shall contain clauses related to exchange and handling of information and software between the PIBL and the external party through electronic and physical modalities shall be addressed.

3.1.4. The contract shall also contain a clause stating that PIBL reserves the right to audit third party facilities and processes for security standards as agreed, monitor activities over the access provided to third parties and take appropriate actions.

3.1.5. Respective departments should ensure that the background checks for the employees of the supplier working for PIBL are conducted by the supplier prior to granting them physical and logical access to PIBL information and information assets.

3.1.6. The concerned Manager/Department Head shall ensure that the third parties have signed the relevant agreements with PIBL.

3.2. Information and communication technology supply chain

3.2.1. Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain including :

3.2.1.1. Defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;

3.2.1.2. For information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;

3.2.1.3. For information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;

3.2.1.4. Implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

3.2.1.5. Implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;

3.2.1.6. Obtaining assurance that critical components and their origin can be traced throughout the supply chain;

3.2.1.7. Obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;

3.2.1.8. Defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

3.2.1.9. Implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

3.3. **Managing changes to supplier services**

3.3.1. Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks adheres:

3.3.2. Changes to supplier agreements;

3.3.3. Changes made by the organization to implement:

3.3.3.1. Enhancements to the current services offered;

3.3.3.2. Development of any new applications and systems;

3.3.3.3. Modifications or updates of the organization's policies and procedures;

3.3.3.4. New or changed controls to resolve information security incidents and to improve security

3.3.4. Changes in supplier services to implement:

3.3.4.1. Changes and enhancement to networks;

3.3.4.2. Use of new technologies;

3.3.4.3. Adoption of new products or newer versions/releases;

3.3.4.4. New development tools and environments;

3.3.4.5. Changes to physical location of service facilities;

3.3.4.6. Change of suppliers;

3.3.4.7. Sub-contracting to another supplier

3.4. **Access to information**

3.4.1. Access to information/data of PIBL shall be provided to third parties only if they have a legitimate business need for the same and shall be controlled to avoid intentional/unintentional disclosure.

3.4.2. The Manager from the concerned department shall submit the request for physical and logical access for third party usage.

3.4.3. The form shall then be submitted to the IT Department for granting logical access and information/details are provided to Administration Department for granting physical access respectively as per physical security policy and procedure.

3.4.4. Logical access should only be granted after ensuring that the confidentiality/non-disclosure agreement has been signed by the third party

3.4.5. Logical access should be provided for a definite period only. If required, it can be renewed based on business requirements.

Refer: "Logical & Physical Access and Asset Allocation Form (Third Parties)" for access.

3.5. **Completion/ Termination/ Extension of the Third Party Access**

3.5.1. The rights provided to the external party shall be disabled by IT team if no extension has been provided by the concerned company representative after the expiry (wherever possible).

3.5.2. When termination of services of any third party takes place, PIBL's information shall be returned and destroyed by the third party at agreement cessation.

3.5.3. In case of premature termination/extension of access rights the Department Head/authorized personnel (after approval from Department Head) shall inform the IT Department and Administration about the termination/extension of the third party access both logical and physical respectively.

3.5.4. The Department Head shall ensure that the final settlement or contract closure with third party takes place only after the IT Department have revoked the access rights

3.6. **Assessing Outsourcing Risks (If any)**

3.6.1. In relation to outsourcing, specifically, the risk assessment shall take due account of the:

3.6.1.1. Nature of logical and physical access to PIBL's information assets and facilities required by the outsourcer to fulfill the contract;

3.6.1.2. Sensitivity, volume and value of any information assets involved;

3.6.1.3. Commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services to PIBL's competitors where this might create conflicts of interest; and

3.6.1.4. Security and commercial controls known to be currently employed by PIBL and/or by the outsourcer.

3.6.2. The result of the risk shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if PIBL will benefit overall by outsourcing the function, taking into account both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (e.g. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

3.6.3. Security measures that need to be implemented by PIBL and the supplier will be identified as a result this Risk Assessment. Implementation of these measures should be added as part of the contract / SLA.

[Refer: "Annexure B: Supplier Information Security Assessment Questionnaire"]

3.7. **Supplier Relationship Management**

3.7.1. PIBL and the supplier should establish a single point of contact from each side to manage the operational issues. Escalation hierarchy should be established for each of the suppliers to resolve long time pending issues related to outsourcing.

3.8. **Supplier Performance Evaluation**

3.8.1. Respective department (which has outsourced the activity) should ensure that the performance of existing suppliers is evaluated, rated and feedback is provided to the supplier, with a view to better service delivery. For the services given by the supplier before clearing the bill concern project manager needs to put their comments on the services provided by the third party & the records of the same are maintained by the account team of IT dept.

3.8.2. Suppliers shall be evaluated performance wise, while renewing the contracts with the existing suppliers.

3.8.3. In the event of SLA / NDA clauses being breached by the supplier, PIBL should initiate action against the outsourced party as defined in the contract / SLA / NDA.

[Refer: "Annexure B: Supplier Information Security Assessment Questionnaire"]

3.9. **Information Security In Project Management**

3.9.1. Information security should be addressed in project management, regardless of the type of the project. Information security should be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project.

3.9.2. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, facility management and other supporting processes.

3.9.3. The project management methods in use should require that:

3.9.3.1. Information security objectives are included in project objectives;

3.9.3.2. An information security risk assessment is conducted at an early stage of the project to identify necessary controls;

3.9.3.3. Information security is part of all phases of the applied project methodology.

3.9.4. Information security implications should be addressed and reviewed regularly in all projects. Responsibilities for information security should be defined and allocated to specified roles defined in the project management methods.

4. Guidelines for Consideration of Contract

4.1. Other than the regular legal issues, PIBL should consider including, but not limited to, the following information security related aspects in the contract with the supplier

4.2. Information Security Policy and Procedures;

4.2.1. Procedures regarding protection of information assets;

4.2.2. Description of each service to be provided;

4.2.3. Provision for transfer of staff where appropriate;

4.2.4. The respective liabilities of the parties to the agreement;

4.2.5. Specific Access Control procedures;

4.2.6. Escalation process for problem resolution;

4.2.7. Contingency arrangements;

4.2.8. Responsibilities regarding hardware and software installation and maintenance;

4.2.9. Change management procedures;

4.2.10. Awareness of suppliers security responsibilities;

4.2.11. Availability of services in the event of a disaster;

5. Responsibilities

5.1. The HOD - IT shall have the following responsibilities:

5.1.1. Evaluate the risk and materiality of all outsourcing, policies and procedures, based on the frame work approved.

[Refer: "Annexure A for Supplier Evaluation and Risk Assessment Form"]

5.1.2. Ensure that every outsourcing contract / requirement has been entered into the ERP system and the approval has been provided by the concerned Department Heads.

5.1.3. Undertake regular review of outsourcing strategies and arrangement for their continued relevance.

5.1.4. Ensure putting in place contingency plan to take care of probable disruptive scenarios.

5.1.5. Communicate information pertaining to material outsourcing risk to the Board.

5.1.6. Finalize review mechanism including periodicity and for reporting to the Board.

5.1.7. Putting in place a central data base on outsourcing.

5.1.8. Finalizing and implementing internal guidelines covering aspects such as material outsourcing, business continuity and management of disaster recovery plan, off-shore outsourcing and self-assessment of existing and proposed outsourcing arrangements etc.

5.2. **The Internal Audit team** Team shall have the following responsibilities:

5.2.1. The Internal Audit Team at PIBL shall ensure audit on outsourcing activities at PIBL as per the criticality of the supplier and the outsourced process including forensic investigations if necessary as demanded by specific incidents which may have occurred.

5.2.2. The key audit findings shall be reported to the Apex Committee.

5.2.3. The audit findings shall also be reported to the Procurement Team.

5.2.4. Key Highlights, Unresolved Issues which are likely to pose security risks shall also be formally communicated to the CISO and to the Apex Committee.

6. Enforcement

6.1. This procedure is applicable to all business associates, contractors, suppliers, visitors, customers, trainees, housekeeping staff, drivers, facility management staff and consultants who visit and work on our premises for limited or extended periods of time.

6.2. Management's interpretation of the clauses in this procedure shall be final and binding. Management reserves the rights to alter or amend any clause in this procedure at any time as per their discretion.

7. Points of Audit

7.1. The audit check points for this procedure shall be as following:

7.1.1. Contracts, SLAs and NDAs

7.1.2. Risk Assessment of Supplier

7.1.3. Nomination of point of contact for each supplier

8. Exceptions

8.1. Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time.

8.2. Exceptions to the Supplier Security Organization Policy may have to be allowed at the time of implementation of this policy and procedure or at the time of making any updation to this document or after implementation on an ad-hoc basis based on business or a specific and a peculiar manifestation of circumstances which could be temporary or permanent in nature.

8.3. All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through an Exception Form and sign-off on the same shall be maintained including ad-hoc requests.

[Refer: "Exception Form" in Annexure B]

1.0 The CISO shall review all exceptions, as the case may be, every year for validity and continuity.

1.1 Anything not specifically stated in this Supplier Security policy and procedure document shall not be considered as implied in any manner. For any clarifications related to this document with respect to its interpretation, applicability and implementation, please write to CISO at ciso@prudentbrokers.com

9. Reference to ISO 27001:2013

9.1. Control Objectives: A.15.1, A.15.2

9.2. Controls: A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2

10. Abbreviations

10.1. ISMS -Information Security Management Systems

10.2. HOD- Head of Department

11. Annexure

Sr. No.	Reference (Policy/Procedure/Guidelines)	Document ID
1	Access Control Policy	PIBL - ISMS - POL – 004
2	Access Control Procedure	PIBL - ISMS - PRO – 004
3	Physical Security Policy	PIBL - ISMS - POL – 006
4	Physical Security Procedure	PIBL - ISMS - PRO – 006
5	Human Resource Security Policy	PIBL - ISMS - POL – 002
6	Human Resource Security Procedure	PIBL - ISMS - PRO – 002
Sr. No.	**Reference Format/Template/Form**	**Document ID**
1	Exception Form	PIBL - ISMS - FMT – 001
2	Supplier Information Security Assessment Questionnaire	PIBL - ISMS - FMT – 024
3	Logical & Physical Access and Asset Allocation Form (Third Parties)	PIBL - ISMS - FMT – 013