# Information Security Management System

## Third Party Security Policy

Document no. JMBGRP/ISMS/Pol-TP

Version no. v1.2

**Document details**

| | | |
|---|---|---|
| **Classification** | Internal | |
| **Released date** | 28.08.2018 | |
| **Description** | The purpose of this policy to ensure security requirements for protection of confidentiality, integrity and availability of business-critical information by third party. | |
| **Custodian** | Corporate IT dept. | |
| **Approved by** | Manish Jaiswal (Group CTO) | |
| **Owner** | Corporate IT Dept. | |

**Distribution list**

| **Name** |
|---|
| To all locations of JMB group. |

**Version History**

| Version no. | Version date | Approved by | Comments | Signature |
|---|---|---|---|---|
| v1.0 | 28.08.2018 | Manish Jaiswal (Group CTO) | Reviewed & no changes | |
| v1.0 | 10.01.2019 | Manish Jaiswal (Group CTO) | Reviewed & no changes | |
| v1.0 | 08.02.2020 | Manish Jaiswal (Group CTO) | Reviewed & no changes | |
| v1.0 | 11.02.2021 | Manish Jaiswal (Group CTO) | Reviewed & no changes | |
| v1.1 | 25.03.2022 | Manish Jaiswal (Group CTO) | Logo changes done in this policy | |
| v1.2 | 28.09.2023 | Manish Jaiswal (Group CTO) | Changes done for “Bank” to “JMBGRP” | |
| v1.3 | 16.10.2024 | Manish Jaiswal (Group CTO) | Modifications done in Section: “Procedure, Responsibilities” | |

# Contents

## Purpose

To ensure that security requirements for protection of confidentiality, integrity and availability of business-critical information are satisfied and maintained when a business process or processes are partially or completely entrusted to a vendor or outsourced.

## Scope

This policy applies to the following:

- All Employees of J.M Baxi Group
  - All Vendors/ contract staff of J.M Baxi Group who have access to information or information systems.

## Policy Statement

- The risks to JMBGRP's information and information processing facilities from external parties shall be identified through a formal risk assessment prior to granting logical or physical access to the external party.
- Vendor Inventorization and identification criticality shall be established for every vendor of JMBGRP.
- JMBGRP shall subject outside entities/third parties such as vendors, auditors, consultants, etc., to the same access restrictions to which an internal user would be subjected to while handling JMBGRP's business related and its customer related information.
- JMBGRP shall provide access to the Information Assets to external party(s) on a need-to-know basis only, thereby preventing misuse or compromise of the same. The information so provided shall always ensure that the external party shall be in a position to fulfill all its contractual obligations as laid down by JMBGRP.
- JMBGRP shall be the custodian of the vendor information as well and it shall at all times ensure privacy of this information is maintained and that this information too shall be protected at all times from getting misused or compromised.
- Monitoring and review of third-party services shall be carried out to ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly.
- Risk Assessment shall be conducted for the vendors as per their criticality with a predefined periodicity as per a standardized framework.
- Changes to the provision of services by third party, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

  In order to ensure that there is compliance demonstrated by the third parties, JMBGRP shall sign agreements which shall address clauses related duration/ non-disclosure/ confidentiality/exchange of information and software in physical and electronic modalities/service delivery and commitment/levels of physical and logical access and their duration thereof. The agreement shall also have relevant clauses related to

creation/storage/transmission/destruction of information assets created in soft/hard form on behalf of JMBGRP or for JMBGRP.

- JMBGRP shall ensure that all services to be provided by the vendor are identified and clearly defined. The relationship with the vendor shall be managed through identified single point of contact (SPoC) /department between JMBGRP and the vendor
- The category of services which shall be outsourced shall also be made available by the procurement cell to the business and reviewed on a yearly basis.
- The vendor selection shall be approved by the unit head/chief followed by the final approval from the Head of Procurement before the process of commencement of services.

## Procedure

1.1 Vendor Security and Information Privacy Procedure addresses the controls, roles and responsibilities of the identified employees/groups for assessment and management of risks on account of the information related to customer may be accessed, processed, communicated, or managed by employees, external parties or the information processing facilities that may be accessed or managed by external parties.

1.2 Every department which wishes to deploy a vendor or avail of any outsourcing activity shall always follow the process of vendor procurement as laid down in this procedure comprising of:

1.2.1 Completion of Vendor Profile and enlisting the service to be outsourced.

1.2.2 Determining Vendor Criticality as per the Annexure

1.2.3 Vendor Risk Assessment and Report

1.2.4 Vendor Agreement Sign Off

1.2.5 Vendor Induction

1.2.6 Vendor Services Roll Out

1.2.7 Vendor Services Review and SLA Monitoring

1.2.8 Vendor Service Closure.

1.3 The abovementioned steps shall be administered by the procurement cell in cooperation with the concerned department through formal process.

1.4 Proper selection of service provider shall be ensured through due diligence by business on the basis of: -

1.4.1 Competence- qualitative and quantitative

1.4.2 Financial strength/business strength

1.4.3 Market report/feedback on track record from users/clients,

1.4.4 Infrastructure facilities.

1.4.5 Compliance with regulatory/statutory requirements and

1.4.6 Security and internal control, audit coverage, reporting and monitoring environment, Business continuity management.

1.4.7 Estimated value of the business to be transacted annually or for the period specified.

1.4.8 Quality assurance and/or security management standards currently followed by the company (e.g. certified with ISO 9000 or ISO/IEC 27001 and other standards

1.5 The Vendor information shall be collected through a form as listed in the annexure and criticality of the vendor at the first level determined as per the steps outlined below in the same annexure.

1.5.1 **Critical** - A function of financial value of the process deployed, business engagement coupled with exchange of information, nature of information systems deployed and those which have access to JMBGRP network. This vendor will have access to Critical /Confidential information of JMBGRP.

1.5.2 **Important** - A function of financial value of the process deployed, business engagement coupled with exchange of information, nature of information systems deployed and those which have access JMBGRP network. This category of vendor will have access to Internal Information of JMBGRP.

1.5.3 **Simple** – A Function of financial value of the process deployed, business engagement coupled with exchange of information, nature of information systems deployed and those which have access to JMBGRP network. These categories of vendors will only have access to public information of JMBGRP.

1.6 After the initial criteria and steps have been fulfilled a vendor assessment shall be executed and report submitted outlining the risks involved.

1.7 The decision to proceed with vendor nomination shall be taken by the department concerned along with the procurement team basis the vendor information and the output of the risk assessment. The approval for outsourcing shall also include:

1.7.1 Job/activities to be outsourced – this will be based on the approved list of vendors and nature of services which could be outsourced as released by the procurement cell.

1.7.2 Need/justification for outsourcing.

1.7.3 Risk factors involved like:

1.7.3.1 Strategic risk, Reputation risk, Compliance risk, Operational risk

1.7.3.2 Exit strategy risk, Counter party risk, Country risk, Contractual risk

1.7.3.3 Concentration and systematic risk, logical access risk, physical access risk

1.7.4 Cost benefits analysis.

1.7.5 Industry practice.

1.7.6 Regulatory compliance etc.

1.8 As far as possible, activities shall be allocated to different service providers depending on business requirements such that system shall not become dependent on single service provider specific at any given point of time. The aggregate exposure allowed to a particular Service Provider is taken into account in case a particular service provider is allowed various functions. In order to manage and minimize operational risk, the service provider shall have an effective internal control function commensurate with the level of perceived risk. It shall be the responsibility of business group to ensure these aspects.

1.9 **Documented agreements:**

1.9.1 The decision on outsourcing and selection of service provider shall be followed by execution of standard agreement drafted for this purpose.

1.9.2 The agreement shall, inter-alia, cover the following:

1.9.2.1 **Parties to the agreement:** Who are the parties involved and when does the agreement commence and the tenure of agreement.

1.9.2.2 **Definitions:** This section shall include the definitions to all the items that are discussed. For example, if activities in the call center are to be outsourced then this section shall cover a “Call” or a “Customer Call”.

1.9.2.3 **Description of services:** This section shall indicate what services are to be covered under the agreement.

1.9.2.4 **Employee section:** This section shall outline the major responsibilities of the vendor with regard to his employees. The vendor shall have in place, appropriate code of conduct for vendor employees with a provision of punitive action in case of any breach by vendor employees.

1.9.2.5 **Related services:** Any related services that the organization feels the vendor shall provide shall be covered in this part.

1.9.2.6 **Service levels:** The required service level and penalties for not adhering to the same shall be specified in this section.

1.9.2.7 **Remedial punitive actions:** For not adhering to the agreed service levels including performance standards, confidentiality and secrecy requirements,

other restrictions as may be deemed necessary by JMBGRP in respect of use of JMBGRP's/brand shall be clearly specified in this section.

1.9.2.8 **Reviews:** The frequency of review to be carried out by the JMBGRP shall be specified in this section.

1.9.2.9 **Training:** Arrangements related to training of the vendor's staff shall be mentioned in this part.

1.9.2.10 **Fees:** This section shall cover the fees payable for each activity performed by the vendor.

1.9.2.11 **Vendor's obligations:** This section shall cover regulatory compliance on the part of the vendor; in particular compliance with respect to the Contract Labor Act, other Labor Laws and Statutory requirements which include IT Act, Cyber Law from the information Security perspective need to be fulfilled by the vendor, and shall be specified clearly.

1.9.2.12 Clauses related to exchange and handling of information and software between the company and the vendor through electronic and physical modalities and handling of media, while in transit.

1.9.2.13 Clauses related to access to information systems while on premises or through remote access, carriage of personal computing devices, media, smart devices in to JMBGRP locations for execution on the responsibilities so assigned.

1.9.2.14 Clause stating that any Information Security incident resulting from non-compliance may result in disciplinary action.

1.9.2.15 Clause stating that JMBGRP reserves the right to audit vendor's facilities and processes for the agreed security standards, monitor activities over the access provided to it and take appropriate actions.

1.9.2.16 Clauses related to conduct forensic investigations on the laptops/computers/portable media/smart devices/phones as used by vendor personnel during the engagement with JMBGRP and post conclusion of contract.

1.9.2.17 Clauses stating that the vendors are responsible for immediately informing the SPoC at JMBGRP of any security breaches concerning JMBGRP's information assets.

1.9.2.18 Any additional clauses as an outcome of the Vendor Risk Assessment conducted.

1.9.2.19 The concerned HOD shall ensure that the vendor has signed the relevant agreements with JMBGRP.

1.9.2.20 **General provisions:** This section shall outline the broad rules regarding non-disclosure and confidentiality of all documents/data entering the vendor's premises through signing of the Non- Disclosure Agreement. The period of

Non- Disclosure shall be specified by the JMBGRP on the data held by the vendor or learning accrued by way of the association with the JMBGRP for a period of 05 years. Failure to comply shall mean automatic legal action.

1.9.2.21 If the vendor subcontracts the work further, the responsibility shall continue to lie with the appointed vendor for any breach/ violation on the SLA by the subcontractor(s). The vendor shall also ensure that clauses to protect its business interest with JMBGRP are included in its contractual agreements with the subcontracting vendors. This shall be an auditable point for the vendor.

1.9.2.22 **Dispute resolution clause:** This section shall describe the escalation matrix for any dispute and the resolution mechanism.

1.9.2.23 **Termination clause:** This section shall have a termination trigger in the Service Level Agreement (SLA) for breach of SLA.

1.10 The agreement documents shall be prepared in consultation and with the approval of the Legal Department.

1.11 The Procurement Cell is only authorized to execute the agreement as per the standard format. Additions/deletion of any clause from the standard agreement, if any, due to business specific reasons, are carried out in consultation with the Corporate Legal Group.

1.12 A grievance redressal mechanism shall be put in place to ensure that grievances, if any, on service-related issues are addressed. The Service Providers of the JMBGRP shall be appropriately updated on such mechanism.

1.13 For any offshore (outside India) outsourcing care shall be exercised in addressing aspects of local regulations, data protection, privacy and confidentiality aspects. All laws impacting such an agreement shall be ascertained by the Legal Team and consent provided to the Procurement Cell in writing stating risks involved before proceeding to enter into a legal contract.

1.14 The storage, retrieval and production of documents which are auditable by JMBGRP shall be the responsibility of the designated officers of the respective business group and business shall identify such officers in respect of their group.

1.15 Any exception to the said process shall be through a written sign off provided by the specific Business head and Head of Procurement along with a formal sign off from the Security In-Charge and Head IT Team

**Vendor Access**

1.16 Access to Information and Information Systems shall be managed as follows:

1.16.1 Access to information and information systems of JMBGRP shall be provided only if there is a legitimate business need for the same and shall be controlled to avoid intentional/ unintentional disclosure.

1.16.2 Access shall be established through the engagement contract, verified by the business process owner and ratified by IT Team.

1.16.3 The concerned department shall submit the request for physical and logical access which shall be reviewed by the Security In-Charge's office. [Refer : Annexure B :Vendor Requisition Form]

1.16.4 Risk assessment for Remote Access shall form a part of the Risk Assessment Process and outcome shall decide the nature of the access to be provided, which stall state the number of people, ports through which access shall be provided and the duration of access to be provided to the identified personnel on the side of the vendor.

1.16.5 Post the risk assessment, a sign-off would be obtained from the HOD of the concerned department on the security impact after which an approval will be given from the Security In-Charge granting physical/ logical access to the vendor (if approved). Assurance has to be sought in writing in case of Critical and Important Vendors for instituting an appropriate Risk Mitigation Plan which shall be reviewed by JMBGRP on a defined periodicity.

1.16.6 An intimation will be sent to IT Team to grant logical access rights for the specified duration after ensuring that the confidentiality/ non-disclosure agreement has been signed by the vendor.

1.16.7 If the vendor is using a personal computing devices to access JMBGRP's information processing facilities, the devices shall be hardened by IT Team before granting access for access within JMBGRP and for access from Vendors Side, secure authentication shall be mandated with a time bound provision. (refer to logical access control policy). Aspects related to time and duration of access shall also be clearly specified during normal working hours, beyond working hours and on designated holidays of JMBGRP.

1.16.8 Carrying portable media, devices to JMBGRP premises shall not be permitted to vendor personnel.

1.16.9 The concerned HOD shall ensure that the vendor personnel are provided communication and training on JMBGRP's information security policies and procedures and awareness training as prescribed by JMBGRP is carried out and a sign-off on the same shall be obtained from the vendor by HR/ Training department.

1.16.10 Logs of logical access to the information and information systems at JMBGRP by the vendor shall be monitored and reviewed.

1.16.11 If mail ID has to be provided to the vendor personnel, then it shall pass through the appropriate requisition process as mandated by the E-Mail Policy at JMBGRP.

1.16.12 Disclosure of information assets of JMBGRP to third parties/outside entities shall be maintained in a log indicating the information that was provided by the information owner. This log shall be important when the time arrives to recover these materials (or obtain a letter certifying the destruction of the materials) at the end of a contract.

1.16.13 The physical access shall be provided by the Contractor Cell as per the prevalent process instituted by Physical Security Department at JMBGRP. The rules covering physical access shall cover:

1.16.13.1 The physical access rules shall clearly specify the time in and time out of the vendor personnel who need to work on premises of JMBGRP.

1.16.13.2 The provision to work beyond working hours of JMBGRP including permission to access the premises on designated holidays of JMBGRP.

1.16.13.3 Carriage of physical material/ documents in and out of the premises of JMBGRP or bringing in material into the JMBGRP premises and restrictions thereof.

1.16.13.4 The security personnel shall have the rights to check the belongings of the vendor personnel when working on JMBGRP premises and escalate should violation be noticed to the concerned business unit manager and initiate disciplinary action.

1.16.13.5 All vendor personnel shall always display their identification cards when working on JMBGRP premises and will be open to checking of the same as per the requirement of the physical security personnel.

1.16.13.6 Carriage of portable media / smart devices shall not be allowed for vendor personnel and exceptions thereof shall have a sign off from the concerned business owner and Security In-Charge's office.

1.16.13.7 Carriage of laptops for work on JMBGRP premises shall be documented and JMBGRP shall have the right to audit the contents of the laptop at any time.

**Service Delivery Management:**

1.17 **Vendor service delivery shall be managed as follows:**

1.17.1 The services provided by the vendor shall be monitored and reviewed regularly (at least once in a year) to ensure compliance to information security terms and conditions and the agreed upon service levels. Services, reports and records provided by the vendor shall be maintained properly to facilitate monitoring and review.

1.17.2 Changes to the provision of services shall be managed, taking into account business criticality, processes involved and re-assessment of risks by the process owner in consultation with the HOD.

1.17.3 Vendors shall be audited as per the ''Vendor Assessment Process'' in the annexure.

1.18 **Vendor Relationship Management**

1.18.1 JMBGRP and the vendor shall establish a single point of contact from each side to manage the operational issues.

1.18.2 Escalation hierarchy shall be established to resolve outstanding issues related to outsourcing for both JMBGRP and the vendor.

1.19 **Completion/Termination/Extension of the access to vendors is to be managed as following:**

1.19.1 If no extension has been provided by the concerned HOD at JMBGRP, the rights granted to the vendor shall expire automatically after expiry of work order.

1.19.2 When termination of services of any vendor takes place, JMBGRP's information shall be returned and/or destroyed by the vendor and a confirmation for the same shall be provided to JMBGRP by the vendor.

1.19.3 In case of premature termination/ extension of access rights, the HOD at JMBGRP shall inform IT Team and the Contractor Cell about the termination/ extension of both logical and physical accesses.

1.19.4 The HOD shall ensure that the final settlement or contract closure with the vendor takes place only after IT Team and Contractor Cell / Procurement Cell have revoked the access rights and a sign-off has been obtained from them of the same.

1.19.5 All physical material (computing devices, media, physical documents, samples, models, prototypes, designs, publications, reports, SOPs amongst others, as provided to the vendor/ personnel shall be returned upon the cessation of the contract and audited for misuse if any and necessary action taken if any violation has been noticed.

1.19.6 JMBGRP shall reserve the rights to audit and even make a physical visit to the vendor location(s) to ensure that no information of JMBGRP is resident on vendor premises and a written sign off obtained from the vendor for the same.

## Responsibilities

- Procurement Cell
  - Evaluate the risk and materiality of all outsourcing, policies and procedures, based on the framework approved. Refer Annexure A for Risk Assessment.
  - Ensure that every outsourcing contract / requirement has been entered into the ERP system and the approval has been provided by the concerned Department Heads/Chiefs.
  - Undertake regular review of outsourcing strategies and arrangement for their continued relevance.
  - Ensure putting in place contingency plan to take care of probable disruptive scenarios.
  - Communicate information pertaining to material outsourcing risk to the Board.
  - Finalize review mechanism including periodicity and for reporting to the Board.
  - Putting in place a central database on outsourcing.
  - 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.

- Internal Audit Team
  - The Internal Audit Team at JMBGRP shall ensure audit on outsourcing activities at JMBGRP as per the criticality of the vendor and the outsourced process including forensic investigations, if necessary, as demanded by specific incidents which may have occurred.
  - The key audit findings shall be reported to the Audit Committee.
  - The audit findings shall also be reported to the Procurement Team.
  - Key Highlights and Unresolved Issues which are likely to pose security risks shall also be formally communicated to the Security In-Charge and to the Apex Committee.

## Enforcement

- This policy and procedure is applicable for all the employees and contractors of the company who have access to and use the information assets and IT assets as listed in the Information Asset Classification sheet which have been created for all the departments. Any violation shall be dealt in accordance with the disciplinary action process as laid down in the Code of Conduct.
- Violations by the vendors shall also come under the purview of the Information Security Framework and action shall be taken accordingly.
- 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 document at any time as per its discretion.

## Metrics

- The metrics which shall be measured by the Security In-Charge's office but not restricted to.
- The periodicity of measurement reporting shall be once every quarter.
- Following are the metrics to be measured:
  - Number of vendor accesses approved v/s number of requests.
  - Number of reported information security incident with regards to vendors
  - Number of instances where on expiry of vendor contracts, access rights were not disabled.
  - Numbers of accesses which were given without carrying out of vendor risk assessment and/or without signing of confidentiality/non- disclosure agreements.
  - Unmitigated High-Risk areas identified for Critical Vendor.

## Exceptions

- 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.
- Exceptions to this Policy and Procedures shall have to be allowed at the time of implementation of this policy and procedures or at the time of making any updation to this document or after implementation on an ad-hoc basis as per business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.
- Any exceptions during implementation shall be submitted by the HODs responsible for the particular vendor. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.

- The Security In-Charge shall review all exceptions, as the case may be, every year for validity and continuity.

## Disclaimer

- JMBGRP reserves all rights and is the exclusive owner of all intellectual property rights over this Acceptable usage Policy and Procedures document. This document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (such as electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior consent from the Apex Committee. The Acceptable usage policy and procedure document is meant to be published on the intranet of JMBGRP and/or any other forum as decided by the management of JMBGRP. Anything not specifically stated in this Acceptable usage policy and procedure document shall not be considered as implied in any manner.
- For any clarifications related to this Acceptable usage policy and procedure document with respect to its interpretation, applicability and implementation, please raise a request at Ticketing Tool.

## References:

- Controls: A.7.2.2

**Annexure- B: Vendor Risk Assessment Form**

(This form is to be filled for Vendors for whom Risk Assessment is required)

## Vendor Information

| | | | | | | |
|---|---|---|---|---|---|---|
| Name of the Company: | | | | | | |
| Company Address: | | | | | | |
| | City: | | PIN: | | Phone: | |
| Type of Business: | | | | | | |
| No of Employees: | | | | | | |
| Name of SPoC: | | | | | | |
| Contact Details of SPoC: | Mobile: | | | | | |
| | Landline: | | | | | |
| | E-mail: | | | | | |
| Brief description of the services being offered by the vendor: | | | | | | |
| Names of employees Deputed on site for service (If Applicable): | 1.) | | | | | |
| | 2.) | | | | | |
| | 3.) | | | | | |
| | 4.) | | | | | |

**Vendor Evaluation**

**Please add more evaluation factors if desired.*