Information Security Management System
Personnel Security Policy & Procedure

Document no. JMBGRP/ISMS/Pol-PS

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document is to clearly define what the employee shall do prior to employment, during the course of employment and finally during change of employment status/transfer/retirement or termination	
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	18.08.2023	Manish Jaiswal (Group CTO)	Document reviewed. Modification done to “References”	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: “Policy Statement, Exceptions, Disclaimer”	

Contents

Purpose

JMBGRP recognizes that its employees are its assets, and they are the primary drivers of the organization's business and vision. It has become imperative that JMBGRP clearly define what the employee shall do prior to employment, during the course of employment and finally during change of employment status/transfer/retirement or termination. The policy defines as to what shall be the measures JMBGRP shall adopt at each stage of employment in context of adherence to the Information Security posture; which JMBGRP wants to establish, maintain and sustain.

Scope

The policy document is applicable to:

- All Locations of J.M Baxi Group in India
- All Employees of J.M Baxi Group
- All Third party/ Contract employees working for J.M Baxi Group

Policy Statement

The personnel security policy shall address all the attributes from the time of pre-selection of the employee till the time the employee is relieved by the organization. It shall also ensure that the selected employee is integrated into the work culture and ethics of the organization effectively. These attributes are mentioned as under:

- Pre-employment
    - Information Security related roles and responsibilities of employees and contractors shall be defined and documented with due consent from the stakeholders, in accordance with the JMBGRP's information security framework.
    - As part of their contractual obligation, employees shall be required to sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.
    - Background checks shall be done either through JMBGRP's HR department or through an approved third party.
- During the Employment
    - Management shall mandate the employees to apply security in accordance with established information security policies and procedures.
    - Management shall ensure that employees are briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems; and they are provided with guidelines to congregate security expectations of their role within the organization.
    - All employees of the organization shall receive awareness training and regular updates in organizational policies and procedures, as relevant for their job function to achieve a level of awareness on security relevant to their roles and

responsibilities within the organization and continue to have the appropriate skills and qualifications.

- There shall be a formal disciplinary process for employees who have violated laid down policies of JMBGRP and action shall be taken, where relevant, as per JMBGRP Code of Conduct (JCoC) to ensure correct and fair action.

- Termination of employment
  - There shall be a formal procedure in place for handling separation of employees from the organization and responsibilities for performing employment termination of employment shall be clearly defined and assigned.
  - The access rights of all employees to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or suitably adjusted upon change in coordination with IT Department.

Procedure

Pre-employment

1.1 HR department shall ensure that pre-employment screening/background checks are performed on all the selected candidates on acceptance of the offer letter. This shall be done for the recruitment of temporary employees, permanent employees and contract employee.

1.2 Shortlisted candidates should be made to submit photocopies of all the documents required and intimation of the same shall be done through the welcome mail sent to the selected candidate. Documents including but not limited to:

1.2.1 Release Letter from current employer (if the candidate was employed in past);

1.2.2 Proof of prior work experience (if the candidate was employed in past);

1.2.3 Proof of Date of Birth (School leaving certificate / Passport / Driving License);

1.2.4 Certificates supporting Academic and Professional qualifications (from School to Last degree) with mark sheets;

1.2.5 Photographs;

1.2.6 PAN card copy;

1.2.7 Passport copy (first two pages and last page), if available;

1.2.8 Last three Pay slips (if the candidate was employed in past)

1.2.9 Duly filled Personal-cum-family Information

1.2.10 Appointment offer letter from J.M Baxi Group

1.3 If it is not possible for the candidate to furnish any of the aforementioned documents at the time of joining, he shall be required to submit an Undertaking stating the proposed date for submission of the documents.

1.4 JMBGRP shall conduct the screening through its own offices or shall employ any other external agency to execute this task.

1.5 The checks shall include the following:

1.5.1 Reference check:

1.5.1.1 Minimum three references shall be taken from the candidate. Preferably one reference should be candidate's previous reporting manager.

1.5.1.2 If the previous reporting Manager is not available, then colleagues from the previous company shall be contacted for reference check.

1.5.1.3 References shall be contacted to assess the correctness of the information provided by the candidate.

1.5.1.4 Records must be maintained for reference checks done.

1.6 Background verification of the candidate undertaken by an appointed agency to carry out some or all of the below-mentioned checks on the prospective candidates and submit the report to HR for further action:

1.6.1 Academic (Except in the case when recruited from campus) and Professional qualifications.

1.6.2 Previous employment check (will be done with the previous employer, not the current employer. Specific inquires shall be made regarding the candidate's performance and conduct).

1.6.3 Correctness of remuneration received at the previous company.

1.6.4 Criminal Records, Incidents related to Governance Violations, Ethical Misconduct and Conduct through social media shall also be checked.

1.6.5 For any misrepresentation of information, submission of incomplete information or information has been withheld; then the candidate's candidature shall be liable to be terminated without notice.

1.6.6 Respective contractors shall provide positive assurance and police verification records for screening for their personnel /contract workers deployed in JMBGRP. Contract /Outsourced work refers to officials, executives, drivers, on-roll security including guest houses, housekeeping, medical staff etc. In the instance that the screening was not carried out or has resulted in any cause of concern, a notification must be duly sent to JMBGRP stating the same.

1.6.7 For each level few additional checks need to be incorporated. These checks are detailed as follows:

1.6.7.1 Employment verification checks.

1.6.7.2 Verification of the employment agreements & NDA's of current and previous organizations related to the projects involving the candidate.

1.6.7.3 Check of any infringement, Governance Violations, Ethical Misconduct, IPR related cases, ongoing/ pending with previous or current employer.

1.6.7.4 Legal check including NDA and other agreements signed by candidate in current and previous companies including criminal records if any.

1.6.7.5 Socioeconomic and lifestyle profiling.

1.6.7.6 In case of any of the above not being done, the responsibility towards hiring shall be with the immediate reporting manager.

1.6.7.7 For employees on contract as hired by JMBGRP in the stated categories, the abovementioned steps shall apply.

1.7 The candidate shall confirm his/ her date of joining with acceptance of offer/ appointment letter in writing.

1.8 All appointment letters shall originate from the HR department only.

1.9 The appointment letter shall include/ take care of the following:

1.9.1 The terms and conditions of the employment

1.9.2 Clause that employee will maintain adherence and compliance to JMBGRP Code of Conduct including confidentiality/ non-disclosure requirements of JMBGRP's information; clauses on protecting JMBGRP's assets including proprietary information and intellectual property and maintaining the integrity of data furnished.

1.9.3 State that employee information security responsibilities extend outside JMBGRP premises and normal working hours whenever appropriate, as in the case of working from home/ working offsite;

1.9.4 Clarify the employee's legal responsibilities and rights (e.g. regarding copyright laws and data protection legislation);

1.9.5 Where appropriate, employee information security responsibilities shall continue for a defined period after the end of employment. This relates to the confidentiality agreement/ NDAs.

1.9.6 Specific mention on breach of information security resulting from non-compliance of the policies and procedures laid down for the same resulting in appropriate disciplinary action against the employee(s).

1.9.7 The company's right to monitor any or all of the activities of the employee during the course of any investigation whether criminal or otherwise.

1.9.8 The company's right to monitor the usage of and audit all personal items/ equipment/ devices that may be/ are used by employees to access/ store/ use/ transmit company's information and information resources.

1.9.9 Statement that the contents of the offer/ appointment letter have been read and understood by the employee and signed by the employee in duplicate and a copy returned to JMBGRP's record.

1.10 The entire process as stated above shall be administered through a Governance Tool or managed through a Portal.

1.11 The abovementioned clauses shall be applicable for personnel on contract and third-party personnel working on the premises of JMBGRP.

During the Employment

1.12 Upon joining the employee shall first sign the JCoC and the joining note which shall clearly state that the employee has read and understood the terms and conditions of the employment. A signed copy of the same shall be returned to the HR department.

1.13 Upon joining, the employee shall undergo an induction program, which shall provide information about the organization, its businesses, its vision and expectations from employees and the information security posture adopted.

1.14 Adequate material may be provided by way of an induction kit (Docket on code of conduct, Handbook on information security, AV Tools such as training movies) to the employee.

1.15 A sign off shall be taken from the employee at the end of the induction program on adherence to the policies and procedures set forth by JMBGRP. The employee shall also sign off stating that he/she has clearly read and understood the vision and business expectations from the employer in discharging his or her roles and responsibilities.

1.16 Any information which has to be shared in the public domain shall be routed corporate communication department. [Refer JCoC]

1.17 The use of social media on the company's assets shall be controlled as per the Acceptable Usage Policy and Procedure and BYOD Policy and Procedure.

1.18 All employees shall display their identification badge when on office premises.

1.19 For any loss of the identity badge, the employee shall inform the Dept. Head, HR and the Gate pass section of the location immediately through an e-mail/phone. The Gate pass section shall acknowledge the receipt of this mail within 1 hour from receipt and block access rights of the card which has been reported to have been misplaced or lost.

1.20 When the employee leaves the organization, the access card shall be returned to Gate pass section by the HOD.

1.21 By default, all employees shall not be permitted entry to the identified secure areas like server rooms/data center etc. at locations.

1.22 The list of banned items is applicable for employees/ external parties as well.

1.23 All employees will adhere to local security setup during entrance in the premises or at the gate.

1.24 Information Security Awareness

1.24.1 Management shall ensure that all the employees and contractors understand and follow the information security policies and procedures.

1.24.2 The HR department shall ensure that the:

1.24.2.1 Information security policies are accessible to all the employees. These shall be made available on the Intranet or through a booklet or any other suitable medium such as a portal.

1.24.2.2 Employees shall be given appropriate information security awareness training at the time of induction and on a periodic basis as needed or based on the training calendar.

1.24.3 HODs shall ensure that contractors related to their department follow the information security policies and procedures.

1.25 Granting Physical and Logical Access

1.25.1 HR and the Employment Cell at HO/ Admin teams at other locations shall facilitate physical access for new employees. HR / Identity Manager shall verify the access required and facilitate the creation & assignment of Access Card/ID card for the new employee. This shall also include recording of the Logical Access which is to be provided to every new employee. The Identity Management Process shall be managed through an appropriate management tool which shall be managed by HR and IT and shall include a Sign Off from the concerned HoD for any change of access rights or revocation of the same on account of change to location/business/department / sabbatical and or resignation from the job.

1.25.2 JMBGRP reserves the right to install video surveillance equipment on premises should it feel the need to do so.

1.25.3 For logical access, refer to the IT Security Procedure (Access Control).

1.25.4 For issue of IT assets, refer to the (Acceptable Usage Policy and Procedure).

1.25.5 As regards Bringing Your Own Device (BYOD) is concerned, this shall be governed by the BYOD Policy & Procedure.

1.25.6 HR and Security In-charge shall have right to push company policies to these devices and audit the devices on a random basis to check for any violation. Should this not be considered acceptable, then the BYOD shall not be permitted to connect to the network.

1.25.7 Sharing of credentials in logical and physical form shall be regarded as a security violation and the employee shall face appropriate disciplinary action.

1.25.8 The above-mentioned clauses shall be applicable for employees on contract or third-party personnel working on the premises of JMBGRP.

1.26 The entire process as stated above shall be administered through a Governance Tool or managed through a Portal.

1.27 The abovementioned clauses shall be applicable for personnel on contract and third-party personnel working on the premises of JMBGRP.

Termination or Change of Employment

1.28 Change of Employment

1.28.1 Change of employment can occur due to transfers, promotions in existing business roles, transfers in new/additional business roles. In all the cases, there could be a change required in the access rights granted to the employee.

1.28.2 All the memos/circulars relating to transfers/promotions/changes in business roles shall originate from the HR department.

1.28.3 The HR department shall issue a transfer letter to the employee with a copy of the same to the administration and IT teams including the current HOD/ business head and Head of the department to which the employee is being transferred. They shall take care of the following:

1.28.3.1 HoD: Begin relieving formalities and ensure that department specific assets are retrieved from the employee. These assets could include tools, keys to storage cabinets/department/etc., safety equipment, manuals, documents and so forth. Existing logical access rights which are not required for the new portfolio shall be communicated to respective IT team for revocation and confirmation for revocation for the same received. HR shall intimate IT of the change and confirm that the communication has been done to the HOD.

1.28.3.2 IT Department: Ensure that all the existing rights which are not required for the new portfolio are be revoked as intimated by current HOD/ business head and HR. After revocation, IT department must send a confirmation of revocation to the departments which sends the request for revocation.

1.28.3.3 Administration Department: Ensure that all the assets issued by Administration department (Mobile, Vehicle Keys & Papers, Identity Card, Credit Card, etc.) and physical access rights are revoked wherever relevant.

1.28.3.4 Any additional access rights required by the employee being transferred should be approved as per the Access Control policy and an identity management system shall be instituted to ensure that all logical access rights are revoked in accordance with the requirement for the changed role.

1.29 Termination of Employment

1.29.1 Termination of employment can happen by way of resignation / retirement / termination of service / absconding from service.

1.29.2 The contract of employment shall be terminable with or without any reason by either party by giving the requisite period of notice in writing.

1.29.3 No notice period is necessary if the employee is asked to leave the organization for any fraud, misconduct, morally unacceptable behavior, indiscipline or incompetence (for termination case).

1.29.4 HR department shall inform the current HOD, IT, Finance, Administration and other relevant departments/ agencies, as applicable, about the employee being relieved/ terminated from the organization. The concerned departments that are intimated, shall exercise their termination responsibilities as follows:

1.29.4.1 HOD: Upon accepting the resignation/ termination notice of the employee, the HOD/ Business HR shall send an email to the employee with a copy to HR who will begin relieving formalities and ensure that department specific assets are retrieved from the employee. It is the responsibility of the HOD to ensure that all business assets with the employee are not misused during the notice period. The HOD/ Business head and HR also reserves the right to have IT assets, information and facilities' rights ceased during the notice period.

1.29.4.2 Administration / HR: Ensure that all the assets, of which Administration/HR department is the custodian, (Mobile, Vehicle Keys & Papers, and Identity Card, Credit Card, Lease Accommodation, furniture & fixtures etc.) and physical access rights are revoked wherever relevant.

1.29.4.3 IT: IT shall ensure that the access logs of the employee are maintained as per the contractual and or regulatory requirement from the date of resignation and start of the notice period from the HR department to the date of relieving. As soon as the intimation of removal of access rights is received it should be put into action and confirmation of the same sent to the originating agency.

1.29.4.4 Reconciliation of access rights revoked.

1.29.4.4.1 At the end of every month HR shall send a list of terminated employees to IT to ensure reconciliation of access rights revoked.

1.29.4.4.2 IT shall reply by mail confirming revocation of access rights.

1.29.4.5 **Finance / Commercial Department:** To revoke rights like authorized removal from directorship or any other position given to the employee.

1.29.4.6 **Legal Department:** To revoke Power of Attorney, if applicable.

1.29.4.7 **Corporate Communication:** To ensure updation of web sites and other press releases, and in the communication as it is made with the external world and stakeholders.

1.29.5 The management approval shall be required from a member of the IL1 (Apex Committee or Security In-charge) to monitor employee's activities during his notice period. The request for the same shall originate from the HoD and seconded by the Security In-charge

1.29.6 HR Department shall conduct the Exit Interview and the same is to be documented.

1.29.7 Following procedure to be followed on termination / last working day:

1.29.7.1 The HR department shall collect the sign offs on the No Due Certificate Form from various departments for termination or change of employment. The signoffs shall be from the concerned Supervisors, HODs, Unit Heads, Administration Department, IT Department & Finance Department.

1.29.7.2 As an interlock to ensure that the clearance is carried out across all functions, the relieving letter / Service Certificate and eventually the final settlement must only happen after the clearance certificate is submitted complete in all aspects.

1.29.7.3 In case of termination, the entire clearance process shall be carried out within the timeline as per HR policy. Under the sole discretion of the HOD and HR, the employee's physical and logical access rights may be restricted within this period.

1.29.7.4 An identity management system shall be instituted to ensure that all logical access rights shall be revoked in accordance with the requirement.

1.29.7.5 HOD shall provide sign off for the following:

1.29.7.5.1 Return of information and other assets in the possession of the employee.

1.29.7.5.2 That the outgoing person has had meeting /handholding/handover with the new joiners and explained the responsibilities of the designation being handled and the new incumbent has understood the same.

1.29.7.5.3 The sign off shall be between the HOD, the new joiners and the outgoing employee.

1.29.7.5.4 Back up of all data in digital and non-digital form has been taken.

1.29.7.5.5 Formatting of the user data is done post taking concurs from Respective Authority/ HOD.

1.29.7.5.6 The computing device(s) is returned to IT Inventory.

1.29.7.5.7 The above-mentioned steps shall be recorded on a portal and signed off by the HOD

1.29.7.6 Administration Department shall provide sign off for the following:

1.29.7.6.1 Retrieval of Photo/Access Badges.

1.29.7.6.2 Retrieval of other assets (Mobile, Vehicle Keys & Papers, Identity Card, Visiting Cards, Credit Card, Lease Accommodation, furniture & fixtures etc.) of which Administration is custodian.

1.29.7.6.3 The same shall be recorded on a portal and signed off by the HOD.

1.29.7.7 IT Department shall provide sign off for the following:

1.29.7.7.1 Removal of logical access rights.

1.29.7.7.2 Retrieval of other assets (e.g. Laptops, Phones, Tokens amongst others) of which IT is the custodian.

1.29.7.7.3 Forwarding of mails to the reporting manager until such time a new incumbent joins the department and archiving of the mails.

1.29.7.7.4 In case where resigned employee's user account needs to be maintained for official purposes or if the application does not permit to remove the user account, then passwords of these accounts should be changed on the last working day of the employee and retained by the concerned HOD.

1.29.7.7.5 The abovementioned steps shall be recorded on a portal and signed by the HOD.

1.29.7.8 Finance Department shall provide sign off for retrieval of signing authorization, removal from directorships or any other position given to the employee.

1.29.7.9 Legal Department shall provide sign off for retrieval/ removal of Power of Attorney.

1.29.7.10 The responsibility for implementing this procedure lies with following personnel:

1.29.7.10.1 Human Resources

1.30.7.10.2 Head of Departments

1.30.7.10.3 Support by IT during each phase of employee engagement.

1.30 The entire process as stated above shall be administered through a Governance Tool or managed through a Portal.

1.31 The abovementioned clauses shall be applicable for personnel on contract and third-party personnel working on the premises of JMBGRP.

Responsibilities

The responsibilities lie with the following personnel:

- HR Department:
  - To formulate the terms of employment and the confidentiality agreements.
  - To conduct pre-employment screening/background checks.
  - To define and include the employees' Information Security responsibilities in their job profile.
  - To arrange and impart information security training for the user.
  - To ensure that the signoffs are received from the relevant departments before any employee is relieved in case of any internal movement or separation of employees.
- HODs:
  - To ensure that all employees are aware of the Information Security responsibilities as a part of their job description.

Enforcement:

- This policy and procedure is applicable for all the employees 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.
- 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 shall be generated by the HR Department once every 90 days.
- The points include as given below, but not restricted to.
    - Time taken to provide users with various access rights and time taken to remove all access rights when the person resigns/retires/re-locates/is terminated. Number of assets for which supplementary controls are applied.
    - Number of personnel who have undergone induction/ trainings vis-à-vis the total no of employees joined.
    - Violations caused by employees and IT and Non-IT and action taken.
    - Number of complete incomplete clearance documents.
    - Number of assets lost by employees and action taken.
    - Number of incidents related to data loss due to process negligence.
    - Number of assets to be returned by employee vis-à-vis to the ones which have been received.
    - Number of exceptions requested, and number of exceptions granted against this policy.
    - Number of records pending closure on the Portal/Governance Tool / Identity Management Tool.

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 Security Policy and Procedures shall 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 shall be of temporary or permanent in nature.
- All exception requests shall be submitted by respective HODs/ Business Security In-charges. 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 the request in Ticketing Tool.

References:

- Controls: A.6.1, A.6.2, A.5.4, A.6.3, A.6.4, A.6.5