Information Security Management System
Physical 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 prevent unauthorized physical access, damage, and interference to the JMBGRP and protect information assets.	
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)	Document reviewed. Modifications done in Section: "4,5"	

Contents

1. Purpose

1.1. The purpose of the policy is to prevent unauthorized physical access, damage, and interference to the JMBGRP companies, and to protect JMBGRP companies' information assets from theft, intentional or unintentional, misuse and natural or manmade disasters.

2. Scope

2.1. This policy is applicable for all locations of JMBGRP industries. It is also applicable to all employees, business associates, contractors, vendors, visitors, customers, trainees, housekeeping staff, facility management staff, and consultants who visit and work on its premises for limited or extended periods of time.

3. Policy Statement

3.1. The selection and implementation of the Physical security controls shall satisfy business need and provide adequate deterrence against any intended or unintended breach by employees, visitors, third parties and at the same time not be disruptive to business processes and requirements.

3.2. Physical security policy and procedure document shall establish a physical security framework to protect and preserve information and various physical assets by addressing the following areas:

3.2.1. **Perimeter Security:** There shall be a formal managed process which shall implement personnel and technical controls to achieve the desirable security level for the perimeter.

3.2.2. **Surveillance:** It shall address the complete electronic surveillance process involving the site selection and the rationale. It shall also define operational and maintenance procedures.

3.2.3. **Access Control:** It shall address the access mechanism to manage the movement of employees and third-party personnel within JMBGRP premise, during and beyond office hours. Covering the process of accessing secure area by employees, visitors, vendors and third-party personnel. Involving the procedural and technological measures to safeguard the secure areas effectively.

3.2.4. **Security Organization:** The location Manager H.R. & Admin/Security In-Charge has the responsibility of implementing the Physical Security Policy and associated Procedures in their respective locations.

3.2.5. **Visitor Management:** It shall cover the selection and implementation of the controls to manage the movement of visitors within JMBGRP premises.

3.2.6. **Vehicle Management:** It defines the process to identify, monitor and control vehicular traffic inside the premises and to restrict the movement of any unauthorized movement inside the premises.

3.2.7. **Material Management:** There shall be a formal documented process to deploy the necessary measures to manage the incoming/outgoing movement of material.

3.2.8. **Key Management:** There shall be a formal documented process to handle the Key Management.

3.2.9. **Waste/ Scrap Disposal:** Controls for managing the disposal of all kind of waste generated in JMBGRP is addressed by implementing the necessary measures.

4. Procedure

Perimeter Security

4.1.General:

4.1.1. In order to protect JMBGRP premises from unauthorized access, perimeter security implementation shall be standardized.

4.1.2. Wherever applicable, to secure the JMBGRP premises from intrusion and trespassing the height of the perimeter wall /fencing shall be at least 8 feet or above.

4.1.3. Wherever applicable, in order to prevent any trespasser from jumping over perimeter walls, concertina coils/barbed wire fence shall be installed, on the perimeter to make crossing over difficult.

4.1.4. **Perimeter Patrolling:** Wherever applicable, a 'Patrolling plan' will be decided by location Manager HR & Admin /Security In-Charge. The patrolling plan should be as follows:

4.1.4.1. The location Manager HR and Admin/Security In-Charge shall daily instruct the Security Supervisor to patrol the premises at random time on hourly basis.

4.1.4.2. A consolidated report on patrolling should be submitted to the location Manager HR and Admin/Security In-Charge daily either in hard copy or on mail.

4.1.4.3. Any unusual activity/incident should be reported to the location Manager HR and Admin/Security In-Charge immediately and also must be mentioned in the patrolling report.

4.1.4.4. The condition of the perimeter wall, perimeter gates, guard posts, perimeter lighting shall be reviewed monthly by the respective location Manager HR and Admin/Security In-Charge.

4.1.5. Internal Area zoning: All locations of JMBGRP will be sub-divided internally to provide additional security to vulnerable areas for either operational, business or regulatory/legal reasons. Procedures related to Internal Zoning shall be applicable for all location categories and are as under:

4.1.5.1. **Zone 1 Common Areas:**

4.1.5.1.1. Entry of all non-business visitors like couriers, delivery boys or any other personnel accompanying the visitor shall be limited to this zone. Security would be responsible to ensure their movement to be restricted to this area.

4.1.5.1.2. Common areas (reception/main gate/visitor meeting room) shall be manned appropriately. Electronic surveillance especially at main entrances and exits to the floors/buildings may be planned to supplement the physical guarding effort.

4.1.5.2. **Zone 2 Work Areas:**

4.1.5.2.1. Employees can access this area.

4.1.5.2.2. Visitors on official business will be allowed after confirmation of the visit by the employee/executive concerned working in that area.

4.1.5.2.3. Photography shall not be permitted in work areas without prior permission.

4.1.5.2.4. Employee awareness regarding display of identity cards and questioning of persons without visible identification, will be raised by conducting awareness sessions.

4.1.5.2.5. Authorization for entry to the office on holidays: - In case of entry to the office on holidays, HOD of the concerned department would send a request mail to the Admin Manager seeking the permission for the concerned employee to work on holidays. The same shall be communicated to the location security.

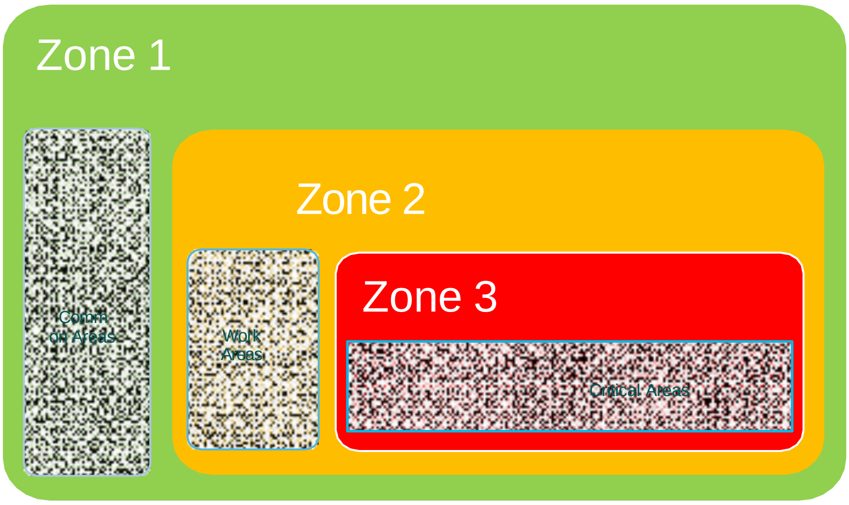
4.1.5.2.6. Senior management cabins shall be locked during non-occupancy.

4.1.5.3. **Zone 3 Critical areas:**

4.1.5.3.1. Those areas in a location which for business, operational reasons entry is restricted. Only staff requiring access to conduct their assigned work will be permitted into these areas. Such as server room, document room, R&D, QC, and EPBAX room.

4.1.5.3.2. Visitors will generally not be permitted in these areas. In case they need to access these areas for operational reasons, they shall be escorted in and out of the area by the host or his nominee.

4.1.5.3.3. Critical areas shall display clear signage mentioning restricted entry into the area.



4.2. Surveillance:

4.2.1. Electronic surveillance is an important control that serves as a deterrent against potential threats, as a monitoring tool and investigation (wherever required). A well- planned surveillance system supplements the guarding effort within a location.

4.2.2. Following points should be considered while planning a surveillance system

4.2.2.1. Security objective.

4.2.2.2. Hours of operation.

4.2.2.3. History of loss / experience.

4.2.2.4. Possibility and extent of loss.

4.2.3. The decision for live monitoring vs. recording review shall be taken by the respective location Manager HR and Admin/Security In-Charge in consultation with concerned senior management staff. Recording history duration (preferable 30 days) shall also be decided and the recording media procured accordingly.

4.2.4. The camera feed shall be available for viewing by authorized individuals only, on the company network. An authorization matrix shall be devised to decide on viewing rights. Access to the system shall be controlled by individual identity and password.

4.2.5. Recording will be done on a Digital Video Recorder (DVR). In case of migration to advance technology, the recording can also be done on Network Video Recorder (NVR) or NAS/SAN storage, as per the compatibility with future technology deployed.

4.2.6. The location Manager HR and Admin/Security In-Charge or a person designated by him shall be responsible for random live monitoring and randomly viewing previous day's recording clips. Records shall be maintained by the designated reviewer of the clips reviewed by him /her, observations (if any) and the action taken.

4.2.7. The location Manager HR and Admin/Security In-Charge or a person designated by him will be responsible for ensuring trouble free operation of the entire surveillance system.

4.2.8. The following shall be checked:

4.2.8.1. Satisfactory camera angles and clarity with varying light conditions.

4.2.8.2. Quality of recorded images.

4.2.8.3. Proper functioning of recording devices.

4.2.8.4. It will be ensured that Annual Maintenance Contracts (AMCs) for the surveillance systems are in place.

4.2.8.5. The maintenance schedule and maintenance / service reports shall be reviewed on a monthly basis by the location Manager HR and Admin/Security In-Charge.

4.2.8.6. Test results will be maintained, and corrective actions initiated as required.

4.3. Access Control:

4.3.1. General:

4.3.1.1. 'No card – no entry' policy will be followed at JMBGRP premises. Compulsory display of identity card by employees and third party staff at entry and while inside the office premises will be ensured. In case of third party/contractor/ vendor staff, their employer issued photo identity card supported by JMBGRP card issued will be checked before entry.

4.3.1.2. To ensure comprehensive and consistent control a Photo Access card, is recommended. The Access cards will be further sub divided in the following categories:

- Photo Card - Employee Card – Saffron lanyard
- Third party staff - Green lanyard
- Visitors – Green lanyard
- The lanyard's color choice assists in ease of identification in the premises & it is company's privilege to choose the colors.

4.3.1.3. Security at the main entry/exit shall ensure due physical checking / frisking of the third party / contractor/vendor staff.

4.3.1.4. For defining access levels, a detailed audit of the location shall be carried out & the premises to be divided into zones.

4.3.1.5. Critical Areas Access:

4.3.1.5.1. Access to the critical areas to be restricted by electronic access control system.

4.3.1.5.2. Access to other critical areas shall be controlled by a stringent authorization process. Only employees, staff working there will be allowed access to these areas. For others a written approval by the concerned department heads will be sought.

4.3.1.5.3. Access to these areas will be limited to the employees working on these particular areas. Approved by their respective department heads.

4.3.1.5.4. Periodic review of the access control logs shall carried out by the concerned department head or by any employee identified/authorized by the concerned department head.

4.3.1.5.5. Periodic reconciliation of access rights to be carried out.

4.4. **Security Organization** –The location Security Process Owner shall have the responsibility of implementing the Physical Security Policy and associated Procedures in their respective locations. His responsibilities will be to:

4.4.1. Customize security procedures to ensure effective implementation of the Physical Security Policy disseminate and implement the Security Policy and Procedures.

4.4.2. Conduct physical security inspections by day and by night to ensure compliance to the procedures.

4.4.3. Ensure due physical checking / frisking of third party / contractor/vendor staff during entry / exit.

4.4.4. Define guard manpower requirements, duties and training requirements.

4.4.5. Carry out weekly audits of records related to access card issue, visitor management procedure, vehicle management, material movement, security and safety equipment check and others for gaps in implementation and / or unusual trends.

4.4.6. Provide guidance to the security staff on the implementation of secure workplace principles and conducting no-notice checks to ensure compliance.

4.4.7. Ensure that physical security equipment [e.g. CCTV, electronic access controls, and fire alarms system and fire extinguisher equipment/system etc.] is inspected on a regular basis to ensure that it is functional.

4.4.8. Facilitate internal/external physical security audits.

4.4.9. Assess emerging threats; align security procedures to combat these, and keep the management informed of developments.

4.4.10. Escalate excessive risks to the management.

4.4.11. Liaise and maintain good working relations with local security and law enforcement authorities.

4.4.12. Conduct awareness program for new joiners and refresher program for existing employees on security awareness.

4.5. Security Guards:

4.5.1. Followings are the duties of the security guards;

4.5.1.1. JMBGRP premises shall be manned 24x7 (round the clock) through a duty roster managed by location Physical Security Owner. The location Security Process Owner shall review the guard roster for attendance and the positions at which they are stationed.

4.5.1.2. Security guards shall be present at the entrances and exits of the JMBGRP premises.

4.5.1.3. Security room near entry gate has to maintain a separate registers for recording visitor /customer/ vendor/ third party/ vehicle movement and material in/out record.

4.5.1.4. Security guard will check doors and windows during his patrolling post working hours and shall report any defect in their condition.

4.5.1.5. The guard will check the vehicles during entry and exit from the premises.

4.5.1.6. The guards will be trained to identify devices like Recording Devices and Camera / Mobile Phones.

4.5.1.7. The guards will be trained in aspects of Information Security such as Social Engineering.

4.5.1.8. The guards will maintain registers and shall monitor material(s) movement.

4.5.1.9. Induction training to the security guards should include capsule on both information and physical security and safety (AV film, security and safety booklet – with emergency numbers).

4.5.1.10. Quarterly training of guards on fire-fighting, emergency response (mock drills) and first-aid in addition to role-training.

4.5.1.11. Guards to be trained on first aid and fire-fighting.

4.5.1.12. A rotation plan, which ensures that all guards shall be rotated weekly, shall be prepared by the security officer/supervisor.

4.6. Keys Management:

4.6.1. List of authorized personnel to draw keys should be available with the security personnel.

4.6.2. Employee shall be issued a key by the Security staff only if he/she has an approval from the respective Department Head.

4.6.3. The authorized employees shall take the keys of respective department and make an entry in the register kept for the purpose at the Security cabin.

4.6.4. All the keys shall be held in a locked cabinet/cupboard in the security room near main entry gate.

4.6.5. A duplicate set of all the keys shall be maintained in a locked cabinet/ cupboard in the location Manager HR and Admin/Security In-Charge’s cabin.

4.6.6. If a key is lost, the employee shall immediately inform the location Security In-Charge, who will take appropriate action.

4.6.7. Reconciliation of all keys to be done by the security supervisor at the end of the day. In case of any deviation the instance to be escalated to the location Security Process Owner.

4.7. Visitor Management: All movement of Visitors going in & out of the premises shall be authorized and recorded.

4.7.1. Security Guidelines for Visitors

4.7.1.1. All visitors must comply with the security and safety guidelines as specified by JMBGRP.

4.7.1.2. Visitor entry to the JMBGRP would be subject to permission from the host/ department head.

4.7.1.3. Appropriate and prominent signage to inform visitors about CCTV surveillance monitoring and safety shall be put up inside JMBGRP premises.

4.7.1.4. A list of unauthorized material as specified by JMBGRP shall be displayed at the gate, which unless specially authorized, is prohibited inside JMBGRP premises.

4.8. Visitors are further categorized as VIP visitor & Non VIP visitor.

4.8.1. VIP Visitors : Following personnel shall be categorized as VIP visitors:

4.8.1.1. Foreign delegates

4.8.1.2. Business Partners

4.8.1.3. Government Officials (based on their designations)

4.8.1.4. Law / Enforcement Department (based on their designations)

4.8.2. VIP Visitors Entry and Exit:

4.8.2.1. VIP Classification for the visitors shall be done by the host based on the business criticality, socio-political status or any other factor distinguishing the status of the visitor. (VIP status of a visitor shall be decided by the department head and shall initiated to the Location Manager / H.R. & Admin / Security Process owner in advance)

4.8.2.2. Time restrictions for entry shall not be applicable to this class of visitors.

4.8.2.3. The details of the VIP visitor shall be obtained from Host or the authorized personnel at least 2 – 3 hours in advance, to ensure minimum discomfort to the visitor. The detail required shall be as follows:

4.8.2.3.1. Number of visitors.

4.8.2.3.2. Name of visitor

4.8.2.3.3. Organization

4.8.2.3.4. Purpose of visit.

4.8.2.3.5. Expected time of arrival and departure.

4.8.2.3.6. Name of host.

4.8.2.3.7. Host / authorized personnel shall be present at the gate to receive the VIP visitor(s).

4.8.2.4. Based on the information provided by the visitor, a visitor card shall be issued for the VIP visitor(s). These shall be collected by the host on behalf of the VIP visitor(s).

4.8.2.5. The host shall then escort the visitor to the respective meeting place.

4.8.2.6. The receiving person will also escort the visitor during his exit and ensure visitor exit procedure is complete.

4.8.3. Non-VIP Visitors - Non VIP visitors are further categorized as:

4.8.3.1. Consultants

4.8.3.2. Vendors

4.8.3.3. Auditors

4.8.3.4. Business Visitors

4.8.3.5. The visitor management at Main Reception / Floor Reception shall ensure proper visitor registration of all visitors.

4.8.4. All Non VIP visitors shall declare their electronic items such as laptops, cameras, CDs, Pen drives and other such material.

4.8.5. Where ever applicable VMS operator shall capture all the details of the visitor in the system, such as, visitor's name, address and contact number, name of the host / department, purpose, organization name, time of the meeting and visitor card number. Else, record the same details in a separate visitor register.

4.8.6. Visitor card shall be issued to all visitors with a VMS generated visitor slip (wherever applicable).

4.8.7. Non VIP Visitor Entry and Exit

4.8.7.1. Entry:

4.8.7.1.1. At the main gate / reception, the Visitor management desk/Security desk shall ensure the authenticity of the visitor by verifying the identification proofs of the visitor by asking for govt. ID.

4.8.7.1.2. Host confirmation shall be carried out and the visitor pass is issued post the host confirmation.

4.8.7.1.3. Wherever applicable the Visitor Management Operator shall capture all the details of the visitor in visitor management system / visitor register such as:

- Name of the Visitor
- Address of the Visitor
- Contact Number
- Name of the Host & Escort
- Host Department
- Purpose of the visit
- Time of the Visit Visitor
- Badge Number Material Declared

4.8.7.1.4. Visitors are requested to declare their electronic items such as:

- Laptops, Pen drives and CDs
- Cameras

- Material declaration slip shall be issued to the Visitor. Material declaration slip shall capture
- Laptop Make, Serial Number and Qty
- Number of Pen drives and CD’s

4.8.7.1.5. Material declaration slip shall be issued to the Visitor. Material declaration slip shall capture:

4.8.7.1.5.1.1. Laptop Make, Serial Number and Qty

4.8.7.1.5.1.2. Number of Pen drives and CD’s

4.8.7.1.5.3. Digital and Video cameras are allowed only after the prior approval from the department head.

4.8.7.2. When in premises:

4.8.7.2.1. All visitors shall prominently display their visitor badge while they are inside the premises

4.8.7.2.2. Host will escort the visitor all the time during the stay of visitor.

4.8.7.3. On Exit:

4.8.7.3.1. Security at the main gate / reception shall collect the Visitor Pass and Badge issued.

4.8.7.3.2. Security shall then enter the Out time of the Visitor in the system.

4.8.7.3.3. Security shall cross check visitor laptop serial number during exit.

4.8.7.3.4. Visitor Pass reconciliation shall be performed daily at 1800 hrs.

4.8.7.3.5. The security on premises shall ensure that no visitors shall remain on premises beyond office hours or Holidays unless and until informed by the host and prior permission has been sought from the department head.

4.8.7.3.6. In case of a visitor's late departure, the security guards shall confirm with the host.

4.9. Vehicle management

4.9.1. A list of authorized vehicle to be documented and made available at the main gate security cabin for vehicle authentication.

4.9.2. The following categories of vehicles will be allowed entry, and parking at the premises parking area.

4.9.2.1. Vehicles owned by senior management/directors.

4.9.2.2. All employees' vehicles (two / four wheelers).

4.9.2.3. Company Owned cars.

4.9.2.4. Company hired contract cars.

4.9.3. Visitor's vehicle entry to be limited to pick-up and drop purposes.

4.10. Material Movement : General

4.10.1. Any material entering the JMBGRP premises shall be checked at the main gate before being allowed into the premises.

4.10.2. Baggage:

4.10.2.1. Baggage belonging to visitors, third party personnel and vendors shall be checked by the security during entry and exit.

4.10.2.2. If any third-party personnel or employee is carrying any travel luggage, then the same shall be checked at the gate and then deposited in the security room/cabin.

4.11. Inward material movement:

4.11.1. Separate gate passes will be provided for material movement for inter- unit movement / maintenance purpose and the same shall authorized by the concerned head of the department.

4.11.2. Any material coming in and going out shall have identified department owner and shall be accompanied by relevant documentation such as a ‘Gate Pass’, ‘Challan’ or a ‘Purchase Order’.

4.11.3. The drivers/cleaners of the material vehicle shall report to the security person at the gate and provide all the documents pertaining to the material.

4.11.4. Material shall be allowed to enter the premises from an earmarked entry only. Material movement shall be allowed only in hours specified by the Manager HR and Admin/Security In-Charge. Deviation if any should be conveyed to the Manager HR and Admin/Security In-Charge in written/by mail in advance the Departmental Heads.

4.11.5. Details of the vehicle carrying the material into JMBGRP premises shall be noted in the register at the perimeter gate.

4.11.6. The material shall be accepted and checked in front of the security guard and an employee from the concerned department. It shall be the responsibility of the employee of the concerned department to ensure that the material is as per the Purchase Order (PO) / Challan. The security guard shall enter the details of the materials received in the ‘Materials IN’ register.

4.11.7. In case the material is received on a holiday or after office hours, it should be accepted on the next working day.

4.11.8. In case of an urgency of receiving the material on a holiday or after working hrs., a telephonic approval should be sought from respective Departmental Head followed by a mail for regularization.

4.11.9. The Security Supervisor / Guard shall stamp the challan or PO after checking the material.

4.12. Outward material movement

4.12.1. Any material being taken out of the premises shall be accompanied by a ‘Gate Pass’ (Returnable or Non-returnable) which is signed by an authorized signatory. This ‘Gate Pass’ shall include details such as, name and quantity(both volume and number of packs) of items in figures as well as words, date and time, purpose, instructed by and prepared by.

4.12.2. The security guard shall check the outgoing material against the details mentioned in the ‘Gate Pass’ in the presence of an employee from the concerned department. It shall be the responsibility of that employee to ensure that appropriate material is being sent out.

4.12.3. A list of authorized signatories along with their sample signatures shall be available at the perimeter entry gate with the Security Supervisor.

4.12.4. The security guard at the perimeter entry gate shall enter the details of the ‘Returnable in the ‘Returnable Materials’ register and the ‘Non-Returnable passes in ‘Material OUT’ register at the perimeter entry gate. These registers shall include the approving authority’s name, purpose, material details (quantity and nomenclature), date and time, department and gate pass number.

4.12.5. The ‘Returnable’ gate pass details shall be reconciled daily and a report shall be sent to all the concerned department heads whose items have gone out but not yet returned. An MIS shall be generated on every quarterly end and sent out to respective department heads.

4.12.6. A security guard shall always be present with the delivery/ pick-up vehicle till the time it is on JMBGRP premises.

4.12.6.1. Record the details in the out-word register.

5. Responsibilities

5.1. The responsibilities lies with the following personnel:

5.1.1. Local HR & Admin team of respective JMBGRP location will be responsible for implementing the physical security of premises, security & maintenance of the equipment's. Physical access for employees, visitors and contractors, Fire and Environmental Protection.

5.1.2. Cabling security (Network cables running over-head & below ground, etc.) is the responsibility of local Admin & Local IT team.

6. Enforcement:

6.1. 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.

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 document at any time as per its discretion.

7. Metrics

7.1. The metrics shall be measured by the Admin Head & IT team.

7.2. The periodicity of reporting shall be quarterly.

7.3. Following are the metrics to be measured:

7.3.1. Number of incidences of theft, robbery complaints for the location.

7.3.2. Unauthorized access incidences recorded.

7.3.3. Alarm system failure incidents.

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 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 updating 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.

8.3. All exception requests shall be submitted by respective HODs/ BISOs. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.

8.4. The CISO shall review all exceptions every year for validity and continuity.

9. Disclaimer

9.1. 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.

9.2. For any clarifications related to this Acceptable usage policy and procedure document with respect to its interpretation, applicability, and implementation, please write to CISO.

10. References:

11. Control Objectives: A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6, A.7.8, A.7.9, A.7.10, A.7.11, A.7.12, A.7.13, A.7.14, 8.1