Information Security Management System

Incident Management Policy & Procedure

Document no. JMBGRP/ISMS/Pol-IM

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The documented policy and methodology for addressing and assessing the risks to JMBGRP's Information and processing facility.	
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 "11. Reference to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: "4, 5, 7"	

Contents

1. Purpose

1.1. The policy seeks to establish a mechanism for capturing events and incidents of IT and Non-IT nature.

1.2. To capture evidence thereof, perform root cause analysis, prepare, and take corrective and preventive action, generate learning is and examine cost impacts of these incidents and events.

1.3. Always ensure that compliance to all the policies and procedures of the organization is adhered to. To adhere to the required statutory and legal compliances as mandated by the law of the land.

2. Scope

2.1. The policy document is applicable to:

2.1.1. All Locations of J.M Baxi Group in India

2.1.2. All Employees of J.M Baxi Group

3. Policy Statement

3.1. To understand as to how this policy shall manifest, it is imperative that one understands the meaning of an Event, an Incident and Crisis.

3.2. An **event** is defined as: Any discernible activity within a system, service, or network that signifies a potential breach of security protocols, procedures, or safeguards. Such activities may include previously unidentified situations that are deemed pertinent from a security perspective.

3.3. An **incident** is defined as: A single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and threatening security.

3.4. A **crisis** refers to a severe and often unexpected event that poses a significant threat to the organization's ability to function normally. It typically involves circumstances that can disrupt operations, jeopardize the safety of personnel, damage assets, or harm the organization's reputation.

Note: For the sake of brevity, this document shall only address incident management process whereas aspects of crises shall be dealt with in Business Continuity Planning / Management.

3.5. JMBGRP shall develop, communicate, and implement formal systems and procedures for detecting and reporting incidents. It shall be ensured that the incidents and weaknesses are reported in time to the appropriate authorities and corrective actions are taken immediately to contain the damage and avoid the recurrence of such events in future.

3.6. Appropriate tools shall be provided to employees. JMBGRP shall endeavor to integrate existing platforms with a unified the Incident Management Portal

3.7. JMBGRP shall ensure that all the risks related to incident reporting and possible controls to address those risks are identified and mitigated.

3.8. JMBGRP shall therefore constitute three teams, one each for Physical Security and IT. The heads of all these teams shall have one line reporting to the Security In-charge at JMBGRP.

3.9. All the incidents shall be investigated by the identified personnel in IT and Physical Security. Evidence relating to a suspected Information Security and/or Physical Security breach shall be formerly recorded, processed and preserved as per legal or business requirements.

3.10. Incidents shall be managed at an Operational, Tactical and Strategic and Executive Level through designated office bearers.

3.11. Necessary Incident Management Maps along with Standard Response procedures shall be developed by the respective teams. So also, aspects of problem management shall also be addressed. Corrective and Preventive action shall be applied as an outcome of the problem management process so as to minimize the occurrence of the incident.

3.12. Incident library shall be maintained, reviewed, and updated on a yearly basis.

3.13. JMBGRP shall establish a formal disciplinary process for dealing with employees who commit security breaches.

3.14. Individual teams shall develop SOP related to incident management, problem management and update their knowledge in a formal manner.

3.15. Employees shall be trained on the incident management process from the purview of individual action.

4. Procedure

This procedure has been structured to address various aspects of incident management and the corresponding measures / roles which need to be considered for effective incident management. The areas covered in this procedure include:

4.1. Reporting Incidents

4.2. Incident Categorization

4.3. Resolution Times

4.4. Incident Detection and Management

4.5. Reporting of Incidents by IT

4.6. Reporting of Incident by Physical Security.

4.7. Analysis of the Incident.

4.8. 4Investigation.

4.9. Forensic investigations.

4.10. Management Reporting

4.1. Reporting Incidents:

4.1.1. All IT incidents shall be entered into the Portal under the section of reporting incidents. The details which will be provided are as stated below.

4.1.1.1. Persons Name / Employee ID.

4.1.1.2. Location

4.1.1.3. Group or Dept Name

4.1.1.4. Categorization of the incident (IT)

4.1.1.5. Date of the event.

4.1.1.6. Nature of the event through a detailed description.

4.1.1.7. Duration for which the event has affected.

4.1.1.8. The user shall submit this information on the form and close the form.

4.1.1.9. Upon closure the employee shall get a return SMS or mail on the ticket number.

4.1.2. IT Related incidents shall be reported into incident management portal.

4.1.3. Upon notification, incidents or events will be categorized into predefined levels as delineated in Annexures A and B, provided at the end of this document. In instances where the incident or event does not correspond with any listed classification, reference to Annexure C for a detailed description and criteria of severity levels to facilitate further classification.

4.1.4. Based on the categorization done, the incident or event shall be diverted to the Physical Security Help Desk, IT Help Desk.

4.1.5. In case the portal is not functioning or is inaccessible, the reporting shall be done through appropriate management channels as quickly as possible.

4.1.6. The employee shall also call to **IT Helpdesk** for IT Incidents

4.1.7. The employee shall call for Physical Security Incidents

4.1.8. The employee shall call to **local admin** for incidents related to **Electrical Maintenance.**

4.1.9. The fastest communication means shall be used be it in person, through **e-mail** or **SMS.** Ideally, duplication of means shall be done, to ensure a receipt.

4.1.10. For any L3 to L1 Incident the employee shall first also inform the reporting manager and appraise on the incident and it nature.

4.1.11. Incident Reporting at JMBGRP between working and non-working hours shall be as under. Secondary communication should the above numbers not respond.

Category	Responsible Personnel	Contact Details
During Working Hours	Mr./Ms./Mrs.	Land Line: Mobile: Email:
Beyond Working Hours	Mr./Ms./Mrs.	Land Line: Mobile: Email:
During Holidays	Mr./Ms./Mrs.	Land Line: Mobile: Email:

4.1.12. During Non- Working Hours/ Holidays:

4.1.12.1. For incidents that happen after normal working hours, following sequential actions shall be followed:

4.1.12.2. The concerned employee shall focus on containing the damage and dealing with the crisis using all available assistance.

4.1.12.3. The concerned authority shall be reached to inform on the incidents within a reasonable time and as early as possible.

4.1.12.4. The reporting procedure shall remain the same.

4.2. Incident Categorization:

4.2.1. Incidents shall be categorized into Physical Security Incidents and IT Incidents. Sometimes there shall be an overlap between the 2 categories such as theft of an IT asset or physical damage to an IT Asset.

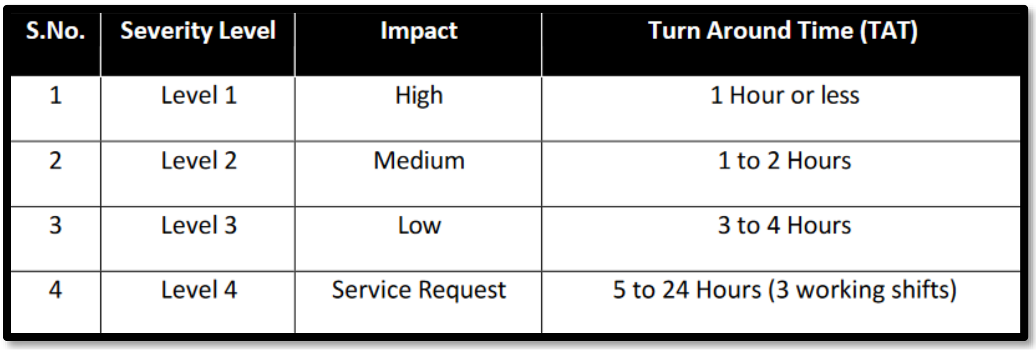
4.2.2. For the stated areas incidents shall be categorized into four levels with Level 4 being the least important and Level 1 being most important. Accordingly, the resolution time shall be defined. Given below are the resolution times by Levels. Categorization of levels by the respective teams shall be based on a formal risk assessment in terms of severity of the incident and likely hood of occurrence.

4.3. Incident Resolution Times:

4.3.1. The resolution times shall be dependent upon the Levels of incidents as provided below. (Refer to **Annexure C** for details for severity level)

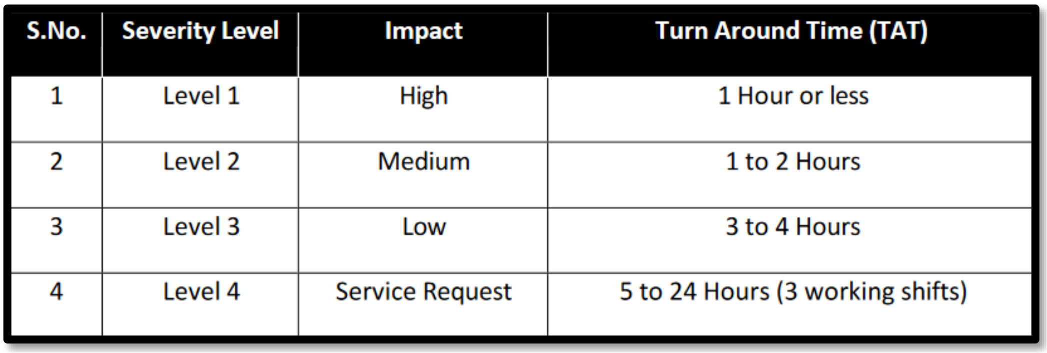
4.3.2. **Turn Around Time** define as the total time to recover the original functionality of the operation after the incident happen.

4.3.3. Service Level Agreement for IT incidents – IT Assist Rule for Incident Management:



S.No.	Severity Level	Impact	Turn Around Time (TAT)
1	Level 1	High	1 Hour or less
2	Level 2	Medium	1 to 2 Hours
3	Level 3	Low	3 to 4 Hours
4	Level 4	Service Request	5 to 24 Hours (3 working shifts)

4.3.4. Service Level Response Time for Physical Security Incidents:



S.No.	Severity Level	Impact	Turn Around Time (TAT)
1	Level 1	High	1 Hour or less
2	Level 2	Medium	1 to 2 Hours
3	Level 3	Low	3 to 4 Hours
4	Level 4	Service Request	5 to 24 Hours (3 working shifts)

4.4. Incident Management and Detection

4.4.1. There shall be standard Incident Resolution process as has been provided below: To govern the Incident Management process effectively, there shall be an executive committee as stated below. The levels have been bifurcated into operational, tactical, strategic and crisis / continuity / disaster recovery. At each level there shall be identified stakeholders who will be responsible for coordination, support, decisioning, escalation and resolution.

Executive Committee – Security In-charge, Chief of Corporate Security Dependent on the severity of an incident it shall be necessary to convene the Crisis Management Committee (CMC) Responsible for providing Business Level 3(local) coordination of an incident	**Crisis Management / Business Continuity / IT DR** **Strategic Incident Management** **Business Head (L3)**
Security In-charge /Specialist Managers/Advisors (L2) Responsible for overall guidance and direction for an incident along with HODs	**Tactical Incident Management**
Helpdesk (L1) Responsible for undertaking the activities required to control an incident, and any subsequent recovery requirements as directed by the IT	**Operational Incident Management**

4.4.2. The participation in the incident management process is given below:

4.4.2.1. At a departmental level the HOD and Departmental Implementer shall coordinate with the concerned teams in IT, Physical Security as the case may be for the reported incident and the ticket generated.

4.4.2.2. Helpdesk (Physical Security, IT) shall undertake the activities required to control an incident, and any subsequent recovery requirement as directed by their Group Leads.

4.4.2.3. Business Information Security Officers (Security In-Charge) shall be responsible for the overall guidance and direction for the security incident and act as coordinators between the Physical Security / IT Team and their respective business process owners and HODs as the case may be. If the incident does not get resolved through Security In-Charge intervention, then the concerned Business Heads shall intervene and shall work together with the respective teams.

4.4.2.4. Failure at the Business Head level, the Executive Management Team shall step in and provide guidance, decisions leading to the closure of the incident. They shall provide strategic inputs to the teams and the Business Heads shall coordinate the activities through the Security In-Charges'. If required the Executive Committee shall also call for the services of Head HR, Legal, Ethics Committee and Vigilance if found necessary. Failure at the Executive Committee Level shall escalate the incident into a crisis situation and shall mandate the intervention of the Managing Director.

4.4.2.5. Once the incident has gone into a crisis mode then for any IT related crisis the necessary Functional Recovery Plans, IT DR Plans shall be invoked and the concerned teams shall get involved in the recovery process.

4.4.2.6. For crisis related to Physical Security, the crisis team from Physical Security shall initiate response in bringing the incident under control.

4.4.2.7. In case of incidents which shall impact all the three areas then all three teams shall work in coordination and the Executive Committee shall provide guidance and direction.

4.4.3. Based on the input provided by the user:

4.4.3.1. The concerned Help Desk Teams shall examine the reported event and start the redress process based on the Turn Around Time (TAT).

4.4.3.2. The Help Desk shall categorize the event as defined in the Incident Register.

4.4.3.3. Level 1 (High) Incidents shall be directly escalated to the Executive Committee comprising of the Chief of Corporate Security, Head of Application and Infrastructure and Security In-Charge.

4.4.3.4. Level 2 (Medium) Incidents shall be escalated to Business Heads of JMBGRP (based on the classification of the incident) and as a process through escalation, if the Turn Around Time has not been met.

4.4.3.5. Level 3 (Normal) Incidents shall be escalated to the Security In-Charge/ Head of Application & Infrastructure (based on the classification of the incident) and as a process through escalation, if the Turn Around Time has not been met.

4.4.3.6. Level 4 (Low) Incidents shall by default qualify to be an incident by virtue of their very nature.

4.4.3.7. Multiple occurrences of Level 1 events at the same time shall qualify it to be a Disaster and the necessary Disaster Management Plan shall be enforced and if the business continuity is getting impacted based on the impact to the RTO (Recovery Time Objective) and RPO (Recovery Point Objective), then the BCP shall be invoked.

4.4.3.8. Incidents manifesting on account of process vulnerabilities shall be addressed as a priority and all the steps related to the redressal of such identified vulnerabilities shall be documented.

4.5. Incident Reporting

4.5.1. The Infrastructure Team / NOC Team/ SOC Team shall also be providing input to be based on the parameters as under:

4.5.1.1. NOC Team to report incidents related to parameters like Bandwidth Uptime, Bandwidth Downtime, Capacity Utilization, and Average Bandwidth Consumption per user/ LAN & WAN Broadcast/Network Latency. They shall monitor the network, categorize the occurrences as events and incidents, and provide the same through a monthly report to the Information Security- Manager along with a corrective and preventive action plan.

4.5.1.2. NOC Team shall also monitor system use like use of internet, use of FTP, Tel Net, IP Messenger, Dame-ware, RD, Citrix etc. and report exceptions and review privilege rights assigned to users, reports from port scan.

4.5.1.3. SOC Team shall manage Security Incident and Event Monitoring (SIEM) Appliance, which shall capture system log files from all the servers in the data center through the correlation rule set, reports the occurrence as event or incident. Logs from server and devices shall be flashed on the Control Console for remedial action by the team.

4.5.1.4. SOC Team shall also monitor the traffic at the perimeter and report on Malware hits/ Spam/Failed Authentications by employees trying to access the network from outside, manifesting across locations/departments/groups and then categorize the same into events and incidents and report to the Information Security-Manager through the monthly MIS and submit a corrective and preventive action plan.

4.5.1.5. Audit logs of user activities shall also be studied by the SOC Team and exceptions if any shall be reported.

4.5.1.6. IT Help Desk shall report on end user computing related incidents and events related to OS patch and AV updates on user systems, Internet Issues, Account Lock Out and Failed Log Ins', Access Issues, Outage, Malfunction, Malware Issues, Data Theft, Application Access related issues.

4.5.1.7. Incidents shall be categorized as per the levels defined above based on their impact to the business and to the reputation of the organization.

4.5.1.8. All incidents shall be logged into IT Assist and tickets shall be used Faults and corrective action taken shall be logged by concerned team into IT Assist.

4.5.1.9. Based on the input from the respective teams a Corrective and Preventive Action Plan (CAPA) shall be provided to the respective Group Leaders for approval with definite timelines, responsibilities, and expected time of completion along with cost impact.

4.5.1.10. The Application Lead is the maker and Head Application and infrastructure is the checker who shall approve the plan based on it-team Assessment of the facts provided versus the cost impact and business impact. Head GIS shall need to provide concurrence / approval depending upon the nature of the plan and criticality.

4.5.1.11. The code of disciplinary action with reference to the Code of Conduct Policy shall be used in acting on the defaulter leading to termination of the employee.

4.6. Incidents as reported by Physical Security Control Room:

4.6.1. The user shall report the occurrence of the event on the Information Security Portal and or the numbers provided.

4.6.2. Should the portal not be available then mail or SMS shall be used.

4.6.3. As a part of the workflow, the reported incident shall be categorized, a ticket shall be issued and acted upon leading to closure as per the Turn Around Times specified.

4.6.4. Depending upon the nature of the event, the report shall be escalated to Business Head / HR Head or Legal for inputs and remedial action.

4.6.5. The nature of the event shall qualify it to be an incident if it has severely compromised Information Security of JMBGRP; JMBGRP has lost its credibility in front of the regulators or it-team customers or brought about severe financial loss.

4.6.6. Evidence shall be transferred from the originating department to the concerned agency responsible for resolution of the event.

4.6.7. This evidence shall be protected by the concerned agency until such time as shall be required to fulfill, legal, regulatory contractual requirements.

4.6.8. The code of disciplinary action with reference to the Code of Conduct Policy shall be used in acting on the defaulter, leading to termination of the employee.

4.6.9. Necessary corrective and Preventive Action Plans shall be prepared and submitted to Chief of Security for review, comments, and approval.

4.7. Analysis of the Incident:

4.7.1. The respective teams shall collect evidence, records, and audit trails of all the incidents.

4.7.2. Previous incidents of similar nature shall be referred to as well.

4.7.3. If the incident cannot be resolved by the laid down processes, then a root cause analysis shall be carried out by the concerned teams.

4.7.4. Based on the analysis appropriate methodology, response structure shall be applied; preventive or corrective controls shall be applied post resolution.

4.7.5. Repository of incidents, problems shall be maintained for reference on the incident portal with restricted access. Learnings from incidents shall also be stored for easy referencing on the same portal with restricted access.

4.7.6. Individual Incident Response Plans shall be updated.

4.8. Investigation:

4.8.1. Where disciplinary or legal action shall be part of the follow-up to an incident, any investigation shall be initiated in a manner that follows documented procedures and conforms to accepted practices at JMBGRP through:

4.8.1.1. Specifying who shall request an investigation, and on what basis or criteria.

4.8.1.2. Appropriate clearances have been acquired from the concerned departments to proceed with the investigation.

4.8.1.3. Specifying who shall initiate an investigation process, including collection of evidence, secure custody and maintaining a chain thereof.

4.8.1.4. Specifying the necessary documentation to initiate an investigation and the documentation required as the investigation proceeds.

4.8.1.5. Procedures for securing and maintaining the integrity of investigation records.

4.8.1.6. Adherence to communication protocol as related to the posting of the investigation status to the relevant stakeholders.

4.9. Forensic investigations:

4.9.1. A process shall be established for dealing with incidents that shall require forensic investigations. For forensic investigations there shall be documented process/procedures

4.9.1.1. Immediate preservation of evidence on discovery of an incident.

4.9.1.2. Compliance with a standard or code of practice for the recovery of admissible evidence if available.

4.9.1.3. Maintenance of a log of evidence recovered and the investigation process undertaken.

4.9.1.4. The need to seek legal advice where evidence is recovered.

4.9.1.5. Notifying staff that actions shall be monitored during the investigations.

4.9.1.6. During any kind of forensic investigations chain of custody shall be maintained. Systems under investigation shall be protected from unauthorized access.

4.10. Management Reporting of the Incident:

4.10.1. The respective Heads of IT Help Desk, Physical Security Control Room shall provide management report monthly for the following:

4.10.1.1. Number of incidents by category which have not been resolved.

4.10.1.2. Number of incidents by category and their occurrence

4.10.1.3. Status of Corrective and Preventive Action Plans

4.10.1.4. Status of Problem Management Initiatives

4.10.1.5. Deviations with reasons

4.10.1.6. Cases undergoing investigations / sub-judice / those which are pending approval for next steps.

4.10.1.7. Incidents pending closure

4.10.1.8. Number of security weaknesses identified, corrected, work in progress.

4.10.1.9. Mandays consumed

4.10.1.10. Financial Impact

4.10.2. Summary of reported incidents shall be provided to the Security In-charge and Executive Committee monthly.

4.10.3. A copy of the report shall also be sent to the Head HR / Head Legal / Ethics Counselor for taking disciplinary and or legal action, if required.

5. Responsibilities

5.1. The responsibilities lie with the following personnel:

5.1.1. IT Helpdesk / Physical Security Control Room:

5.1.1.1. Record incidents

5.1.1.2. Escalate as per TAT violations and matrix

5.1.1.3. Analyze the incidents

5.1.1.4. Resolve Incidents

5.1.1.5. Prepare and monitor CAPA

5.1.1.6. Provide Update to Executive Committee

5.2. Chief Of Security- Physical Security, Head Application & Infrastructure and CTO (IT):

5.2.1. Ensure that TAT are maintained and corrective action is initiated.

5.2.2. Ensure that employees can report incidents for the respective categories with ease.

5.2.3. Create and maintain an updated and current directory of incidents with categorization.

5.2.4. Communicate of best practices to prevent incidents from occurring to employees through the portal.

5.2.5. Maintain and update incident response SOPs

5.2.6. Ensuring that Incident management plans are exercised/tested in agreed timeframes.

5.2.7. Coordinating the bi-annual policy compliance activity as a joint activity under the aegis of the Executive Committee.

5.2.8. Escalating incident management risks in accordance with the Risk Management Framework

5.2.9. Liaison with local emergency services (Fire Brigade, Police, CERT-In, NASSCOM, Hospitals, Transport Providers, Hotels, First Aid Services, Doctor and Paramedic Panel on call; as the case may be along with that of the concerned government departments if necessary.

5.2.10. Maintaining records, evidences, documents, statements, background information as related to the incidents, learnings from incidents.

5.2.11. Conduct incident drills once every year for their respective domains on a sample of critical incident triggers.

5.3. Executive Committee:

5.3.1. Assuming complete control and responsibility and management of incidents.

5.3.2. Highlighting to the office of MD incidents that threaten the safety of JMBGRP staff or shall have a quantitative (e.g., financial, service levels etc.) and/or qualitative (e.g., operational, reputational, legal, and regulatory) impact on the BU to the Crisis Coordinator without delay.

5.3.3. Coordinating and providing guidance and support during situations of Crisis / Disaster to the affected stakeholders.

5.3.4. Control and approval of all internal and external communications relating to the incident – e.g., press releases, speaking to media.

5.3.5. Ensuring that the incident registers are reviewed, current and updated by the respective teams.

5.3.6. Reviewing of the Monthly Status Update Reports and providing strategic guidance and inputs for remediation.

5.3.7. Reviewing Corrective and Preventive Action Plans as submitted by the three incident management teams.

5.3.8. Initiating audits once every 12 months for the incident management process.

5.3.9. Reviewing the outcome of the testing of the incident management plans and providing inputs and guidance so as to improve planned outcomes.

5.3.10. Providing assurance to the office of MD on the current levels of preparedness on incident and crisis response.

5.4. SECURITY IN-CHARGE:

5.4.1. Facilitating in the management of incidents affecting their vertical in accordance with incident management plans.

5.4.2. Facilitating in the invocation of crisis response, continuity plans as applicable for the vertical.

5.4.3. Providing regular updates on the status of the incident to the Business Heads (strategic incident control) for controlling the incident.

5.4.4. Initiating the invocation of incident response teams (HR, IT, premises etc.) and issuing them specific tasks relating to the incident.

5.4.5. Compiling post-incident reports and forwarding them to the BU Executive Management for approval/action.

5.4.6. Ensuring that employees in the vertical are equipped to respond to incidents and adequate levels of training BU staff who are required to react to incidents are fully briefed and for key posts, deputies are appointed to ensure coverage is maintained.

5.5. Employees:

5.5.1. Report incidents through the means provided.

5.5.2. Report weaknesses wherever spotted which could later on escalate into incidents and crisis situations.

5.5.3. Keep your reporting manager informed about your actions and also keep the reporting manager appraised on the incident reported.

5.5.4. Employees shall ensure that contact details (respective help desks) shall always be available with them.

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 it-team discretion.

7. Metrics

7.1. The metrics shall be compiled by the teams. These shall be reported to CTO on quarterly basis.

7.2. The metrics to be measured have been IT Head and Physical Security Manager shall work towards identifying any other key metric to be added to this list, which shall give a representative picture about the state of IT/physical security.

7.3. The parameters to be measured are as given below, but not restricted to:

7.3.1. Number of events by levels.

7.3.2. Number of escalations done.

7.3.3. Number of incidents by type (IT, Physical Security).

7.3.4. Resolution time for an event and that for an incident across three teams.

7.3.5. Number of Incidents which got converted into a crisis situation by teams.

7.3.6. Number policy violations for which employees were punished.

7.3.7. Business Groups which had highest number of incidents by category.

7.3.8. Number of unresolved problems and weaknesses

7.3.9. Incidents for which investigation got impacted on account damage to evidence.

7.3.10. Number of unsuccessful incident testing drills

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 reasons 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/ Security In-Charges. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.

8.4. The Security In-charge 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 it-team interpretation, applicability, and implementation, please raise request in Ticketing Tool

10. References:

Controls: 5.24, 5.25, 5.26, 5.27, 5.28, 8.15, 8.16

Annexure A: Master list for IT Incidents

Incident Category	Suggested Levels
WAN Failure	Level 1
LAN Failure	Level 2
Datacenter Crash	Level 1
Network Device failure (providing xx business/month)	Level 1
Server failure	Level 1
Website defacement	Level 1
Password sharing	Level 1
Denial of services giving xx business/month	Level 1
Cabling failure in datacenter	Level 1
Cabling failure	Level 2
Cabling failure with xx business/month	Level 1
Laptop/ Desktop issues of management	Level 1
Laptop/ Desktop issues with xx business/month	Level 1
PC booting problems	Level 2
Hard disk crash on PC's	Level 2
Hard disk crash on PC's of branches with xx business/month	Level 1
Printer problems	Level 2
Failed login	Level 3
Account lockout	Level 3
DR failure	Level 1
Backup failure	Level 1
Backup restoration failure	Level 1
Exceeding of TAT by 20%	Level 1
Exceeding of TAT by 10%	Level 2
Exceeding of TAT by 5%	Level 3
Bandwidth uptime at xx%	Level 1
Bandwidth uptime at yy%	Level 2
Bandwidth uptime at zz%	Level 3

Ratio of unpatched to patched system at xx%	Level 1
`Ratio of unpatched to patched system at yy%	Level 2
Ratio of unpatched to patched system at zz%	Level 3
Antivirus update at 50%	Level 1
Antivirus update at 70%	Level 2
Antivirus update at 90%	Level 3
Installation of unauthorized freeware/sharewares	Level 1
Pornographic/movies/songs found in the system	Level 1
Unofficial downloading	Level 2
Transaction of confidential data on public emails	Level 1
Transaction of official business on public mails	Level 1
Unauthorized drive/folder sharing	Level 1
Identified server logs not attended to	Level 1
Chronic virus signatures not removed	Level 1
Unlocked PC/Laptops	Level 2
Unauthorized usage of portable media	Level 1
Default Administrative rights on Desktop/Laptops	Level 1
Administrative rights on Desktop/Laptops	Level 1
Inconsistent build of equipments/PC/Laptops.	Level 2
Application failure	Level 1
Contingency plan not present	Level 1
Improper role authorization	Level 2
AD reviews not done	Level 1
DC reviews not done	Level 1
PC audits not done	Level 2
Voice audits not done	Level 2
Staff calibration not done	Level 2
Late reporting of employees	Level 2
Substance abuse by employees	Level 1
Phone sweeps for official and personal calls not done	Level 2
Process notes not provided by businesses	Level 2

NC in audits beyond xx%	Level 2
Unauthorized people found in the premise	Level 1
Non replenishment of papers	Level 2
Photocopiers not services	Level 2
Not adherence to SLA	Level 2
SLA reviews not being done	Level 2
Report spooling in the ERP	Level 2

Annexure B: Master list for Critical Non-IT Incidents

Incident Category	HO
Bomb Scare	Level 1
Vehicle Borne Suicide Bomber	Level 1
Vehicle Borne Improvised Explosive Device	Level 1
Improvised Explosive Device	Level 1
Suicide Bomber	Level 1
Armed Attack	Level 1
Unconventional Attack (Chemical, Biological, Radiological, Nuclear)	Level 1
Hijacking/ Hostage Situation	Level 1
Fire	Level 1
Flood	Level 1
Homicide	Level 1
Organized or Deliberate Disruptions	Level 1
Civil Disturbances	Level 1
Major Earthquake	Level 1
Major accident on location	Level 1
Robbery	Level 1
Suicide	Level 1
Terrorist Attack	Level 1
UPS Failure	Level 1
War	Level 1
Mob/Vandalism/Arson	Level 2
Sabotage	Level 2
Major Theft	Level 2
Worker Strikes (3rd Party)	Level 2
Power & DG Failure	Level 2
Burglary	Level 2
Vehicle Accident	Level 2

Annexure C: Severity Level Description and Criteria

Severity	Description	Criteria
Level 1	A critical incident with very high impact. Critical issue that warrants public notification and impacting many business functions of the organization	• Many systems are in a critical state and actively impacting huge number of users/ employees who are unable to do their tasks. • Extreme damage to the reputation of the business leading to revenue loss. • Functionality has been severely impaired for a long time, breaking SLA. • Major compliance violation at company level. • Vulnerability exposing customer and personal data has been identified.
Level 2	A major incident with significant impact. Critical issue actively impacting many business functions of the organization	• Few systems are in a critical state and actively impacting many users. • Potential high damage to company reputation and revenue loss. • A smaller group of users have been affected, disrupting non-essential services. • Medium compliance violation. • Devices / applications affected are of critical nature, however impact is limited.
Level 3	A minor incident with low impact	• A small number of users affected. • Minor compliance violation. • Minimal number of employees are affected and / or able to deliver their services requiring extra efforts / expenses. • Potential moderate damage to business reputation.
Level 4	Minor issues requiring action, but not affecting business as usual	• Isolated incident which affects a few users, such as an isolated spam or virus identified on a few users. • Minor incident causing performance issue • Individual user system failure. • Minor system failure and / or loss of network connectivity. • Impacted business / tasks are not time sensitive.