Information Security Management System
Business Continuity Policy & Procedure

Document no. JMBGRP/ISMS/Pol-BC

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The document showcases outline the responsibility of the JMBGRP and their employee in the event of a crisis in order to maintain as normal a service as practically possible including the information security aspects.	
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 " Reference to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Document reviewed. Modifications done in Section : "4,5,7,8,9,10"	

Contents

1. Purpose

1.1. The purpose of the Business Continuity Policy is to outline the responsibility of the JMBGRP and their employee in the event of a crisis in order to maintain as normal a service as practically possible including the information security aspects. The over-riding aim is to ensure a prompt and efficient recovery of critical activities from any incident or physical disaster that may affect the JMBGRP's ability to operate and deliver its services. It must be recognized that any such event not only impacts on employees, premises, technology, and operations, but also on the JMBGRP brand, status, relationships and reputation and that all business continuity arrangements should ensure that the JMBGRP meet its legal, contractual, statutory and regulatory obligations to both its employees and dependent stakeholders.

2. Scope

2.1. The scope of this policy at JMBGRP applies company-wide, covering all departments, employees, contractors, and stakeholders. It addresses various risk scenarios like natural disasters, cyber threats, and pandemics, ensuring a comprehensive approach to risk management. The policy outlines procedures for incident response, recovery, and regular testing to validate the plan's effectiveness. Compliance with industry standards and continuous improvement through periodic reviews are integral to the policy's implementation.

3. Policy Statement

3.1. JMBGRP shall develop, implement and maintain a Business Continuity Management System (BCMS) in order to ensure the prompt and efficient recovery of its critical activities from any incident or physical disaster affecting its ability to operate and deliver its services. It is the policy of the JMBGRP to take all reasonable steps to ensure that in the event of a service interruption, the organization will be able to respond appropriately and continue to deliver its essential functions. JMBGRP shall build a BCMS that:

3.1.1. Ensure redundancy and resilience are integrated into operational processes to mitigate the impact of disruptions.

3.1.2. Manage business interruption risks in accordance with Business Continuity Plan and related Risk.

3.1.3. Develop resumption plans based on criticality of business functions.

3.1.4. Identify and document roles and responsibilities for key staff positions to plan, review and implement the Business Continuity Plan.

3.1.5. Minimize the impact of function loss on JMBGRP's stakeholders and the community.

3.1.6. Minimize the impact of function loss on JMBGRP reputation.

3.1.7. Minimize any risk associated with public health, safety and/or welfare.

3.1.8. Ensure that JMBGRP considers regulatory requirements and/or compliance with legally enforceable contracts during outages.

3.1.9. Maintain control of expenditure and minimize extraordinary costs resulting from incidents.

3.1.10. Include Information Security Continuity in considerations and impacted parameter.

4. Procedure

4.1. Approach to Business Continuity Management (BCM)

4.1.1. JMBGRP is responsible for operations of a wide range of services and in the event of an emergency or business interruption, it is essential that critical services which support our commissioning activities can be restored and maintained as soon as is practically possible.

4.1.2. Business Continuity Management (BCM) is a holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

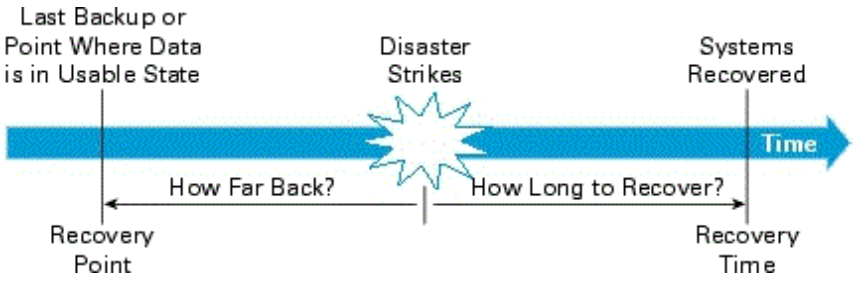
4.1.3. In case of an emergency or business interruption, JMBGRP will strive to maintain services at or near their usual standard, though achieving this may not always be feasible. To address this, the organization will identify, define, and prioritize its functions through a Business Impact Analysis (BIA)

4.2. Understanding the organization

4.2.1. Business impact analysis (BIA) is the process of analyzing business functions and determining the effect that a business disruption might have upon them, and how these vary over time. The aim of the business impact analysis is to ensure that JMBGRP has identified those activities that support its key services in advance of an incident, so that robust business continuity plans can be put into place for those identified critical activities.

4.3. Business Impact Analysis process:

4.3.1. The business impact analysis shall be done to assess the requirements for RTO (Recovery Time Objective) and RPO (Recovery Point Objective) for business continuity and disaster recovery perspective. The process of identifying business functions and the effect a business disruption will have on them. Risk assessment is the process of risk identification, analysis and evaluation using a risk matrix. Hazards shall be identified, and risk assessment shall be done for the same.



4.3.2. **Recovery Time Objective:** Recovery Time Objective (RTO) refers to the targeted duration within which a business process or system must be restored after a disruption in order to avoid significant consequences or losses. It represents the maximum tolerable downtime for an organization's operations or services.

4.3.3. Recovery Point Objectives (RPO):

4.3.3.1. Recovery Point Objectives (RPO) refer to the maximum tolerable period in which data might be lost due to a disruption. It defines the acceptable amount of data loss measured in time preceding a system failure or outage that can be tolerated by an organization.

4.3.3.2. The business impact analysis shall:

4.3.3.2.1. Defines the function and its supporting processes.

4.3.3.2.2. Determines the impacts of a disruption.

4.3.3.2.3. Determines the minimum resources needed to meet those objectives.

4.3.3.2.4. Considers any statutory obligations or legal requirements placed on the JMBGRP.

4.3.3.3. JMBGRP business impact analysis results in the identification of those activities whose loss would have the greatest impact in the shortest time and need to be recovered most rapidly.

4.3.3.4. The community risk register will be considered when undertaking business impact analysis in order to enable the organization to understand the threats to, and vulnerabilities o critical activities and supporting resources, Information Security, including those provided by suppliers and partners.

4.4. Determining business continuity management strategy.

4.4.1. There are many and varied possible causes of service disruption. Business continuity planning will be carried out to minimize the effects of a number of potentially disruptive events. A series of robust plans and mitigation will be developed for these priority areas. The list is not exhaustive, and judgement will be applied in each case:

4.4.1.1. People: Loss of key staff short and long-term including significant national or international incidents impacting on the JMBGRP, such as a pandemic.

4.4.1.2. Premises: Loss of primary workplace in the short and long term.

4.4.1.3. Technology: Loss of information and communications technology Infrastructure services.

4.4.1.4. Information: Loss of data or impact on security

4.4.1.5. Suppliers & Partners: Business continuity affecting suppliers and/or partners.

4.4.1.6. Any other requirements as identified by the business impact analysis process.

4.5. Developing and implementing the business continuity Management response

4.5.1. The following areas will be included in the organization's Business Continuity Plan:

4.5.1.1. Critical Activities: Those activities whose loss would have the greatest impact in the shortest time and need to be recovered most rapidly. Critical activities will be reflected on JMBGRP Risk Register, as appropriate**.**

4.5.2. Business Continuity Team

Designation	Telephone
APEX Committee	
Head, Admin	
Head, IT	
MD, JMBGRP	
Corporate Security In-charge	

4.5.3. Communications Strategy

4.5.3.1. Both Internal and external communications are important and critical at the time of disaster, a major incident or any business continuity incident and how the JMBGRP cascades the Information.

4.5.3.2. The response to an emergency or business continuity incident does not necessarily or automatically translate into the declaration of a major incident and the implementation of a full recovery operation. Incidents may cause a temporary or partial interruption of activities with limited or no short term or longer-term impact. It will be the responsibility of the JMBGRP Executive team (CXO), as available, to evaluate and declare the appropriate level of response.

4.5.3.3. The below mentioned guidelines shall be followed for a good BCP communication strategy:

- Good communication is essential at a time of crisis. A communications strategy will be developed to ensure there are appropriate statements for internal and external communication and processes for ensuring communication to all staff in the case of an emergency. This strategy will be the same across all plans.

- The strategy will include reference to procedures for regular communications with partner organizations and other interested parties. This is particularly important during the planning stage

for known disruptions such as winter weather. Formal reporting and situation updates may also be required in the lead up to and during a disruption to create a local, regional and national overview of effects across JMBGRP.

- The main objective of the strategy will be to Deliver relevant messages about the incident to the relevant stakeholders.
- Utilize relevant media channels to reassure and inform the public.
- Ensure that messages are timely and relevant to the target audience.
- A cascade structure will be developed to ensure key individuals within and external to the organization have been informed of incidents.

4.5.4. Business Continuity incident rating - JMBGRP Risk Management Policy Description and score:

4.5.4.1. The severity of an incident will be identified as follows:

- **Insignificant – Low 1-5**
- **Minor – Medium 6-11**
- **Moderate - High 12-15**
- **Major - Very High 16-20**
- **Catastrophic - Extreme 25**

4.5.4.2. The severity level will indicate the urgency of recovering the business service, and also the order in which services should be reinstated. The risks to our stakeholders resulting from an incident affecting the JMBGRP could be significant.

4.5.5. Incident Identification

4.5.5.1. An incident or set of circumstances which might present a risk to the continuity of a JMBGRP function or service may be identified by any member of staff. When an incident or set of circumstances which might present a risk to the continuity of JMBGRP function or service is identified, it is important that the person identifying the incident knows what to do. In the initial stages, this will involve making sure that the right people have been informed.

4.5.5.2. The Business Impact Analysis sets out a list of priority incidents:

- Staffing shortage: Loss of key staff short and long-term including through epidemic
  / pandemic illness, industrial action, and transport disruption.

- Loss of operating premises: Contamination, disruption to utilities (water, gas, electricity, heating/cooling), fire, flooding, structural defect / failure.

- Information Technology failure: major electronic attacks or severe disruption to the IT network and systems (telephone network, data network, active directory, Antivirus, Firewall, hardware failure, loss of major application, loss of mobile phone network, loss of switchboard, server failure).

- Information/data loss: Data stolen / lost, destruction of paper files, failure of back-up or failsafe, temporary loss of connection, Cyber security crisis.

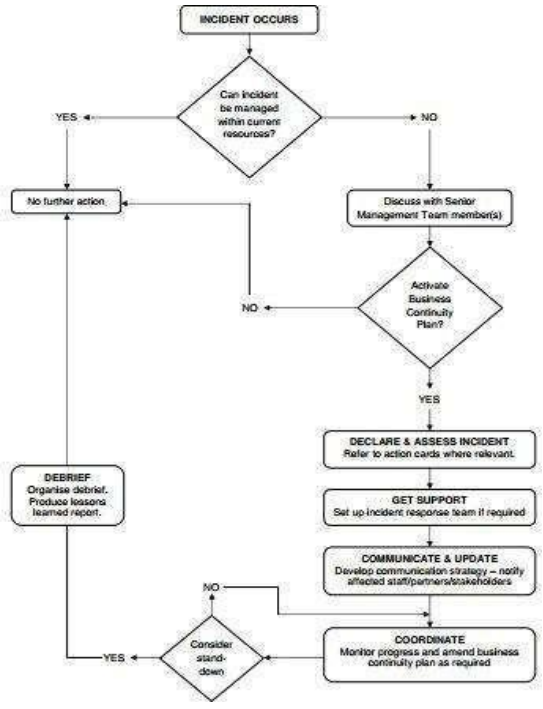
- Supplier failure: Contract breach, industrial action, stock management failure, supplier goes into administration, supply chain collapse.

4.5.6. Incident Declaration

4.5.6.1. The following Officers of the JMBGRP can declare an incident where business continuity is disrupted or at risk of disruption:

Designation	Telephone
Head, Admin	
Head, IT	
MD, JMBGRP	
Security In-charge	
ISO	
Head, Physical Security	

4.5.6.2. The diagram below describes the process for invoking and cycle of a business continuity incident:



4.6. Exercising, maintaining and reviewing.

4.6.1. Exercises can expose vulnerabilities in an organization's structure, initiate processes needed to strengthen both internal and external communication and can help improve management decision making during an incident. They are also used to assess and identify gaps in competencies and further training that is required for our staff.

4.6.2. The on-going viability of the business continuity program can only be determined through continual tests and improvements. The Business Owners will be responsible for ensuring regular tests and revisions are made to the business continuity plan to ensure they provide the level of assurance required.

4.6.3. Exercises and tests will:

- Be consistent with the scope and objectives of the business continuity Management system (BCMS)
- Be based on appropriate scenarios that are well planned with clearly defined aims and objectives.
- Minimize the risk of disruption of operations.
- Produce post-exercise reports.
- Be conducted at planned intervals and when there are significant changes within the organization or to the environment in which it operates.
- Share lessons learned and post-exercise reports with all interested Parties and update the concerned business continuity plan accordingly.

Note: Business Continuity Test or exercise for JMBGRP location, critical business functions, and applications shall be conducted at least once a year.

4.6.4. **Training:** All staff will be offered relevant training commensurate with their duties and responsibilities. Staff requiring support should speak to their line manager in the first instance. Support may also be obtained through their HR Department.

4.6.5. Communication: Business Continuity Plan shall be communicated to all employees, contractors and interested parties.

4.6.6. Associated Documents

4.6.6.1. The following documentation is to be read in reference to this policy:

- Information Security Risk Assessment Policy & Procedure
- Business Continuity Plan
- Emergency Plan & Procedures

5. Responsibilities

5.1. The responsibility lies with the following personnel:

5.2. APEX Committee

- Enforcing compliance through assurance activities, provision of appropriate levels of resource and budget to achieve the required level of business continuity competence.
- Coordinating the overall management of an incident which necessitates invocation of business continuity and recovery planning.
- Reviewing the business continuity status and the application of the policy and standards in all business undertakings.
- Strategic direction of organizational recovery plans.
- Ensuring information governance standards continue to be applied to data and information during an incident.
- Deciding when to escalate to the Emergency Preparedness, Resilience & Response Policy framework and deciding when to escalate to the Area Team.
- Leading the recovery plan after the incident.
- Communication with media such as TV, Newspaper, bulletin, magazine etc. in case itis required.

5.3. Security In-charge

- Supporting staff across the organization to develop operational business continuity plans.
- Ensuring that the organizational Business Continuity Plan is reviewed and updated at regular intervals to determine whether any changes are required to procedures or responsibilities.
- Managing training and awareness of the plan and maintaining the plan including change control and testing.

5.4. Head - Admin/HR/IT

- Communication to employee and stakeholders/interested parties in case of invocation of Business continuity and disaster recovery Plan.
- Provide logistics support for Business Continuity and recovery Plan.
- Ensuring the progress of organizational Business Continuity and recovery Plan to comply RTO.

5.5. Audit Committee

- Ratifying Business Continuity Planning.
- Seeking assurance that up-to-date policies and plans are being implemented effectively in the event of a business continuity incident.

5.6. HOD

- Assessing their specific area of expertise and planning actions for any necessary recovery phase, setting out procedures and staffing needs and specifying any equipment or technical resource which may be required in the recovery phase.
- Holding two hard copies of the 'Business Continuity Plan' allocated to them. It is intended that one copy should be located at the holder's home address, so it is easily accessible and the second in a folder clearly marked as 'Business Continuity Plan (BCP)' at their office base. The BCP folder will also contain recovery procedures, contacts, and lists of vital materials or instructions on how to obtain them.

5.7. Employee

- Achieving an adequate level of general awareness regarding Business continuity.
- Being aware of the contents of their own business areas disaster recovery plan and any specific role or responsibilities allocated.
- Participating actively in the business continuity program wherever required.

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 right to alter or amend any clause in this document at any time asper its discretion.

7. Evidence

7.1. The evidence shall be maintained by Security In-Charge

7.2. The evidence to be maintained are as follows:

- Business Continuity Plan document
- Business Continuity Test/Drill Report
- Snapshot of evidence for BCP test/drill
- Evidence for review of BCP and BCP test/drill
- Evidence for approval of BCP and BCP test/drill

8. Metrics

8.1. The metrics shall be measured by the Security In-Charge.

8.2. The periodicity of reporting shall be quarterly.

8.3. Following are the metrics to be measured:

- Number of BCP tests conducted.
- Number of successful/failed BCP test

9. Exceptions

9.1. 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.

9.2. 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.

9.3. All exception requests shall be submitted by respective HODs/ Security In-charge. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester. [Refer: Annexure – A: Exception From]

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

10. Disclaimer

10.1. 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.

10.2. For any clarifications related to this Acceptable usage policy and procedure document with respect to its interpretation, applicability and implementation, please raise a request on Ticketing Tool.

11. References:

Control: .5.30 , 7.5