|  |
| --- |
| Business Continuity Plan |

****

**ROYAL SECURITIES EXCHANGE OF BHUTAN**

# **Contents**

[**Contents** 1](#_Toc147497215)

[**1.** **BACKGROUND** 1](#_Toc147497216)

[**1.1.** **Purpose of Business Continuity Plan** 1](#_Toc147497217)

[**1.2.** **Scope of Business Continuity Plan** 3](#_Toc147497218)

[**2.** **Risk Assessment** 4](#_Toc147497219)

[**2.1.** **System Failure** 4](#_Toc147497220)

[**2.2.** **Natural Disaster Risk** 4](#_Toc147497221)

[**3.** **Business Impact Analysis** 5](#_Toc147497222)

[**3.1.** **Critical Function** 5](#_Toc147497223)

[**3.2.** **Maximum Allowable Downtime (MAD)** 6](#_Toc147497224)

[**4.** **Prevention and Mitigation Strategies** 6](#_Toc147497225)

[**5.** **IT HR-Retention Policy** 13](#_Toc147497226)

[**5.1.** **Competitive Compensation** 14](#_Toc147497227)

[**5.2.** **Knowledge Sharing** 14](#_Toc147497228)

[**5.3.** **Cross-Functional Training** 14](#_Toc147497229)

[**5.4.** **Succession Planning** 14](#_Toc147497230)

[**5.4.1.** **Identifying Potential Successors** 15](#_Toc147497231)

[**5.4.2.** **Cross-Training and Skill Development** 16](#_Toc147497232)

[**5.4.3.** **Transition Planning** 16](#_Toc147497233)

[**5.4.4.** **Recruitment and On boarding** 17](#_Toc147497234)

[**6.** **Documentation** 17](#_Toc147497235)

[**6.1.** **System Codes and Source Code document:** 18](#_Toc147497236)

[**6.2.** **Password Management:** 18](#_Toc147497237)

[**6.3.** **Network and Infrastructure Design:** 19](#_Toc147497238)

[**6.4.** **Database Information:** 19](#_Toc147497239)

[**6.5.** **Training and Knowledge Transfer:** 19](#_Toc147497240)

[**6.6.** **Documentation Review:** 19](#_Toc147497241)

[**6.7.** **Accessibility in Emergency:** 20](#_Toc147497242)

[**6.8.** **Support Documentation:** 20](#_Toc147497243)

[**6.9.** **Documentation Retention:** 20](#_Toc147497244)

[**7.** **BCP Team and Their Responsibilities:** 20](#_Toc147497245)

[**8.** **Detailed plan for implementation of BCP immediately following occurrence of disruptions:** 21](#_Toc147497246)

[**9.** **Expenditure incurred during emergency:** 24](#_Toc147497247)

[**10.** **Periodic review and update of BCP:** 24](#_Toc147497248)

[**11.** **Emergency contact toolkit:** 24](#_Toc147497249)

# **BACKGROUND**

This executive summary encapsulates the key findings and recommendations of the Pay Revision Report by RSEB. The report delves into the crucial topic of salary adjustments to ensure competitiveness, retention, and equitable compensation within the organization.

# **Purpose of Business Continuity Plan**

The purpose of a Business Continuity Plan (BCP) for the Royal Securities Exchange of Bhutan (RSEB) is multifaceted and crucial for the organization's resilience and sustainability. Here are the detailed purposes of the BCP:

1. **Ensure Business Resilience:** The primary purpose of the BCP is to ensure that RSEB can continue its critical business operations, even in the face of unexpected disruptions. This includes the ability to continue trading securities, maintain data integrity, and provide services to clients without significant interruptions. It is to ensure that RSEB can maintain critical operations, especially those reliant on its in-house developed software, even when faced with significant disruptions. Given the limited availability of IT professionals, preserving the functionality of these systems is paramount.
2. **Risk Management:** The BCP helps RSEB identify, assess, and mitigate risks that could disrupt its operations. By understanding these risks, the organization can take proactive measures to reduce their impact and likelihood. Recognizing the critical dependency on IT systems and the shortage of local IT talent, the BCP aims to mitigate risks associated with system failures, data breaches, and loss of institutional knowledge. It seeks to ensure that the organization can continue functioning effectively even when IT expertise is scarce.
3. **Talent Retention and Development:** The BCP includes strategies for talent retention, skills development, and knowledge transfer within the IT department. It outlines measures to retain existing IT professionals, attract new talent, and nurture the skills needed to maintain and enhance the in-house software.
4. **Succession Planning:** Given the trend of IT professionals leaving Bhutan for better opportunities abroad, the BCP incorporates succession planning. It identifies key IT roles and prepares backup staff or cross-trains employees to fill critical positions in case of sudden departures.
5. **Knowledge Preservation:** To address the potential loss of institutional knowledge due to IT staff turnover, the BCP encourages the creation of comprehensive documentation and knowledge-sharing practices. This ensures that critical information about the in-house software and systems is preserved and accessible to all relevant personnel.
6. **Efficient System Recovery:** In the event of system failures or disruptions, the BCP emphasizes swift recovery procedures. It ensures that IT HR resources are allocated efficiently to restore critical software and systems, minimizing downtime and financial losses.
7. **Strategic Recruitment:** To mitigate the shortage of IT professionals, the BCP may recommend strategic recruitment practices. This could involve actively seeking IT talent from educational institutions, developing partnerships with local IT organizations, or exploring remote work arrangements.
8. **Long-Term IT Sustainability:** Beyond immediate continuity concerns, the BCP encourages long-term IT sustainability planning. It includes strategies for adapting to changes in the IT landscape, staying updated with technological advancements, and fostering a culture of innovation.
9. **Protect Client Interests:** RSEB is responsible for handling financial assets and investments for clients. The BCP ensures that these assets are safeguarded, and client interests are protected, even during crises.
10. **Compliance and Regulation:** Regulatory bodies often require financial institutions like RSEB to have a BCP in place to ensure business continuity. Compliance with these regulations is a fundamental purpose of the plan.
11. **Minimize Financial Losses:** Disruptions in trading or data breaches can result in financial losses. The BCP aims to minimize such losses by having strategies in place to quickly recover operations.
12. **Maintain Reputation and Trust:** Any significant disruption can damage the reputation and trust of RSEB in the eyes of its clients and stakeholders. The BCP helps in maintaining a positive image by demonstrating preparedness and resilience.
13. **Ensure Data Integrity:** RSEB relies heavily on IT systems for its operations. The BCP ensures that data integrity is preserved, and sensitive financial information remains secure during and after disruptions.
14. **Preserve Employee Safety:** The BCP outlines procedures for employee safety during crises, ensuring their well-being while they work to restore operations.
15. **Regain Normal Operations:** After a disruption, the BCP provides a structured approach to recover and return to normal operations as quickly as possible, minimizing downtime.
16. **Strategic Planning:** The BCP fosters strategic thinking within the organization. It requires RSEB to analyze vulnerabilities, assess the impact of disruptions, and develop strategies to overcome challenges. This can lead to better long-term strategic planning.
17. **Stakeholder Communication:** Effective communication is vital during crises. The BCP defines communication strategies for notifying clients, employees, regulatory bodies, and other stakeholders about the status of operations and recovery efforts.
18. **Legal and Ethical Responsibility:** The BCP ensures that RSEB fulfils its legal and ethical responsibilities to clients, shareholders, and the financial market by providing a framework for resilience and continuity.

In summary, the BCP for RSEB serves as a comprehensive strategy to protect the organization's interests, maintain its operational capabilities, and ensure the safety and satisfaction of its clients, employees, and stakeholders during and after disruptive events. It is an essential tool for risk management and business sustainability. In essence, the BCP for RSEB goes beyond traditional business continuity planning to address the unique challenges posed by IT HR dependency and the in-house software. It strives to secure the organization's technological backbone, talent pool, and data integrity, ensuring uninterrupted operations and long-term sustainability in a competitive IT environment.

# **Scope of Business Continuity Plan**

The BCP focuses on ensuring the uninterrupted operation of critical business functions, especially those heavily reliant on in-house developed software and IT infrastructure. It encompasses IT systems, data protection, IT human resources management, vendor relationships, regulatory compliance, physical infrastructure, communication, and stakeholder engagement. Additionally, it emphasizes testing, documentation, knowledge management, long-term sustainability, audit, and third-party dependencies to guarantee business resilience and adaptability during disruptions.

# **Risk Assessment**

# **System Failure**

In a scenario where IT staff attrition becomes a significant concern, the risk of system failure takes on a new dimension. The key aspects to consider are as follows:

1. **Dependency on Few IT Resources:** With only three IT professionals who possess the knowledge of RSEB's proprietary IT systems, the organization is vulnerable to disruptions caused by staff departures. If any of these IT professionals decide to leave for better opportunities abroad or elsewhere, RSEB may face a critical gap in its IT operations.
2. **Knowledge Concentration:** The IT system's coding and architecture knowledge is highly concentrated within this small group of IT resources. The departure of even one member could result in a knowledge vacuum, making it challenging to maintain, troubleshoot, or enhance the IT system.
3. **Impact on Business Operations:** The consequences of IT staff attrition could be severe. It may lead to extended downtime, unresolved system issues, delays in system updates or improvements, and a decline in the overall reliability of the IT infrastructure. These disruptions can directly impact trading activities, data management, and customer service.

# **Natural Disaster Risk**

1. **Vulnerability to Natural Disasters:** Bhutan is susceptible to various natural disasters, including earthquakes, floods, landslides, and flash floods. Given the geographical location of RSEB, it's important to acknowledge the potential impact of these disasters on operations.
2. **Physical Infrastructure Damage:** Natural disasters can result in physical damage to RSEB's facilities, including data centers, servers, and IT hardware. This damage can disrupt IT operations and lead to data loss.

# **Business Impact Analysis**

# **Critical Function**

1. **Capital Market Solution (CaMS):** CaMS is a fully integrated system that automates end-to-end processes for the stock market. It encompasses trading, clearing, depository, and brokers' back-office systems. CaMS is critical to RSEB's operations as it supports real-time order processing, flexibility for entering buy and sell orders, agent brokers, mobile application usage, client terminals, and real-time subscription management for corporate actions like Rights Issues and IPOs.
2. **Mobile Capital Market Solution (MCaMs):** MCaMs complements CaMS by providing mobile access to critical capital market functions. It enables users to stay connected and engage in stock market activities via mobile devices. MCaMs is essential for ensuring that market participants can access trading and investment services even when they are not at their desktops.
3. **IT Human Resources (IT HR):** Given the limited availability of IT professionals in Bhutan and their critical role in maintaining and developing RSEB's in-house software, IT HR is a vital component of the organization's operations. Their expertise is essential for ensuring the functionality, security, and continuity of RSEB's IT systems. The sudden departure or unavailability of IT HR personnel could lead to significant disruptions and risks to RSEB's IT-dependent operations.
4. **Failure of Data Center, Servers, and Networks**: The Data Center, including servers and networks, is the backbone of RSEB's IT infrastructure. Its failure can disrupt all critical functions, including CaMS and MCaMs, rendering them inaccessible. The failure of these core IT components is a critical concern as it could lead to significant operational downtime and financial losses. The Data Centre design along with specific IP address is attached as **“Annexure 1”**

# **Maximum Allowable Downtime (MAD)**

Considering the significance of these critical functions, including IT HR, the Maximum Allowable Downtime (MAD) should be set at a very low threshold. Specifically, downtime for these critical components should not exceed two hours. Any disruption beyond this timeframe could have severe implications for RSEB's ability to conduct its core business activities.

# **Prevention and Mitigation Strategies**

1. **Cybersecurity Measures:** Given the increasing threat of cyberattacks, RSEB should proactively invest in robust cybersecurity measures. This includes regular security audits, implementing advanced firewalls, intrusion detection systems, and data encryption. Conducting periodic employee training on cybersecurity best practices can also mitigate the risk of security breaches.

Following regular activities is integrated into the organization's cybersecurity and business continuity practices to ensure ongoing protection and resilience against evolving threats and risks. The timeline and frequency of activities are defined as follows:

| **Time Interval** | **Mitigation Activities** | **Responsibility** | **Reporting Process** |
| --- | --- | --- | --- |
| Daily | **Log and Event Monitoring:** Review logs and events from security systems, firewalls, and servers for anomalies and potential threats. | IT HEAD | Report any suspicious activities or incidents to the General Manager |
| **User Account Monitoring:** Regularly review user accounts and access rights. Disable or remove accounts for employees who have left the organization or changed roles. | IT HEAD | Report changes or terminations to the General Manager. |
| Weekly | **Vulnerability Scanning:** Conduct weekly vulnerability scans to identify weaknesses in the network and systems. Prioritize and address critical vulnerabilities. | IT HEAD | Share vulnerability scan results and action plans directly with the General Manager. |
| **Patch Management:** Review and apply security patches and updates to operating systems and software. Test patches in a controlled environment before deployment. | IT HEAD | Communicate patching schedules and updates directly to the General Manager. |
| **Backup Testing:** Verify the integrity and availability of backups. Perform periodic backup and recovery tests to ensure data can be restored in case of an incident. | IT HEAD | Share backup test results and issues directly with the General Manager. |
| Monthly | **Security Awareness Training:** Provide ongoing cybersecurity training for employees. Keep them informed about current threats and best practices. | IT HEAD | Monitor and report employee training compliance directly to the General Manager. |
| **Incident Response Drills:** Conduct simulated incident response exercises to test the effectiveness of the response plan and identify areas for improvement. | IT HEAD | Document incident response drill outcomes and share them directly with the General Manager. |
| Quarterly | **Security Audits:** Perform quarterly security audits and assessments to identify vulnerabilities, assess compliance, and evaluate the overall security posture. | IT HEAD | Share audit findings and recommendations directly with the General Manager. |
| **Policy Review:** Review and update cybersecurity policies, procedures, and guidelines to reflect changes in technology and threat landscape. | IT HEAD | Report policy updates and changes directly to the General Manager. |
| Semi-Annually | **Vendor Assessments:** Review and assess the cybersecurity practices of third-party vendors and service providers. Ensure they meet security standards and requirements. | IT HEAD | Share vendor assessment reports and findings directly with the General Manager. |
| . **Risk Assessment:** Conduct a semi-annual risk assessment to identify new threats and vulnerabilities and adjust the mitigation strategy accordingly. | IT HEAD | Report risk assessment results and mitigation plans directly to the General Manager. |
| Annually | **BCP Review:** Review and update the Business Continuity Plan annually. Ensure it reflects changes in the organization, technology, and lessons learned from incidents. | IT HEAD | Share updated BCP details directly with the General Manager. |
| **Policy Training:** Reinforce cybersecurity policies and procedures through annual training sessions for all employees. | IT HEAD | Monitor and report employee training compliance directly to the General Manager. |

1. **Regular System Maintenance:** Preventive maintenance of IT systems, including CaMS, MCaMs, and the Data Center, is essential to keep them in optimal working condition. Regular updates, patches, and system health checks should be performed to identify and rectify vulnerabilities before they become exploitable.

The table outlines a comprehensive schedule of regular system maintenance activities, each designed to ensure the optimal functioning, security, and resilience of the RSEB's critical IT systems.

| **Maintenance Activity** | **Details** | **Responsible Department** | **Reporting Process** |
| --- | --- | --- | --- |
| **Daily** | | | |
| System Health Checks | Review system health, logs, resources. | IT Team | Any anomalies reported to GM daily. |
| Log Management | Analyze logs for security insights. | IT Team | Reports sent to GM for review. |
| **Weekly** |  |  |  |
| Backup Verification | Confirm backup success, test restore. | IT Team | Backup status reported to GM. |
| Software Updates | Review updates, schedule, test. | IT Team | Installation reports to GM. |
| **Monthly** | | | |
| Performance Tuning | Assess and optimize system performance. | IT Team | Performance improvements report to GM |
| **Quarterly** | | | |
| Security Audits | Conduct security audits, assessments. | IT Security | Audit findings and actions repot to GM |
| **Semi-Annually** | | | |
| Capacity Planning | Evaluate resource utilization. | IT Team | Capacity plans reported to GM. |
| **Annually** | | | |
| System Documentation | Review and update documentation. | IT Team | Updated documentation reported to GM. |

1. **Backup Systems:** To ensure business continuity in case of system failures or data corruption, RSEB should maintain a comprehensive backup and recovery strategy. Regularly back up critical data and configurations for CaMS, MCaMs, and IT systems. These backups should be stored securely, both onsite and offsite, and regularly tested to ensure they can be restored quickly when needed.

To ensure business continuity and data integrity by maintaining a robust backup and recovery strategy for critical systems.

Daily Backup:

| **Task** | **Timeframe** | **Responsible Party** |
| --- | --- | --- |
| Daily Data Backup | Daily | IT Team |
| Check Backup Logs | Daily | IT Team |
| Offsite Backup Rotation | Daily/Weekly | IT Team |

Weekly Backup:

| **Task** | **Timeframe** | **Responsible Party** |
| --- | --- | --- |
| Weekly Backup Testing | Weekly | IT Team |
| Verify Data Backup | Weekly | IT Team |

Monthly Backup:

| **Task** | **Timeframe** | **Responsible Party** |
| --- | --- | --- |
| Monthly Backup Integrity Check | Monthly | IT Team |
| Monthly Backup Testing | Monthly | IT Team |

**Reporting:**

Daily Data Backup Status Report: This report will provide an overview of daily backups, including success or failure status, and any issues encountered.

**Weekly Backup Testing Report**: This report will detail the results of weekly backup testing, ensuring that backups are viable for recovery.

**Weekly Data Backup Verification Report**: This report will verify the accuracy and completeness of weekly backups.

**Monthly Backup Integrity Report**: This report will verify the integrity of the monthly backups, ensuring data consistency and reliability.

**Monthly Backup Testing Report**: This report will detail the results of monthly backup testing.

**Responsibility:**

The IT team is responsible for executing daily data backups, checking backup logs, rotating offsite backups, conducting weekly backup testing, performing weekly data backup verification, conducting monthly backup integrity checks, and performing monthly backup testing. They are also responsible for generating and distributing the backup status reports to the General Manager.

By including regular backup verification and testing, the IT team can further ensure the reliability and effectiveness of the backup systems, reducing the risk of data loss and enhancing the organization's ability to recover swiftly in case of system failures or data corruption.

1. **Offsite Data Storage**: Critical data, especially related to CaMS and MCaMs, should be replicated and stored at an offsite location. In the event of a catastrophic event at the main data center, this offsite data can be used to restore operations swiftly. The offsite location should have robust security measures to protect the data.

**Mitigation Activity:** Offsite Data Storage and Disaster Recovery (DR)

Purpose: To ensure data redundancy, minimize data loss, and facilitate swift recovery in the event of a catastrophic event at the main data center.

**Data Replication**:

Critical data, including CaMS and MCaMs data, will be regularly replicated to an offsite location.

Replication frequency: Daily.

**Offsite Data Storage Location:**

DR facility provided by the Bhutan Telecom in Phuentsholing

**Data Encryption:**

Encrypt all data transferred to the offsite location to maintain data security during transit.

**Regular Testing:**

Conduct regular testing of the offsite data storage and recovery process to ensure data integrity and retrieval capability.

**Disaster Recovery (DR) Team Formation:**

Establish a dedicated Disaster Recovery (DR) Team responsible for overseeing

**DR activities.**

DR Plan Development:

Develop a comprehensive Disaster Recovery (DR) Plan detailing recovery procedures, roles, and responsibilities.

Include specific recovery time objectives (RTO) for critical systems.

**Documentation:**

Maintain up-to-date documentation of offsite data storage procedures and DR plans.

**Recovery Procedures:**

Document specific recovery procedures for critical systems, including CaMS and MCaMs.

Include step-by-step instructions for system restoration, data recovery, and testing procedures.

Assign responsible individuals for each step of the recovery process.

Responsibilities:

| **Responsibility** | **Description** |
| --- | --- |
| IT Team | - Ensure daily data replication to the offsite location.  - Implement data encryption for data in transit.  - Conduct regular testing of the offsite data storage and recovery process.  - Maintain up-to-date documentation of offsite data storage procedures. |
| Disaster Recovery (DR) Team | - Formulate and oversee the Disaster Recovery (DR) Plan.  - Develop and maintain documentation of recovery procedures.  - Conduct regular DR plan testing and exercises.  - Execute recovery procedures in the event of a disaster. |
| Security Team | - Implement and manage security measures at the offsite storage location. - Ensure access controls, surveillance, and environmental controls are in place and effective. |
| Management | - Provide support and resources for the implementation and maintenance of offsite data storage and DR activities.  - Ensure compliance with security and environmental standards. |

1. **Redundancy in IT HR:** Recognizing that IT HR is a critical function, RSEB should work on creating redundancy within the IT team. Cross-training team members in different IT functions can help mitigate risks associated with the sudden unavailability or departure of key IT personnel. The redundancy in IT HR is explained in chapter number 5.
2. **Incident Response Plan:** Develop and regularly update an incident response plan that outlines the steps to be taken in the event of disruptions, including cyberattacks, system failures, or IT HR unavailability. This plan should detail roles and responsibilities, communication protocols, and the sequence of actions to ensure a coordinated response.
3. **Regular Testing and Drills:** Regularly conduct simulation exercises and drills to assess the effectiveness of the BCP and to train staff on how to respond to different types of disruptions. These drills should include scenarios related to IT system failures, data breaches, and the departure of key IT personnel.
4. **Collaboration with Vendors:** Even though our IT team has developed the overall system, maintaining a positive relationship with IT vendors can be beneficial. They can provide support and expertise during critical times, such as system upgrades or complex issue resolution.

# **IT HR-Retention Policy**

The RSEB recognizes the critical importance of IT Human Resources (HR) in maintaining the operational efficiency and business continuity of our organization. Given the recent trend of IT professionals seeking better opportunities abroad, the RSEB acknowledges the need for a robust retention policy to ensure the continuity of our IT operations. This policy outlines our commitment to retaining and developing IT talent to safeguard our day-to-day operations and long-term strategic objectives.

## **Competitive Compensation**

RSEB recognizes that attracting and retaining top IT talent requires offering competitive compensation packages. To ensure that RSEB’s IT professionals are compensated fairly and in line with industry standards, RSEB shall conduct regular salary benchmarking exercises. RSEB will also provide annual performance-based salary increments and bonuses to reward excellence and loyalty. RSEB has provided 50% scarcity allowance of their basic pay.

## **Knowledge Sharing**

To create redundancy within the IT team, the RSEB will establish a culture of knowledge sharing. Team members will be encouraged to document their work processes, share best practices, and provide training sessions to colleagues. This will ensure that critical knowledge is not confined to individual employees but is distributed across the team. The General manager and the IT head will take the full responsibility of knowledge sharing and prepare documents to establish the requisite talent pool is always available in the RSEB.

## **Cross-Functional Training**

RSEB will implement cross-functional training programs designed to equip IT team members with the skills and knowledge necessary to perform key functions within the IT department. This will include rotations and job shadowing to expose employees to different aspects of IT operations. The IT head will take responsibility of rotating the cross-functional responsibility and job shadowing amongst the IT employees.

## **Succession Planning**

Succession planning for the IT team at the RSEB is crucial to ensure the seamless continuity of operations, especially for the development and maintenance of critical systems like MCaMs and CaMs. As RSEB has only three IT employees, including the IT head, it is essential to establish a succession plan that allows for the proactive identification and development of potential successors. This plan will not only address the current need for redundancy but also ensure a smooth transition when key IT personnel decide to leave.

## **Identifying Potential Successors**

IT Employees:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SL. No | Name | Position | Experience in RSEB | System Developed | Programming language and Framework |
| 1 | Bijoy Chhetri | IT Head | 12 years | CaMS, mCaMS (Mobile App), BCE, Auction | PHP, Dart, Python, JavaScript, HTML, Laravel, Django, Flutter |
| 2 | Tashi Dendup | System Developer | 4 years | CaMS, Bhutan Crowdfunding, Auction, website | PHP, Python, JavaScript, HTML, Vue JS, Laravel, Django |
| 3 | Deepak Archarya | System Developer | 7 months | BCE, Escrow System | PHP, Python, JavaScript, HTML, Laravel, Django |

Based on the above information, the potential successors within the IT team are as follows:

**Successor to IT Head (Bijoy Chhetri):**

Mr. Tashi Dendup

**Successor to Mr. Tashi Dendup (System Developer):**

Mr. Deepak Archarya

It is crucial to emphasize that a smooth transition of knowledge and responsibilities should take place before any officer leaves their position. This involves a comprehensive handover process where the successor confirms their readiness to assume the departing officer's responsibilities. This ensures a seamless transfer of knowledge and expertise, maintaining the continuity of critical roles within the organization.

This table above provides a clear overview of the potential successors, their experience, the systems they've worked on, and their technical skills, making it easier for the succession planning process. Further, it is imperative for RSEB to maintain a minimum of three IT professionals possessing the necessary skills to operate RSEB's systems effectively. Additionally, the Board should consider granting the authority to directly hire experienced human resources for RSEB when required.

## **Cross-Training and Skill Development**

Training Plan: Develop a training and skill development plan for potential successors. This plan should cover technical skills related to Mcams, Cams, PHP, MariaDB, and other relevant technologies. IT departemet to develop the plan.

Mentorship: Assign senior IT team members as mentors to guide and train potential successors.

## **Transition Planning**

**Notice Period and Transition Plan:** All IT team members must provide a minimum of six months' notice before leaving the organization, allowing sufficient time for a smooth transition. During this six-month period, the departing employee is responsible for creating a comprehensive handover plan, which must be approved by the management, including the IT Head. This plan will detail the transfer of responsibilities, system access, and knowledge sharing between the departing employee and their successor.

**Promotion and Advisory Role:** Upon submitting their notice, the successor will automatically be promoted to the departing employee's position. The departing employee will then assume the role of an advisor to the successor, ensuring a successful transition. If the handover is completed satisfactorily before the six-month period, the management may release the departing employee earlier.

**Successor Recruitment:** In cases where a departing employee does not have a designated successor, the management will promptly initiate the recruitment process through various channels, including competitive hiring or headhunting. This recruitment should be finalized within one month. Once the new employee is hired, they will assume the role of the departing employee's successor, and the handover process will be facilitated by the departing employee.

## **Recruitment and On boarding**

External Hiring: If no suitable internal candidates are available, initiate the recruitment process to hire qualified individuals. This process should start well in advance of the expected departure date.

Onboarding: Ensure that new hires receive thorough onboarding and orientation to understand the organization's systems and culture.

# **Documentation**

Effective documentation management is the cornerstone of a resilient and secure information technology environment. In an era where technological systems form the backbone of our operations, the ability to capture, organize, and safeguard critical information is paramount. This outlines the fundamental principles and importance of document management within RSEB.

In today's rapidly evolving IT landscape, RSEB relies on in-house developed systems and applications, including our mobile app, to drive efficiency and innovation. These systems encompass intricate programing codes, intricate database structures, and an array of interconnected components such as API that connects to different external and internal system. So managing the code documentation, password management and infrastructure design is not only a best practice but an absolute necessity.

Documentation management extends beyond the mere accumulation of files; it encompasses the meticulous recording and preservation of vital details related to system codes, passwords, network and infrastructure design, and database structures. These records serve as a repository of knowledge, enabling our organization to:

1. **Ensure Continuity:** In the face of unforeseen disruptions, a well-documented system empowers our IT team to recover swiftly and resume operations, minimizing downtime and losses.
2. **Facilitate Knowledge Transfer**: Properly documented systems allow for seamless knowledge transfer between team members, ensuring that critical insights and expertise are retained within our organization.
3. **Enhance Security:** By safeguarding passwords and access credentials, we fortify our defences against unauthorized access and data breaches.

In this documentation management framework, responsibility is assigned, access is controlled, and best practices are established for each category of documentation. Regular updates and thorough reviews ensure that our records remain accurate, accessible, and aligned with evolving organizational needs.

Furthermore, this documentation management strategy promotes a culture of accountability and transparency within our IT team. It empowers our members to contribute actively to the collective knowledge base and strengthens our resilience in the face of adversity.

# **System Codes and Source Code document:**

The RSEB have now currently developed the following systems:

1. CAMS
2. MCAMS(Mobile App)
3. Auction
4. Bhutan Commodity Exchange System
5. Crowdfunding Platform

The System is developed using PHP, JSP and the database is in MariaDB. The mobile app is developed in flutter. The IT Head is responsible for managing and safeguarding the source code and system codes.

The RSEB has developed documentation for each code line explaining the logic and coding techniques. This code document is essential for business continuity and imparting knowledge to the new recruits.

Location: The source code repository and the code documentation is hosted on a secure server, accessible only to authorized personnel.

Access Control: Access to the source code repository is restricted to IT personnel with appropriate permissions.

Version Control: Version control system is used to track changes, updates, and historical versions of the source code.

Regular Backups: Schedule regular backups of the source code repository to prevent data loss is done through the backup policy.

# **Password Management:**

Responsibility: The IT Head is responsible for password management.

Password Storage: Passwords must be securely stored using encryption and stored in a password management system/ or register.

Access Control: Access to the password management system is restricted to authorized personnel only.

Regular Updates: Passwords should be regularly updated and never shared in plaintext.

# **Network and Infrastructure Design:**

Responsibility: Network and infrastructure design documentation are managed by the IT Head.

Documentation Location: These documents should be stored in a secure location, preferably offline, and regularly updated.

Access Control: Limit access to network and infrastructure design documents to authorized personnel.

Change Tracking: Implement a change tracking system to record any modifications to network and infrastructure design.

# **Database Information:**

Responsibility: The IT Head is responsible for managing and documenting database information.

Database Documentation: Maintain documentation about the database schema, data dictionaries, and backup procedures.

Access Control: Limit access to database information to authorized IT personnel.

Regular Backups: Ensure regular backups of critical databases and document the backup process.

# **Training and Knowledge Transfer:**

The General Manager will conduct regular training sessions for IT personnel to ensure they understand the importance of documentation management and can effectively access and utilize the documentation.

# **Documentation Review:**

The General Manager will periodically review and update all documentation to ensure it remains accurate and up-to-date.

# **Accessibility in Emergency:**

Access to all critical documentation will be under the control of the General Manager and the IT Head. In the absence of both the General Manager and the IT Head, access will be granted to the IT Head's successor.

The General Manager will also ensure that designated personnel can access essential documents in emergency situations, even if primary access points become unavailable

# **Support Documentation:**

The IT team will maintain a comprehensive log detailing all software maintenance activities and changes carried out in response to any user issues in the software. This document should be updated promptly as issues are resolved. The historical record of issues resolved by the IT team will serve as a valuable reference for addressing future problems.

# **Documentation Retention:**

All critical documentation should be securely printed and maintained in duplicate. One copy should be stored in a bank's safe deposit box located outside the office premises, and the other copy should be secured in the office vault. Access to the office vault should be restricted to the General Manager and the IT Head.

Regular updates to documents should be carried out according to the version management, and these updates must also be printed and stored in a similar manner.

# **BCP Team and Their Responsibilities:**

|  |  |
| --- | --- |
| **Position** | **BCP Team** |
| Report to | Board |
| Team Member | Chief Executive Officer, Chairperson  General Manager  IT Head |
| Roles/responsibilities | 1. Convene an emergency meeting immediately following occurrence of the mishap/incident 2. Appoint focal persons for liaising with relevant emergency and risk mitigation agencies 3. Inform/communicate situation report to Board members, regulators and other relevant authorities 4. Coordinate and supervise immediate evacuation and emergency response efforts 5. Implement BCP as per BCP Activation details contained under Section on 8 of this document 6. Facilitate recovery/restoration of business operations to normalcy within the set Recovery Time Objective 7. Ensuring periodic review and update of BCP |

# **Detailed plan for implementation of BCP immediately following occurrence of disruptions:**

The following table lays out the detailed plan for implementation of the mitigation and recovery strategy immediately following the occurrence of threat/disruption:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nature/Type of risk** | | **Immediate response**  **(On occurrence)** | **Responsible team** | **Mitigation Strategy to be implemented** | **Recovery time objective** |
| 1. **Total loss of access to work place facility** - owing to occurrence of natural calamities like fire, earthquake, windstorm, flood, Acts of terrorism; | | 1. Inform BCP team  2. Prepare to move/transport critical operational staff to backup site  3. Initiate setting up of work place for staff at backup site | 1.CEO  2.GM  3. Head, IT  4.Head ADM | 1. GM , IT Head & relevant staff move to backup site 2. Commence work from backup location 3. Communicate with customer regarding the disaster and share new contact numbers. | 1. Preparation – 1st day 2. Move to site – 2nd day 3. Commence work – 3rd day |
| 1. **Partial loss of access to workplace facility -** owing to occurrence of natural calamities like fire, earthquake, windstorm, flood, Acts of terrorism; | | 1. Inform BCP Mgt team  2. Assess ground situation and map staff requirement to the functions disrupted  3. Arrange for moving of relevant staff to operate from backup site  4. Arrange workplace for staff at backup site | 1.CEO  2.GM  3. Head, IT  4.Head ADM | 1.IT Head & relevant staff move to backup site  2.Commence work from backup location  3.Communicate with customer regarding the disaster and share new contact numbers.  4.Perform Damage Assessment | 1.Preparation – 1st day  2.Move to site – 2nd day  3.Commence work – 3rd day |
| 1. **Total Server/System failure** - Loss/failure to provide core services due to systems failure/malfunction; | | 1.Inform BCP Mgt team  2. Assess ground situation and chalk out next course of action (server recovery)  3. If the primary site is not functional, initiate arrangement to connect to recovery site online. | 1.CEO  2.GM  3. Head, IT  4.Head ADM | 1. IT Head & Critical staff to assess possible alternatives.  2.Switch to Recovery site if primary site not recoverable.  3.Recover data from recovery site  4.Communicate with customer regarding the disaster.  5.Commence work on brining primary site online. | 1.Conduct situation Assessment – 1st Day  2.Switch on Recovery site – 2nd Day  3.Work on transiting to Primary Site – 3rd Day  4.Conduct Detailed Assessment/Report – 4th Day |
| 1. **Loss of Data** - Loss/failure due to the cyber-attacks (hacking) | | 1.Inform BCP Mgt team  2. Assess extent of loss and recoverability of lost data  3. Inform Regulators and stakeholders  4. Switch to the Recovery Site | 1.CEO  2.GM  3. Head, IT  4.Head ADM | 1. IT Head & Critical staff to assess extent or severity of loss.  2.Commence data recovery work using Recovery site  4.Carry out in-depth study and identify point/source of data breach and prepare future mitigation strategies. | 1.Assessing extent/severity of data Loss- 1st day onward  2.Commence data recovery work - 2nd Day  3.Work on Recovering data to the Primary Site -4th Day |
| 1. **People movement restrictions -** Restrictions on people (employee) movement during times of lockdowns owing to epidemics and pandemics | | 1.Contact Central Command Centre, RMA  2. Brief entire staff on the situation  3. Liaise with Command Centre for Emergency movement pass  3. Enable necessary remote access system. | 1. Focal Person  2.IT Official | 1. Focal Person to liaise with Central Command Center for guidance and direction.  2. Facilitate movement of critical staff to worksite  3. Execute work-from-home arrangement for non-critical staff  4. Implement work monitoring/reporting system | 1.Liaising with CC – 1st hour  2.Briefing all staff – 1st hour  3. Arranging for movement pass for critical staff – 1st day  4. Commence W-F-Home – 1st day |
| 1. **Total Loss of Internet connectivity** – if internet service of current service provider is down | 1.Inform BCP Mgt team  2. ITD Head to obtain firsthand information on the nature/expected duration of disruption  3. Assess ground situation and prepare to swich to next service provider | | 1.CEO  2.GM  3. Head, IT  4.Head ADM | 1. IT Head to liaise with alternate network service provider.  2.Work on brining the primary connectivity operational. | 1.Failure Assessment – 1st Day  2.Fixing of Failure – 1st Day  3.Switch to secondary service provider if necessary. -2nd Day |
| 1. **Total Failure of electricity:**  * *Gridline* * *Substation* * *Workplace* | 1.Inform BCP Mgt team  2. Head, ADM to liaise with BPC (grid failure) or NPPF Real Estate in case of power outages at work place and obtain 1st hand information on nature/expected duration of service disruption 3.Monitor the UPS usage and ensure Ups backup if power outage extends more than 1 Hrs. | | 1.CEO  2.GM  3. Head, IT  4.Head ADM | 1. IT Head to assess & monitor UPS battery life. 2. Turn off power for non-critical system to extend battery life. 3. Liaise with GM to restore power supply if power outage has occurred at substation or workplace. 4. Arrange for UPS backup | 1.Depending on situation, arrange necessary back up - 1st hour  2.Liaise with relevant suppliers for backup resources- 1st Day |

# **Expenditure incurred during emergency:**

CEO shall be empowered to approve funds for the purchase of goods and services that are critical to facilitating quick recovery/restoration of business to normalcy. He shall, however submit a report of his decisions to the Board as soon as possible for necessary ratification.

# **Periodic review and update of BCP:**

The GM shall be responsible for updating all information in the Emergency Contact Toolkit as and when changes occur. He/she shall be responsible for incorporating the relevant changes in the BCP document and initiating review, update and testing of the BCP at least once a year to reflect changes in RSEB’s IT environment, business priorities, operational structure and other factors.

# **Emergency contact toolkit:**

1. **Emergency contact**:

|  |  |
| --- | --- |
| Helpline | Emergency Number |
| Fire | 110 |
| Traffic | 111 |
| Ambulance | 112 |
| Crime | 113 |
| Disaster Communication | 999 |

1. **Agency Contact Number Toll free**

|  |  |
| --- | --- |
| Helpline | Emergency Number |
| Bhutan Power Corporation | 1250 |
| Bhutan Telecom | 1600 |
| Tashi Cell | 7700 |
| RMA’s Command Center | 1025 |
| RICB | 181 |
| BIL | 201 |