Disaster Recovery Procedure and Plan

[Brgy. Poblacion District III, Pozorrubio Pangasinan]

Group Members:

Hannah Rose O. Corpuz

Aaron E. Lopez

Jeamkely Vhon S. Bautista

1.1 Introduction

Barangays, which are the smallest local government units in the Philippines, play a vital role in responding to and recovering from disasters. The Barangay Poblacion District III Disaster Recovery Procedure gives the local authorities a framework for planning, preparing, responding to, and recovering from disasters.

A disaster recovery procedure and plan, which is an essential document, outlines the steps that a community must follow to ensure the continuation of important services and operations in the event of a catastrophe. Unavoidable events like disasters, which can strike at any time and have devastating consequences for communities, are a constant risk. The barangay must have a complete disaster recovery plan (DRP) in place to safeguard the health and safety of inhabitants, minimize damage, and swiftly resume normal operations.

1.2 Scope

This disaster recovery plan is designed to ensure the protection and recovery of important assets of Barangay Poblacion 3 in the event of a disaster. The plan covers a range of assets like physical infrastructure, equipment, data, and documents. The plan assumes that the barangay has identified its critical assets and has conducted a risk assessment to prioritize these assets for protection and recovery.

The plan also defines a sequence of steps and procedures for disaster response and recovery, including emergency response procedures, damage assessment and prioritization, resource allocation and mobilization, recovery strategies, and testing and validation. The plan includes arrangements for maintaining critical operations during and after a disaster and restoring normal operations as quickly as possible.

The plan also recognizes the need for ongoing maintenance and testing to ensure the plan's effectiveness and to identify areas for improvement. The plan will be regularly reviewed and updated to reflect changes in the barangay's critical assets, risks, and response capabilities. The plan will be communicated to all relevant stakeholders, including barangay officials, residents, and third-party suppliers, to ensure a coordinated and effective response to a disaster.

1.3 Aims

1. To ensure the safety and protection of the barangay’s residents.
2. To manage and respond to unforeseen and impactful occurrences that may be encountered.
3. To reduce and lessen the negative impact on the operations of barangay services as much as possible.
4. To enable normal working to be resumed in the shortest possible time to maximize work efficiency.
5. To ensure business continuity by minimizing the impact of an IT disruption on the organization's operations, reputation, and financial stability, and to facilitate the prompt recovery of critical IT systems and data.

1.4 Objectives

- To identify critical IT systems used by the barangay and prioritize their recovery to ensure essential functions can be restored first.
- To establish clear roles and responsibilities for all involved in IT disaster recovery efforts, ensuring that everyone knows what to do during a crisis.
- To establish reliable and efficient communication channels to ensure all stakeholders are informed and updates are shared promptly.
- To ensure all necessary IT resources, such as backup systems, data, and applications, are readily available to support the recovery process.
- To regularly test and update the IT disaster recovery plan to reflect changes in barangay operations, technology, and potential risks.
- To protect the integrity and security of data, systems, and applications, while recovering from disaster or major disruption.
- To comply with industry regulations and best practices for IT disaster recovery planning, ensuring that the barangay is prepared to meet its obligations in this regard.
- To minimize financial losses incurred because of an IT disaster.
- To minimize the impact of an IT disaster or disruption on the barangay's operations, ensuring continuity and limiting downtime.

1.5 Preparation

1.5.1 Preventative Strategies

- Conduct regular risk assessments
- Establish an emergency response team
- Implement disaster-resistant infrastructure
- Develop a communication plan

- Regularly backup critical data and documents
- Conduct regular drills and exercises for the community.

1.5.2 Acceptable Use

Ensure that they have a structured approach in place to manage the impacts of a disaster effectively, minimize damage, and promptly resume normal operations. It also recognizes the importance of digitizing documents for backup and provisions for secure storage and management of digital documents to ensure their availability and integrity. It is regularly reviewed and updated to reflect changes in the barangay's critical assets, risks, and response capabilities.

1.5.3 Communicating the Plan

Communicate the Disaster Recovery Plan, the barangay can ensure that everyone is prepared to respond and recover from disasters, safeguard important assets, and minimize the negative impact on operations.

1.5.4 Testing and Review

To ensure the effectiveness of a disaster recovery plan, it is important to review and test the plan. The review should include a check that the plan is up-to-date and includes all necessary information. Testing the plan involves running a simulated disaster scenario to evaluate the plan's effectiveness, followed by an evaluation to identify areas for improvement. Based on the evaluation, changes can be made to the plan as necessary, and the plan should be regularly reviewed and updated to remain effective. It is also important to train key staff members on any changes made to the plan. Lastly, it is important for the IT management team to regularly test their backup systems. This ensures that there are no issues when a disaster occurs and confirms that the data remains safe and secure.

1.5.5 Making Templates Readily Available

Having templates readily accessible for reporting, recording, logging incidents, actions, and communicating with stakeholders is highly recommended.

1.6 Barangay Disaster Recovery Team and Access Rights

1.6.1 Recovery and Response Team

In the event of this plan having to be initiated, the personnel named below will form the Disaster Recovery Team and take control of the following:

	Name	Position in Brgy	Contact Details
Team Leader	Hon. Felipe Legaspi	Barangay Captain	09106468293
Backup and Recovery Administrator	Mrs. Jovita Reyes	Barangay ICT (Information and Communication Technology) Admin and Secretary	Not Available
Communication	Mr. Michael Valdez	Barangay Kagawad Radio Officer	Not Available
Emergency Response Team	Mr. Honorato Pecson	Barangay Kagawad Driver	Not Available
	Mr. Arthur Valdez	Barangay Health Worker	09950277722
	Mrs. Evelyn Quirimit	Barangay Health Worker	Not Available

Table 1.1 Recovery and Response Team

1.6.2 Back up Management and Access

List of personnel in the barangay that has access to the back up of E-documents and data of every person within the barangay poblacion III.

Name	Position in Brgy	Contact Details
Hon. Felipe Legaspi	Barangay Captain	09106468293
Mrs. Jovita Reyes	Barangay ICT Admin and Secretary	Not Available
Ms. Elizabeth Quinto	Barangay Assistant Secretary	09108273124

Table 1.2 Back up Management and Access

1.6.3 Emergency Response Volunteers

This is a list of volunteers in the barangay willing to help respond to community needs during a disaster.

Name	Contact Details
Hon. Felipe Legaspi	09106468293
Mrs. Jovita Reyes	Not Available
Ms. Elizabeth Quinto	09108273124

Table 1.3 Emergency Response Volunteer

In the event of an incident, it may be helpful to consider how you would access the following:

- Important contact information
- Communication channels
- Evacuation routes and meeting areas
- Emergency supplies and resources
- Hazard maps and critical infrastructure
- Roles and responsibilities
- Document backup system
- Collaborative agreements
- Information dissemination methods

It is crucial to regularly review and update the disaster preparedness plan to ensure its relevance and alignment with the evolving needs of the community, including the backup of important documents through a reliable system.

1.7 Backup Strategy

Process	Backup Type (Include on-site/ off-site)
Backup on-site through external storage	Regularly, it is crucial to create backups of barangay records that have been digitized. These backups should be stored on external storage devices like external hard drives, network-attached storage (NAS), or tape drives. These storage devices are kept at the same location and allow quick retrieval of backups when needed.
Cloud Backup	To ensure additional protection, it is recommended to store backups of the barangay records off-site using cloud-based backup services. These services securely transmit and store the data from the records in the cloud. This approach enables remote access to the backups and facilitates disaster recovery in case of an on-site catastrophe or calamity. By leveraging the cloud, the barangay records are safeguarded and accessible from anywhere, offering an extra layer of security and flexibility.
Disk Imaging	By capturing a comprehensive image or snapshot of the disks or partitions containing the barangay records, it is possible to create a complete replica of the entire system. This method facilitates a full system recovery by restoring the entire disk image onto a new machine or disk
Incremental backup	In this approach, only the changes or updates made since the last backup are stored. Instead of duplicating the entire dataset, only the modified or new files are backed up, reducing the backup time and storage space required. This strategy is useful for organizations with enormous amounts of data that change frequently, as it allows for efficient backups while still ensuring data integrity and the ability to restore to a specific point in time.
Central server replication	Establish a centralized backup server in a separate location, either inside the same firm or at a distant data center. The data barangay is duplicated and synchronized with the central server in real time or regularly.
Hybrid Backup	Use a hybrid of on-site and off-site backup techniques. Regular on-site backups, for example, can be supplemented with periodic cloud backups for extra off-site security.
HR / Personnel Records	On-site backups involve storing data physically at the barangay hall using local servers or storage devices. Off-site backups, however, utilize cloud backup or remote data replication to store copies of personnel records in

	a separate location. This dual approach provides quick access to backups and enhanced protection against on-site incidents, thereby improving the security and availability of personnel records.

Table 2.1 Back Up Strategy

1.8 Disaster Recovery Plan

A. Create a Disaster Response Team and Document Responsibilities:

1. Establish a Disaster Recovery Team (DRT) that will be responsible for the recovery process. This team should include individuals from different departments or organizations within the barangay, such as local government officials, emergency services personnel, community leaders, and volunteers.

2. Develop a communication plan that will keep all stakeholders informed during and after the disaster. This plan should include contact information for team members, communication channels to reach out to the people of the community, the municipality, and other barangay, and protocols for sharing updates and valuable information.

B. Set Clear RTOs and RPOs:

1. Ensure rapid recovery from any disaster by setting clear Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). RTO denotes the maximum acceptable downtime for critical systems or services, while RPO indicates the maximum acceptable data loss.

2. Identify critical systems and applications in the barangay, assess their impact on operations, and determine the appropriate RTO and RPO for each of them.

C. Make a blueprint of the Network Infrastructure:

1. Create detailed documentation of the barangay's network infrastructure, including hardware, software, and connectivity details. This documentation will facilitate faster and easier system recovery in case of corruption or cyberattacks.

2. Conduct a risk assessment to identify potential hazards specific to the barangay, such as natural disasters, infrastructure vulnerabilities, or security threats. Assess the impact of these hazards on critical systems and applications.

3. Develop a comprehensive Disaster Recovery Plan (DRP) that outlines procedures and protocols to follow in a disaster. This plan should include steps for data backup and restoration, IT recovery, and business continuity.

4. Regularly back up all critical systems, applications, and data, and store them securely off-site or in the cloud. Consider the dependencies between systems and prioritize their recovery accordingly.

D. Select a Disaster Recovery Solution:

1. Develop a contingency plan that outlines alternative solutions for critical systems and applications in case of failure. This may include redundant systems, backup locations, or cloud-based services.

2. Choose a disaster recovery solution that offers quick recovery times and ensures system availability during and after a disaster.

3. Establish an emergency response plan that outlines what to do in an emergency, including evacuation procedures, safety guidelines, and emergency contacts.

4. Develop a training program to educate employees, volunteers, and stakeholders on the disaster recovery plan and emergency response procedures. Conduct regular training sessions to ensure everyone is familiar with their roles and responsibilities.

E. Create a checklist of criteria for initiating the Disaster Response Plan:

1. Create a checklist of specific criteria that will help the recovery team identify when it is time to activate the Disaster Recovery Plan. This will prevent wasting resources or delaying the response when a disaster occurs. Criteria may include factors such as the severity of the event, the impact on critical systems, or the safety of personnel.

F. Document the Disaster Recovery Process:

1. Ensure data and operations are restored quickly after a disaster by creating step-by-step instructions for the disaster recovery team. These instructions should outline the necessary actions, tasks, and procedures to initiate and execute the recovery effort.

2. Store copies of the disaster recovery plan in multiple locations, including off-site storage or secure cloud services, to protect it from corruption or physical loss during a disaster.

G. Test your Disaster Recovery Plan:

1. Conduct regular tests of the disaster recovery plan to ensure that all procedures are up-to-date, effective, and can be executed in a timely manner. Test different scenarios and simulate various disaster situations to evaluate the plan's effectiveness.

2. Perform partial recovery tests at least twice a year and conduct full recovery simulations annually to validate the plan's functionality and identify any areas that need improvement.

H. Review and update your Disaster Recovery Plan regularly:

1. Regularly review and update the disaster recovery plan to reflect any changes in business operations, modern technology, or potential hazards. Assign a responsible person or team to conduct periodic reviews and make necessary revisions to keep the plan relevant and effective.

2. Involve key stakeholders in the review process, including the DRT members, community leaders, and relevant government agencies. Seek feedback and incorporate their insights into the plan.

1.9 Data Recovery

To assist data recovery in a barangay setting, it is important to follow certain guidelines when damage to a computer or backup material is suspected. Here are the recommended steps:

1. Do not turn off electrical power to any computer.
2. Do not attempt to retrieve data by running the hard drive, backup disc, or tape.
3. Do not tamper with or move damaged computers, discs, or tapes.
4. Isolate devices from the network in the event of a suspected cyber-attack.

In cases of suspected data damage or cyber-attacks, it is advisable to seek professional assistance from IT experts or data recovery specialists who have the knowledge and tools to handle such situations.

1.10 Key Roles and Responsibilities

These roles and responsibilities can vary depending on the specific structure and needs of the barangay. It is important to adapt and tailor them accordingly to the local context and requirements.

Barangay Captain

- Oversees the overall operations and administration of the barangay.
- Represents the barangay in official functions and meetings.
- Implements barangay policies and programs.
- Collaborates with local government units and other organizations for community development.
- Ensures the delivery of basic services to barangay residents.

Barangay Secretary

- Records and documents barangay council meetings and proceedings.
- Maintains and updates barangay files and records.
- Prepares official correspondence and reports.
- Assists in the dissemination of information within the barangay.

Barangay Treasurer

- Manages the barangay's finances and budget.
- Collects and records barangay revenues and fees.

- Pays authorized expenses and ensures proper documentation.
- Prepares financial reports and statements.
- Assists in the auditing of barangay accounts.

Barangay Kagawad and Tanod (Barangay Watchmen)

- Maintains peace and order within the barangay.
- Conducts regular patrols and reports any suspicious activities.
- Assists in traffic management and crowd control.
- Assists in disaster preparedness and response.
- Aids barangay residents in need.

Barangay Health Workers

- Promotes health and wellness in the barangay.
- Conducts health education and awareness campaigns.
- Assists in the implementation of vaccination programs.
- Monitors and reports health issues and concerns.
- Provides basic medical assistance and referrals.

Barangay Livelihood Officer

- Facilitates livelihood programs and projects.
- Assists in skills training and capacity building.
- Identifies opportunities for income generation.
- Provides support and resources to entrepreneurs.
- Monitors and evaluates the impact of livelihood initiatives.

1.11 Insurance

As part of the barangay's disaster risk and preparedness strategies, maintaining contact with insurance providers is essential. It is important to be aware of any omissions, liability clauses, or specific requirements that, if not fulfilled, could potentially invalidate insurance coverage. The following insurance contacts should be documented:

During business hours, please contact: Mr. John Ubaldo, City Treasurer's Office

Phone: 09950283712

For emergencies or outside of business hours, please contact: Ms. Maxine Reyes

Phone: 09957728392

Location of insurance policy: City Treasurer's Office, Municipal Building of Pozorrubio

Regularly reviewing and updating the insurance component of the DRPP is recommended to address any changes in coverage or policy requirements.

Policy Name	Coverage Type	Coverage Period	Amount Coverage	Known Exemptions	Next Renewal Date
Barangay Members Health Insurance	Health Insurance	January 01, 2023, to December 31, 2024	Php 5,000.00	Dental and orthodontic treatments are not covered. Additionally, there may be waiting periods for coverage of pre-existing conditions.	January 01, 2024
Fire Policy	Property Insurance (Fire coverage)	May 04, 2023, to May 04, 2024	Php 10,000.00	Damage from earthquakes, floods, and acts of war	May 04, 2024

				are not covered. Certain high-risk commodities or hazardous compounds may be specifically excluded from the policy.	
Equipment Policy	Property Insurance (Equipment coverage)	May 04, 2023, to May 04, 2024	Php 25,000.00 per any one occurrence	Normal wear and tear, mechanical breakdown, and damage caused by willful or negligent activities are not covered. Certain high-risk or specialized equipment types may be specifically excluded from the coverage.	May 04, 2024

Table 3.1 Insurance Policy

1.12 Media Communication Protocol

Within the framework of the Barangay Disaster Risk and Preparedness Plan (DRPP), it is essential to establish a designated system for media communication during and after a disaster. This system adheres to predefined guidelines, as outlined in the Critical Incident Plan, ensuring effective handling of post-disaster communication with media outlets. The following principles should be observed by the staff responsible for media contact:

1. Provision of Verified Facts: The staff assigned to media contact should focus solely on delivering verified and accurate information. Maintaining the integrity of the information shared with the media and the public is of utmost importance.

2. Confirmation Procedures: In situations where confirming specific details may require additional time, it is acceptable to respond with statements such as "I am currently unable to provide that information." Once accurate information becomes available, it should be promptly shared with the media.

3. Addressing Information Requests: The staff responsible for media contact should consider the following essential aspects when responding to media inquiries:

    - Purpose of the Information Request: Understand the purpose behind the media's need for information.
    - Specific Details Required: Determine the exact information sought by the media.
    - Target Audience: Identify the intended recipients of the information.
    - Preferred Medium of Information Delivery: Ascertain the media's desired method of receiving the information (e.g., press release, interview).
    - Compliance with Standards and Criteria: Consider any special standards or criteria the information must meet.
    - Contextual Background: Assess whether additional contextual or background information is necessary.
    - Designated Information Provider: Determine the staff member responsible for supplying the required information.

4. Redirecting Inquiries: Personnel who have not been assigned the task of media communication should politely direct media inquiries or calls to the appropriate designated personnel. This ensures that accurate and consistent information is conveyed to the media.

By adhering to these media communication protocols, the barangay can effectively manage information requests following a disaster, promote transparency, and maintain control over the dissemination of accurate information.

Assigned Media Liaison(s):

Name: Mrs. Jovita Reyes	Role: Barangay Secretary
Name: Mr. Michael Valdez	Role: Barangay Kagawad/Radio Officer

1.13 Critical Activities and Data Assets

Digitizing Important Documents for Backup:

- Data Assets: Essential documents such as legal records, identification records, property records, financial records, emergency contact information, and critical infrastructure plans.
- Criticality: The loss of these documents could significantly impact the operations and decision-making processes of the barangay.
- Recovery Time: 24 hours for initial restoration, followed by ongoing backup updates.
- Temporary Workarounds: Implement manual record-keeping systems as a backup until digital restoration is completed.
- Outsourcing: Explore the possibility of outsourcing document digitization and backup services to expedite the process, if needed.
- Additional Resources: Allocate budget for document management systems, secure servers, and data backup solutions.

Disaster Plan for the Barangay:

- Data Assets: Emergency response plans, evacuation plans, communication protocols, hazard assessments, asset inventories, and community resources.
- Criticality: These plans and resources are crucial for efficiently responding to and mitigating various disaster scenarios.

- Recovery Time: 4 hours for initial activation and implementation of the disaster plan.
- Temporary Workarounds: Maintain physical copies of the plans and establish alternative communication channels in case of digital system failures.
- Outsourcing: Collaborate with external disaster management agencies or neighboring barangays to coordinate response efforts and share resources.
- Additional Resources: Allocate budget for training personnel in disaster response protocols, acquiring necessary safety equipment, and conducting regular drills and exercises.

Critical Activities	Data Asset Required for Service Continuity	Recovery Time	Workaround ? (Yes/No)	Temporary Workaround /Outsourcing Options	Additional Resources or Costs
Digitizing Important Documents	Legal records, identification records, property records, financial records, emergency contact information, critical infrastructure plans	24 hours	No	Maintain physical copies as backup	Document management systems, secure servers, data backup solutions
Disaster Response and Evacuation Plans	Comprehensive plans for several types of disasters, evacuation routes, designated shelters, resource allocation	Immediate	No	Maintain physical copies, regular drills, and training sessions	N/A
Critical Infrastructure Inventory	Inventory of essential infrastructure assets (roads,	Ongoing	No	Regularly update physical copies	N/A

	bridges, schools, healthcare facilities, utilities)				
Community Resource Database	Database of community resources (volunteer groups, NGOs (nongovernment organizations), medical facilities, disaster relief organizations)	Ongoing	No	Regularly update physical copies	N/A
Communication Protocols and Systems	Communication protocols, contact lists, communication channels, emergency broadcasting procedures	Immediate	Yes/No	Implement alternative channels if necessary	N/A

Table 4.1 Critical Activities and Data Assets

1.14 Contact List and Notification Calling Tree

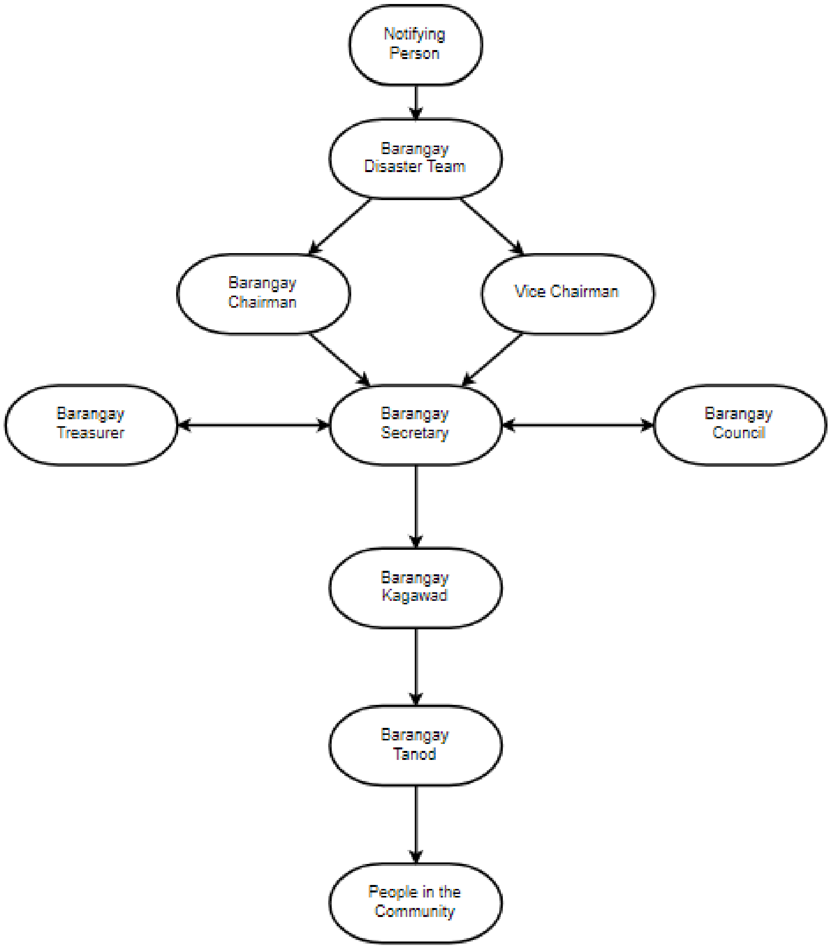

Figure 1.1 Notification Calling Tree

Appendix 1

A.1. Incident Impact Assessment

Operational	No Impact	There is no noticeable impact on the barangay's ability to function.
	Minor Impact	Although there is some functional impairment, it is minor. Tasks can still be accomplished, but they might require more time and be less efficient compared to normal conditions.
	Medium Impact	Some residents are no longer able to receive crucial services from the barangay. The loss of capability is evident, but with forethought and additional resources, workarounds are achievable.
	High Impact	Barangay residents can no longer depend on essential services provided by the barangay hall. It is highly likely that the barangay will either shut down or experience significant disruptions.

Table 5.1 Operational

Information	No Breach	There has been no unauthorized access, breach, or loss of data.
	Data Breach	Data that is not associated with individuals and falls under the category of personal information encompasses items such as action plans, instructional plans, policies, and meeting notes.

	Personal Data Breach	the event of unauthorized access or retrieval of sensitive personally identifiable information, any data that has the potential to cause a notable impact on the affected individuals or involved parties must be promptly reported to the ICO (Information Commissioner's Office) within a period of 72 hours (about 3 days).
	Integrity Loss	data breach has occurred where data, including sensitive personal information, has been altered or erased. This incident also involves instances of data corruption.

Table 5.2 Information

Restoration	Existing Resources	With the resources readily available to the cloud, recovery may be assisted quickly.
	Facilitated by Additional Resources	With extra resources that are conveniently accessible, recovery can be supported within a certain period.
	Third Party Services	Recovery is not assured, and outside assistance is necessary to aid or partially restore recovery.
	Not Recoverable	It is not possible to recover from the incident. Data might have been removed, encrypted, or backups failed.

Table 5.3 Restoration

Appendix 2

A.2. Risk Management

5 = Very High	5 = Severe
1 = Very Low	1 = Minor

Disaster Scenario	Probability Rating	Impact Rating	Mitigations / Alternatives Actions
Water Leak			For Barangay Hall, it is essential to ensure that servers are not placed directly on the floor. It is recommended to locate servers and other computers far from water pipelines when possible. Implementing the use of moisture detectors can provide a certain level of early warning in case of any moisture-related issues.
Fire			Ensuring the presence of off-site backups for the numerous critical records and files in the barangay is a vital practice that should be performed regularly. Additionally, maintaining clean and well-ventilated server areas, free from dust, is of utmost importance. It is crucial to emphasize the significance of implementing appropriate cabling and procedures to prevent the rapid spread of fires from other parts of the building to the establishment.
Vandalism			To maintain security within the barangay hall, it is important to discourage and detect instances of vandalism by implementing CCTV surveillance. Physical protection of servers should be ensured through locks and access restrictions. It is advisable to have separate and unique keys specifically designated for server rooms, instead of relying on general keys that may be shared throughout the establishment.
Power Failure			To address power interruptions, the inclusion of solar panels and a generator can be implemented as alternative power solutions. With the option for remote monitoring of uninterrupted power supply (UPS) systems and the availability of redundant UPS solutions are provided.
Cyber Attack			Examine backup rotations, apply security upgrades, and keep an eye on anti-virus and malware solutions. End users are also protected by strong screening.

Loss of Communication / Network Services			Minimize the risk of communication disruptions, implementing redundancy in wide area network (WAN) connections, ensuring resilience in voice networks, and utilizing diversely or alternatively routed trunks can be effective measures. These strategies help to decrease the probability of communication loss.
Loss of Building Access			If barangay premises cannot be accessed, an agreement with San Roque elementary school for temporary shelter to use their facilities and classrooms which can sustain key systems. Use cloud technologies to services and operation with the residents.

Table 6.1 Risk Management

Appendix 3

A.3 Communication Template

A. 3.1 School Open / Establishment Open

[Date]

Dear Residents,

I am writing to inform you about an incident that has affected our barangay, particularly [mention the specific incident, such as a natural disaster or a significant event]. As a result, we are currently facing [briefly explain the impact of the incident, such as disruption to services, infrastructure damage, or temporary closure of establishments].

Our barangay officials and relevant authorities are actively working to address the situation and ensure the safety and well-being of our community members. Although we understand that this may cause inconvenience and concerns, we want to assure you that every effort is being made to restore normalcy as quickly as possible.

At present, we anticipate that it may take [estimated time] to fully resolve the situation and restore all services. We are in constant communication with [list any organizations or agencies involved in the recovery efforts, if applicable] to expedite the process and minimize any further disruption.

During this period, we have conducted a thorough risk assessment to address any potential safety concerns and safeguard the welfare of our residents. We have implemented necessary measures to mitigate risks and ensure that necessary services are available to the best of our abilities.

While our barangay continues to recover, we kindly request your cooperation and understanding. We encourage you to stay updated through official channels, such as our [barangay website/social media platforms], where we will provide regular updates on the progress and any changes that may affect you or your children.

Please rest assured that the barangay officials are dedicated to resolving this situation and supporting our community. If you have any specific questions or require assistance, please do not hesitate to contact us at [provide contact information].

Thank you for your understanding, patience, and cooperation during this challenging time. Together, we will overcome these difficulties and emerge stronger as a community.

Yours sincerely,

[Your Name]

[Your Position]

Barangay Poblacion District 3

A.3.2 School Closure / Establishment Closure

[Date]

Dear Residents,

Subject: Temporary Closure of Barangay Poblacion District 3 Facilities

I am writing to inform you about an unfortunate incident that has led to the temporary closure of our facilities at Barangay Poblacion District 3. We have encountered [briefly describe the incident, such as a fire, natural disaster, or unforeseen circumstances].

Due to this incident, we are facing challenges in maintaining normal operations. Our priority is to ensure the safety and well-being of our community members, including students, teachers, and staff.

We want to assure you that we are taking immediate actions to address the situation. Here are some crucial details regarding the closure:

1. Duration: At present, we are unable to determine the exact timeline for reopening. However, we are working diligently to resolve the issues and restore normalcy as soon as possible.

2. Safety Measures: We have conducted a thorough risk assessment in coordination with relevant authorities and experts. This step ensures that necessary precautions are taken to safeguard the welfare of everyone associated with our facilities.

3. Communication Channels: We understand the importance of keeping you informed throughout this process. We will provide updates regularly via [mention communication channels you will use, such as website, social media platforms, or text messages].

We understand that this closure may pose inconveniences, especially regarding childcare arrangements. We apologize for any disruption caused and assure you that we are doing everything we can to minimize the impact on our community.

During this period, we encourage you to stay connected with us through our official communication channels for the latest updates. If you have any urgent concerns or queries, please do not hesitate to contact our dedicated helpline at [provide a contact number or email address].

We appreciate your understanding, support, and patience during this challenging time. The safety and well-being of our community remain our top priority, and we will continue to work diligently towards resolving the situation.

Thank you for your cooperation.

Yours sincerely,

[Your Name]

[Your Position]

[Contact Information]

A.3.3 Staff Statement Open

Dear Residents of Barangay Poblacion District 3,

I hope this message finds you well. As a staff member of Barangay Poblacion District 3, I want to take a moment to share crucial information with you regarding our comprehensive Disaster Recovery Plan. We understand the importance of safeguarding our community and ensuring business continuity during unforeseen events.

We believe that transparent and open communication is vital during times of uncertainty. We encourage you to contact us with any questions or to discuss specific aspects of our Disaster Recovery Plan relevant to our barangay. We welcome the opportunity to address your concerns and strengthen our partnership in ensuring the safety and well-being of our community.

Please note that staff members have been advised not to comment or make statements regarding the Disaster Recovery Plan for Barangay Poblacion District 3. We remain committed to ensuring the continuity and resilience of our operations and will continue to invest in the necessary resources and best practices to uphold the highest standards of safety and preparedness.

Thank you for your trust and cooperation in making Barangay Poblacion District 3 a resilient and secure community. For any inquiries or assistance, please contact us through our official channels. You can reach us on our Facebook page, [Facebook link] or call us at [Contact Details].

Best regards,

[Name]

[Position]

Barangay Poblacion District 3

A.3.4 Staff Statement Closure

Subject: Urgent: Important Information Regarding Recent Cybersecurity Incident

Dear Valued Residents,

I am writing to you as *ICT Admin and Secretary* of Barangay Poblacion-III with a sense of urgency and concern regarding a recent cybersecurity incident that has resulted in the unauthorized access and potential compromise of your information. We understand the gravity of this situation and want to provide you with immediate details, actions we are taking, and guidance to mitigate any potential impact on your data.

Regrettably, we have experienced a cyber-attack on our systems, and your information may have been accessed without authorization. Our utmost priority is to address this incident promptly, secure your data, and ensure that such incidents do not occur in the future.

We apologize for any inconvenience and concern this incident may have caused. We are committed to transparent communication, ongoing improvements in our security practices, and earning back your trust.

Your data are of paramount importance to us. We assure you that we are actively working to restore the integrity of our systems and fortify our defenses against cyber threats. Please reach out to our official Facebook page, Barangay Poblacion III or you may contact us at 0915 3444 234 for inquiries and assistance.

Thank you for your understanding and continued support as we address this cyber-attack and reinforce our commitment to your data security.

Best regards,

Mrs. Jovita Reyes

Barangay ICT Admin and Secretary

Barangay Poblacion III – Pozorrubio, Pangasinan

A.3.5. Media Statement

MEDIA STATEMENT FOR IMMEDIATE RELEASE

[Date the media statement will be released]

Subject: Barangay Poblacion III to Cybersecurity Incident

Pozorrubio, Pangasinan – Poblacion III, acknowledges and takes full responsibility for a recent cybersecurity incident that has impacted the security and privacy of our resident's data. We are deeply committed to the security and privacy of our residents, and we apologize for any inconvenience or concern this incident may have caused.

Upon discovery of the incident, our dedicated Disaster Recovery Team with the lead of Mrs. Jovita Reyes, immediately initiated a comprehensive investigation to assess the extent of the breach and implement remedial measures. We have also engaged external cybersecurity experts to support our efforts and ensure a swift and thorough response.

Our dedicated technical team is available to address any questions or concerns that our residents may have. We understand the importance of timely and accurate communication and will provide updates through our official Facebook page, Barangay Poblacion III or you may contact us at 0915 3444 234 for inquiries and assistance.

We would like to thank our Residents for their trust and patience during this challenging time. We remain steadfast in our commitment to ensuring the security and privacy of resident's data and will continue to work tirelessly to restore your confidence in our services.

A.3.6. Standard Response – Residents

Subject: Important Message to the Residents of Barangay Poblacion III

Dear [Resident's Name],

We would like to inform you about a recent incident that has affected our operations in Barangay Poblacion III. The details of the incident are as follows:

Date/Time of Incident: May 23, 2023, 8:15am
Nature of Incident: cyber-attack

We want to assure you that we are actively addressing the situation and taking necessary steps to restore services and ensure the safety of our community. Our team is diligently working on resolving the issue and minimizing any potential impact.

While we cannot provide an exact timeline for system restoration at this moment, please be assured that we are doing everything possible to expedite the process. Our priority is to resume normal operations as soon as possible.

For further inquiries or updates, we kindly request you to direct your inquiries to our assigned contact person *Ms. Elizabeth Quinto (09108273124)* our Barangay Assistant Secretary or visit our official Barangay Facebook page, Poblacion III for the latest information. We will also utilize other predetermined communication channels to keep you informed.

We apologize for any inconvenience caused by this incident and appreciate your understanding and support during this challenging time. Your trust and partnership with us are highly valued, and we are committed to resolving the matter swiftly.

Thank you for your cooperation.

Best regards,

Ms. Elizabeth Quinto

Barangay Assistant Secretary

Barangay Poblacion III – Pozorrubio, Pangasinan

A.3.7. Standard Response – Resident

Subject: Resident Inquiry: Disaster/Cyber-Attack Incident

Dear [Resident's Name],

Thank you for contacting us regarding the recent incident that has impacted Barangay Poblacion III. We acknowledge your concerns and want to assure you that we are actively addressing the situation and working diligently to resolve it.

We understand the inconvenience and worry caused by this incident. Our dedicated team is tirelessly investigating the matter, mitigating the impact, and restoring normal operations as quickly as possible.

Rest assured, safeguarding the security and privacy of your data remains our utmost priority. We have implemented heightened security measures to prevent unauthorized access and are taking steps to strengthen our systems to prevent future incidents.

We appreciate your understanding and patience during this challenging period. Your trust and partnership with us are invaluable, and we are fully committed to resolving this situation promptly and transparently. For any inquiries or assistance, please contact us through our official Facebook page or call 0915 3444 234.

Once again, we apologize for any inconvenience caused, and we deeply appreciate your ongoing support.

Best regards,

Hon. Felipe Legaspi

Barangay Captain

Barangay Poblacion III – Pozorrubio, Pangasinan

Appendix 4

A.4. Disaster Recovery Event Recording Form

Description or reference of disaster:	
Date of the incident:	
Date of the incident report:	
Date/time disaster recovery commenced:	
Data recovery work was completed:	
Was full recovery achieved?	

1.18.1 Relevant Referrals

Referral To	Contact Details	Contacted On (Time / Date)	Contacted By	Response

1.18.2 Actions Log

Recovery Tasks (In order of completion)	Person Responsible	Completion Date	Comments	Outcome
		Estimated Actual		

Appendix 5

A.5. Post Incident Evaluation

Response Grades 1-5
1 = Poor, ineffective and slow
5 = Efficient, well communicated, and effective

Action	Response Grading	Comments for Improvements / Amendments
Initial Incident Notification		
Enactment of the Action plan		
Coordination of the Disaster Recovery Team		
Communications Strategy		
Impact minimization		
Backup and restore processes		
Were contingency plans sufficient?		

Staff roles assigned and carried out correctly?		
Timescale for resolution / restore		
Was full recovery achieved?		
Log any requirements for additional training and suggested changes to policy / procedure:		