Foreword

Manila Teachers Mutual Aid System, Inc. (the "Association") in cooperation of Risk Management Committee recognized the need to revise and regularly update the Risk Management Manual of the Association, to keep pace with the anticipated rapid regulatory changes that are unavoidable in a dynamic economic environment. A revised Manual would also be able to appropriately take into account the strengthened supervisory and regulatory arrangements set out in the Insurance Commission (IC) regulations and other issuances. This Manual is one of the products that effort the benefits from the inputs of many concerned departments of the Association. We are hopeful that this Manual and its subsequent updates will be able to more effectively disseminate the regulatory issuances of the IC on a timely basis and provide appropriate guidance as mutual benefit association. Our vision is to be one of the leading providers of a high quality and diverse range of financial products and services through efficiency and innovativeness.

Preface

Manila Teachers Mutual Aid System, Inc. (the "Association") like any other mutual benefit association, are exposed to a variety of risks including credit, interest rate, liquidity, capital and operational risk. Failure to adequately manage these risks exposes the Association not only to the possibility that the association may suffer losses, but, more importantly, to the possibility that the association may not achieve the strategic business objectives. The focus of this manual has been traditionally on operational aspects, with attention to risk mainly directed towards Risk Management Plan, Business Development, Recovery and Continuity Plan, HR Risk Management Plan, IT Disaster and Emergency Preparedness. It is clear, however, that all types of risk is critical, more so as the Association adopt innovative technological products and related financial innovation. Therefore, it is imperative that our Association take the responsibility to carefully evaluate all types and levels of risk in the business operations and activities.

Presidential Decree No. 1566 *"Strengthening the Philippine Disaster Control, Capability and Establishing the National Program for Community Disaster Preparedness"* stresses the need for us Filipinos to seek survival against hazards. It states the urgency of need to direct, control and coordinates manpower, material, money, and spiritual resources in meeting disasters.

Rule 1040 of the Occupational Safety and Health Standards (as amended) states that each agency shall provide for the organization of disaster control groups/health safety committee in every place of employment and the conduct of periodic drills and exercises in workplaces.

The Manila Teachers Disaster Risk Reduction Management Manual (Primer) is based/adapted from the Department of Education Resource Manual on the topic, flyers from the Philippine Institute of Volcano logy and Seismology, handouts during seminars and information on disaster risk reduction accessed from the Internet.

Besides complying with the Presidential Decree to prepare establishments and their employees for any untoward events caused by nature, man or machine, risk disaster management awareness is one of its advocacies. It believes in the importance of preserving life and properties

protecting them from hazards mentioned above. It also believes that the awareness program should be relayed to its members who come to visit the office for one reason or another. Likewise, it encourages it employees and members to disseminate the information contained in this manual/primer to their families and neighbours. Manila Teachers subscribe to the dictum: ***THE LIFE SAVE MAYBE YOUR OWN.***

In connection with fire and earthquake drills, these are held every six (6) months, some announced and other unannounced.

This resource manual puts into executable procedures the policy statement. It provides information and competence on disaster management. It outlines the program and spells out the role of every employee of the Association. It illustrates the procedures that maybe employed during and after the occurrence of a disaster. It offers safeguarding mechanisms to protect and preserve properties, facilities, equipment, fixtures and records. On the other hand, alternative delivery of service is predetermined to ensure continuity of service. This is to carry out the duties and responsibilities of every employee to deliver the necessary services even in time of emergencies and calamities. Sustainability of the service program is always an issue, so, provision of the monitoring and evaluation procedures ensures the continuity and effectiveness of the Disaster Risk Management Program.

To realize the goal of this resource manual, which is to protect the lives and properties, facilities, records, every employee should:

- Analyze the condition of his/her area
- Identify possible hazards/threats
- Follow strictly the disaster management strategies especially in time of calamity/disaster
- Provide feedback to management for policy formulation

In order to effectively achieve the expected response in times of adversity, it is likewise suggested the Association officials and personnel take time to understand, practice and internalize the risk reduction measures to eventually make a habit of being prepared before, during and after a calamity, be it a natural or human-made/induced hazard.

RISK MANAGEMENT COMMITTEE

MISSION

We, at the Manila Teachers' are committed to be a performance-driven and customer focused financial institution by providing divers and high quality financial products and services.

VISION

Our Vision at the Manila Teachers' is to be one of the leading providers of a high quality and diverse range of financial products and services through efficiency and innovativeness.

CORPORATE CORE VALUES

Integrity	We adhere to the principles of honesty, loyalty, trust and ethical practices.
Quality Service	We are committed to excellence in service.
Teamwork	We believe in collective effort in attaining goals.
Innovativeness	We encourage creativity in doing our work.
Professionalism	We uphold the highest standard of professional behaviour.

OBJECTIVES

- To encourage thrift and savings among members
- To encourage members to pool their resources into a common fund and
- To provide housing loans

GOALS

- To expand area of coverage nationwide
- To increase membership by 100%
- To increase resources to P2 billion pesos

RATIONALE

The **Manila Teachers Mutual Aid System, Inc.** Is a mutual benefit association supervised by the Insurance Commission and registered with the Securities and Exchange Commission.

As a mutual benefit association, its priority is **service** not profit. It values people as human beings who must be treated as one wants himself/herself be treated. People who come to transact business with the association are always served with a smile.

It values people and one manifestation of such concern is giving priority to risk disaster reduction management to guide its officers, managers, heads of services and employees on what to do before, during and after the occurrence of any hazard to prevent its disastrous impact and damages.

I. STATEMENT OF POLICY:

The Association, equipped with its more than 40 years of experience, managed to attain its present stable financial conditions without discounting the inherent risks in its operations. Therefore, in its quest to sustain the future profitability and stability in the use of its resources, it shall continue with the policy of adopting this Risk Management Plan to minimize if not eliminate, and/or mitigate if not prevent, the impact of all identified risks and the risk that may identified as it faces the future.

II. DEFINITION:

A Risk is an event or condition that, if occurs, could have a positive or negative effect on the Association's objectives. Risk Management is the process of identifying, assessing to, monitoring and controlling, and reporting risks.

This Risk Management Plan defines how risks related with our Association will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the Association's operations and provides standards on the practices for recording and prioritizing risks by the Top Management.

III. RISK CATEGORIES:

The Association based on its history has categorized the potential risk that it may be exposed to in the order of its importance, *i.e.* inherent nature to our business operations as define by historical experience, probability and impact, urgency, etc. And these are as follows:

- **Credit Risk** – it encompasses policies and procedure in the Loan Grant which is the major product and services of the Association, or source of business income of the Association incidental to its services to its members.
- **Operational Risk** – relates to policies and procedures business processes, safeguards for an efficient discharge of functions, safe keep of resources both human and material, business continuity and recovery, disruption in the delivery of committed services, competitiveness and social dimension of the Association.
- **Capital Risk** – relates to policies and procedures to prevent capital flight by stakeholders, major loss or damage of capital assets, catastrophic events, and adverse changes in governing laws and significant loss in market share of the Association.

IV. METHODOLOGY

The following methods will be used to assist in the identification of detailed risks associated with the foregoing major categories:

- Brainstorming
- SWOT Analysis (Strengths, Weaknesses, Opportunities and Threats)
- Etc.

- **RISK STRATEGY**

Once a risk has been identified, then there are several strategy options that management can take. Experts in this field have identified and published strategies to deal with negative risks and to deal with opportunities and one that will work with either type. **These are discussed as follows:**

- **(+)(-) Acceptance** – management has either decided not to alter the policy to avoid the risk, or there are no alternatives to dealing with the risks.

- **(-) Avoid** – changing the policy or plan so that the risk can be avoided. Risks identified early on will more likely be able to use this strategy. As the operation continues, the cost and time needed to avoid a risk will grow.

- **(-) Mitigate** – taking additional actions to lessen the impact that a risk may have on the operation. One example is to include an additional Questions and Answers testing round before the general release of a policy. By instituting this round of testing, the chances that more issues are captured prior to implementation will reduce the risk of releasing a decision that is faulty.

- **(-) Transfer –** ability to move the risk to a third party that will own the risk and the response. This is most often done by carrying insurance or by contracting. This does not eliminate the risk but it simply moves it to a third party. Usually, transference increases the operating cost as the third party request a premium to carry the liability.

- **(+) Exploit –** some people may see exploitation as a bad word. In this context it is simply taking full advantage of a possible opportunity for a situation on hand. While risk is uncertain, this strategy is used to make the likelihood of the risk increase so that the management can capitalize on the results.

- **(+) Share –** this is like the transference strategy. This can be done by sharing the positive opportunities of a project with a third party. Example would be to form a joint venture so that the full potential of opportunity is developed.

- **(+) Enhanced –** increases the impact of an opportunity as well as the likelihood that the opportunity will happen. This will require altering the plan to make sure that the opportunity discussed is a reality and increases the benefits of the full project.

- **RISK ANALYSIS**

Risk Analysis is an essential managerial perception that is needed to identify existing and potential threats, vulnerabilities, and other workplace hazards that can compromise the performance of the association set-up and overall performance.

There are **two fundamental types** of risk analysis: quantitative and qualitative. Each method has pros and cons, and there is significant controversy over which approach is superior.

a. **Quantitative Risk Analysis**

This is a process to analyze numerically the probability of each risk and its consequence on project objectives and then documented for reporting to the President and CEO.

b. Qualitative Risk Analysis

Process of assessing the impact and likelihood of identified risks and prioritizes risk according to their potential effect on project objectives. Requires that the probability and consequences of the risks be evaluated using established qualitative-analysis methods and tools. The probability and impact of occurrence for each identified risk will be assessed by the Management Committee, with input from the Risk Management Project Team.

SUMMARY	
QUALITATIVE	**QUANTITATIVE**
risk-level	product/project-level
subjective evaluation of probability and impact	probabilistic estimates of time and cost
quick and easy to perform	time consuming
no special software or tools required	may require specialized tools

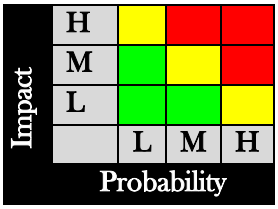
Risks identified will be assessed to identify the range of possible outcomes as to **probability** and **impact**. Risks will be prioritized by their level of importance, i.e., high to medium probability and impact.

a. Probability

- High – Greater than *<70%>* probability of occurrence
- Medium – Between *<30%>* and *<70%>* probability of occurrence
- Low – Below *<30%>* probability of occurrence

b. Impact

- High – Risk that has the potential to greatly impact operational cost, schedule or performance
- Medium – Risk that has the potential to slightly impact operational cost, schedule or performance
- Low – Risk that has relatively little impact on operational cost, schedule or performance



Risks that fall within the RED and YELLOW zones will have risk response plan which may include both a risk response strategy (see page 11) and a risk contingency plan (see page 14).

○ RISK RESPONSE PLANNING

Process of developing options and determining actions to enhance opportunities and reduce threats to project's objectives. Ensures that identified risks are properly addressed and effectiveness of responses planning will directly determine whether risk increases or decreases for the project.

Each major risk (*those falling in the Red & Yellow zones*) will be assigned for proper monitoring and controlling purposes to ensure that the risk will not "fall through the cracks".

Tools and Techniques for Risk Response Planning:

The strategy that is most likely to be effective should be selected for each risk. Then, specific actions should be developed to implement that strategy. Primary and backup strategies may be selected.

For each major risk, one of the following approaches from those as mentioned earlier will be selected to address it:

- **Avoidance -** Eliminate the threat or condition or to protect the project objectives from its impact.
- **Mitigation -** Seeks to reduce the probability and/or consequences of an adverse risk event to an acceptable threshold.
- **Acceptance -** Not to change the project plan to deal with a risk or is unable to identify any other suitable response strategy.
- **Contingency Plan -** Applied to identify risks that arise during the project.
- **Transference -** Shift the consequence of a risk to a third party together with ownership of the response by making another party responsible for the risk (rediscounting, receivable factoring, buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include adding resources, etc. Any secondary risks that result from risk mitigation response will be documented and follow the risk management protocol as the primary risks.

For each major risk that is to be mitigated or that is accepted, a course of action will be outlined in the event that the risk does materialize in order to minimize its impact.

- **RISK MONITORING, CONTROLLING, AND REPORTING**

Process of keeping track of the identified risks, monitoring residual risks and identifying new risks, ensuring the execution of risk plans, and evaluating their effectiveness in reducing risk.

A **"Top 10 Risk List"** (see page 16-17 of Identified Risks) will be maintained and will be reported as a component of the reporting process to the Board of Directors.

As Risk Events occur, the list will be re-prioritized during monthly reviews and risk management plan will reflect any and all changes to the risk lists including secondary and residual risks.

Management will be notified of significant and important changes to risk status as a component to the Monthly Manager's Report

The Branch Offices, or Extension Offices, and all other Departments in their areas of concern will:

- Help develop the risk response and risk trigger and carry out the execution of the risk response, if a risk event occurs.
- Participate in the review, re-evaluation, and modification of the probability and impact for each risk item on a monthly basis.
- Identify and participate in the analysis of any new risks that occur.
- Escalate issues/problems to Risk Management Project Team that,
  - Significantly impact the triple constraint or trigger another risk event to occur.

- Require action prior to the next monthly review
- Risk strategy is not effective or productive causing the need to execute the contingency plan.

○ RISK CONTINGENCY PLAN AND FUND

Project risk plan balances the investment of the mitigation against the benefit for the project. The Project Team often develops an alternative method for accomplishing a project goal when a risk event has been identified that may frustrate the accomplishment of that goal.

A **risk contingency budget** will be established to prepare in advance for the possibility that some risks will not be identified and managed successfully. The risk contingency budget will contain funds that can be tapped in the event of its realization and will be named Contingency Fund which is appropriated as a provision out of undistributed earnings.

Aside from the supplemental budget, a yearly budget shall be allocated for Risk Management activities that are related to, identifying, analyzing, tracking, controlling, managing, and planning for risks; it may also include creating and updating the risk response strategies and contingency plans discussed in this manual.

V. BASIC PREMISES

A. IDENTIFIED RISKS

Among others, the following significant risks per department of the Association with rated probability and impact have been identified on the basis of the experience during the preceding 55 years of its existence that needs management focus and attention.

OPERATIONS DEPARTMENT	PROBABILITY	IMPACT
1. Withdrawal of Capital	Medium	High
2. Interest Rates	Low	Low
3. Market Saturation	High	Low
4. Decrease in Membership	High	Medium
5. Customer satisfaction	Low	Low
6. Unsecured Consumption Loans	High	High
7. Information Technology Risk	Medium	High
8. Liquidity Risk		
-failure of collection	Medium	High
-revocation of APDS Deduction code	Low	High
-Change in order of priority in APDS	Low	High
-Queuing system	Low	High
-Insufficient Net Pay by borrower	Low	High
-Death of borrower and co-maker	Medium	Medium

IT DEPARTMENT	PROBABILITY	IMPACT
1. Network Cable Failure	High	High
2. Obsolescence of Software	High	High
3. Router Failure	High	High
4. Hacking	Medium	High

5. Network Switch Failure	Medium	High
6. Server Failure	Medium	High
7. Earthquake	Low	High
8. Fire on premises	Low	High
9. Flood/storm surge	High	Low
10. Lightning strike	Medium	Medium
11. Terrorism attack	Low	High
12. Tsunami	Low	High
13. Typhoon	High	Low
14. Volcanic eruption	Low	Low
15. Employee turnover	Medium	Medium
16. PC Failure	Medium	Medium
17. Poor perimeter	Medium	Medium
18. Power failure	Low	High
19. Telco Carrier failure	Low	High
20. Riots, protest	Low	Low
21. IT User error	Low	Medium
22. Non-IT User error	Low	Medium
23. Sabotage	Low	Medium
24. Strike	Low	Low
25. CO trunk line	Low	Low
26. Defective software	Low	High
27. Firewall failure	Low	Medium
28. Logistics failure	Low	Low
29. Loss of software	Low	Low
30. PBX failure	Low	Low
31. Software development	Low	Low
32. Tape back-up software failure	Low	Low
33. Virus	Low	Medium

ACCOUNTING DEPARTMENT	PROBABILITY	IMPACT
1. Unrealistic accounting estimates	Low	High
2. Bad debts	Low	High
3. Physical Security- Fire	Low	High
4. Undelivered Bank Statements	Low	Medium
5. Accessibility of all Accounting Documents	High	High
6. Staff retirement/resignation	Medium	Medium
7. Computer breakdown	Medium	Medium
8. Accounting system and application	High	High

FINANCE DEPARTMENT	PROBABILITY	IMPACT
1. Bank runs of Depository	Low	High
2. Theft and robbery	Low	Medium
3. Over exposure of credit risk	High	High
4. Lost files	Low	Low
5. Malversation of funds	Low	Medium

AUDIT DEPARTMENT	PROBABILITY	IMPACT
1. Failure to identify the complete audit universe	Low	High
2. Failure to perform risk assessment	Low	High
3. Failure to make an annual audit plan	Low	High
4. Limited resources of information	Medium	Medium

5. Lack of cooperation from auditees	Low	Low
6. Recommend change that addresses only the symptoms of a problem	Low	High
7. Inability to effect change	Medium	High
8. Untimely report	Medium	Low
9. Failure to obtain full value from audit staff	Medium	Medium
10. Turn-over rate of auditors	Low	Low

ADMIN DEPARTMENT	PROBABILITY	IMPACT
1. Earthquake	Low	High
2. Fire	Medium	Low
3. Investment	Low	Medium
4. Inventories	Medium	Medium
5. Secured Loan	High	Medium
6. Expansion	Medium	Medium
7. Collection	Medium	High
8. Projects	Low	Low
9. Capital	Medium	High
10. Budget	Low	Low
11. Loan Amount	High	High
12. Property Maintenance	Medium	Medium

- **Write Off**

A write off is a reduction in the recorded amount of an asset, occurs upon the realization that an asset no longer can be converted into cash. In general, write off is accomplished by shifting some or all of the balance in an asset account to an expense account. And when an account receivable cannot be collected, it is usually offset against the allowance for doubtful accounts.

For classified loans falling under Loss where a 100% provision of specific allowance for probable losses have already been booked, this are to be recommended automatically for write off if the main cause of the non-payment of the account is the death of the member-borrower. For reasons other than death, every June and December of each year, the Accounting Department shall provide the Operations Department on the amount of savings deposits from concerned co-makers of doubtful accounts for application to said account.

- **Interest Rate and Computation**

The President and CEO as authorized by the Board of Directors shall have the discretion to fix the rate of interest for the loan products of the Association. In order to maintain its competitiveness in the light of the restrictions on interest rate as a pre-condition of the Department of Education accreditation and Memorandum Agreement, the *President and CEO is empowered to determine the strategic procedures in the methods of charging interest and service fees, from discounted to add-on or simple straight line to effective interest rate, as the prevailing conditions of the time will allow.* This is to ensure flexibility and immediate response to the demands of market and competition.

❖ OPERATIONAL RISK

Operational Risk is defined broadly and as a fundamental risk – the risk of loss due to failures in people, processes, systems or external events. A constant cyclic process which includes risk assessment, risk decision making, and implementation of risk controls, which results in acceptance, mitigation, or avoidance of risk. Some operational risk categories are:

1. Computer Breakdown
2. Retirement and Resignation
3. Accounting system and application
4. Inability to effect change
5. Limited resources of information
6. Access to all accounting documents

The risks identified with the operations on account of probability and impact focused mainly on computer hardware, programs and human resources. The IT Department has designed a business continuity program to ensure that disruption in operations will be minimal and early return to normal operations is achieved at the least possible downtime. They are responsible for keeping the integrity of back up data and information on a regular daily and weekly basis. Sufficient back up equipments are maintained in the off site in Kamias, Quezon City.

Inadequate number of well capable technical staff is pooled in the Head Office who is well trained to restoring and restarting of business processes as soon as the need arises. Competitive employee benefits shall be provided to secure loyalty of existing employees and avoid brain drain in its work force. External and Internal training on latest developments and technologies shall be provided on a program of Continuing Education among the IT people to enhance their proficiency and expertise. The Compliance Officer is given added authority to effect change by way of providing easy access to information within the organization. This will facilitate the timely compliance with all the mandates required by the authority.

The criterion and specific guidelines governing the Operational Risk shall be addressed in the *Business Recovery and Continuity Plan* which is presented in a separate policy guideline. The *Emergency Preparedness plan* will likewise address risks associated with natural calamities such as earthquake, typhoon and flood; risks that at present generation are very real and proven by our recent firsthand experience here in Metro Manila, all scientifically attributed to the global climate change. For Risk attributed to Retirement and Resignation, the *HR Risk Management Plan* as discussed in the later section of this manual will be the reference guide.

➢ Risk Assets

Real and other properties acquired, receivables and investments shall be subject to impairment provisions as required by the applicable rules and regulations of the Insurance Code. The idea is to have a time related valuation of assets formerly held in the books at cost in order to present a more realistic and fair presentation of financial statements. If the amount of this assets exceeds P 5M in book value, it shall be appraised by duly accredited external appraisers, otherwise, an in-house appraisal shall be made every other year; except when there is a material decline in value of the assets when an Immediate re-appraisal shall be conducted. These assets shall be classified as SUBSTANDARD because of their nature as non liquid and non-productive. The corresponding amount of 25% of its cost shall be set up as a

provision for probable losses and form part of the Allowance for probable losses which the Accounting Department shall look into every year to guarantee its inclusion in the amount of provisions.

- **Insurance Coverage**

The Association shall ensure that all insurable assets are covered by insurance from reputable Insurance Company, such that in any adverse eventuality the losses that may be incurred are reduced if not totally recoverable. All Transportation Equipment that are not yet fully depreciated shall be covered by Comprehensive Insurance against loss due to theft, acts of nature, accident and the like. Office buildings shall be insured against the risk of fire, earthquake, typhoon and flood. Employees handling monetary accountabilities shall be bonded from reputable bonding company. Adequate group insurance for all regular employees shall be provided in accordance with existing approved fringe benefits for Officers and Staff of the Association.

The Administrative Division is hereby designated to determine the adequacy of insurance coverage of all risk assets of the Association and to secure sufficient protection from perils that may cause unnecessary loss due to unforeseen eventuality. They shall be responsible for the timely inception of insurance policies and its renewal on a year-to-year basis. The idea is to transfer the impact of the potential risk on losses of vital resources arising from either natural calamities or manmade destructions.

❖ CAPITAL RISK

The risk of the association faces that may lose all or part of the principal amount, like; Withdrawal of Capital

The Association shall at all times concentrate with its main purpose of fostering brotherhood and mutual help and benefit among its members and to encourage the habit of thrift and savings among its members thru accumulation of savings for the duration of their membership with the Association, and to provide financial assistance to to the beneficiary/ies of deceased members.

In order to maintain the integrity of the financial statements of the Association, it shall adhere to the precepts and principles as required by the Philippine Accounting Standards on Financial Reporting. An independent External Auditor shall be appointed from the list of duly accredited firm of Certified Public Accountants.

- **Risk Management Project Team**

The Risk Management Project Team is tasked to oversee and implement this risk management plan through its regular monthly meeting or a special meeting that may be called to address pressing concerns. It shall report directly to the President who in turn will report the progress of the plan to the Committee appointed by the Board of Directors.

B. CONTINUING DEVELOPMENT

The plan will be updated from time to time as experience dictates, development arises and need occurs.

EFFECTIVITY

This policy shall take effect immediately upon approval of the Board of Directors.

BY AUTHORITY OF THE BOARD OF DIRECTORS

(SGD.) VIRGILIO S. LACSON
President and CEO

BUSINESS DEVELOPMENT PLAN

I. STATEMENT OF POLICY:

In line with our Mission Statement of a "performance driven and customer focused" financial institution, it shall be the policy of the Association to provide first and foremost quality service to its members long before and above the profitability of each transaction. However, it should only be to the extent that the stability of its financial condition is not sacrificed, and the required liquidity and solvency of its operations are maintained. It must therefore be cleared to all that the complete satisfaction of the members or excellent customer experience shall play the most vital role in our operation.

II. OBJECTIVES:

The business operations of the Association should therefore be aligned to the attainment of the following objectives:

a. Members Satisfaction

While maintaining market dominance, retention of loyal members and recruitment of new ones should focus on the careful management of suggestions and feedbacks for a timely and effective corrective measures and policies.

b. Management Integrity

Adherence to acceptable practices in corporate governance, strengthen risk management, continually improve product quality and efficient service delivery.

c. Financial Growth

Operating under the principle of Management by Objective, pursuit of new business opportunities, leverage with the market conditions, improve margin, reduction in the operating cost and enhance efficiency.

d. Organizational Development

Improve employee morale, loyalty, prestige and social stature, increase competence and develop career path, promote wellness and safety to increase productivity, enhance internal business processes and comply with regulatory and statutory requirements.

III. LIMITATIONS:

As a duly licensed mutual benefit association, membership is confined to Public School Teachers and employees of the Department of Education on regular/permanent status nationwide, and, including, officers and employees of the Association. Having defined the quantitative limit of its growth to the given number of employees of the government agency, DepEd, management must live to the fact that the growth in the target market is dictated by the development in the national government, vis-à-vis the budget allocated for the manpower recruitment of the said agency. The objective therefore, should logically follow as only to saturate the potential number of membership from the given numbers of appointments as approved in the national budget which are made on a fiscal year to year basis.

The goal is to get the 100% membership of the niche, all of the regular/permanent employees in the plantilla of the civil service personnel for DepEd. But consideration must be given to the complexities of some of the autonomous region and therefore, under the present context must be set aside in this business development plan. The second limitation is to the potential income from the operations as the main product of the association is loans to its members. Department of Education who is tasked and required under the MOA to deduct for and in behalf of the association has instituted an Accreditation Process for its Automatic Payroll Deduction System (APDS).

IV. MARKETING STRATEGY:

The high levels of domestic liquidity coupled with an accommodative administration in the DepEd provided an environment of competition with mix challenges and opportunities. As deduction codes are provided to more accredited institutions, the market is flooded with more alternatives for our members to choose from. Growth in lending opportunities set the stage for heightened competition of the market share among the industry players, lowering the spreads for lending with borrowers demand for longer term loans.

Sustainability of the operations require for the introduction of more attractive packages and seemingly beneficial features. Speed, accessibility and convenience in the transaction are paramount to entice our members to continue with us and not be lured by our competitors. Liberality for larger amount of loans granted shall be allowed as long as the parameters set forth in our lending policies are present. Likewise, request for longer repayment terms where circumstances may allow shall be given due consideration and approval at the discretion of the approving authority. The rule of the game shall be not to allow our members to get out from our Association in favor of the other lending institutions or competitors. Focused market research, develop an actionable segmentation of the Association financing market to more effectively target, understand and serve members with a smile.

V. STRATEGIC PLAN:

The past 40 years of the Association has given rise to its present financial stability and modest growth of loyal membership. We have the rich experience and knowledge of our customer's character and behavior in conceptualizing the strategic plan for the future growth of our organization.

A. The next five years shall focus on the following offices in cities and towns previously registered with the Insurance Commission as follows:

Region I	Urdaneta City, Alaminos, Candon, Ilocos Sur
Region II	Ilagan City, Isabela
Region III	San Fernando, Pampanga; Bataan; Tarlac
Region IV-A	Lucena City; Gumaca, Batangas City, Batangas, Sta. Cruz, Laguna; Cavite;

Region IV-B	Palawan; Marinduque
Region V	Naga City, Camarines Sur
CAR	Baguio City;
NCR	Pasig;

B. On top of the following, registration with Insurance Commission for newly open branch offices/satellite offices shall commence for the following:

Pagadian Lodge
Dipolog Satellite Office
Ipil Office
Cagayan De Oro Lodge
Malaybalay Satellite Office
Mambajao Satellite Office
Iligan City Satellite Office
Ozamiz City Satellite Office
Tagum Lodge
Davao Satellite Office
Nabunturan Satellite Office
Malita Satellite Office
Mati Satellite Office
Tacurong Lodge
Koronadal City Satellite Office
Kidapawan Satellite Office
Alabel, Saranggani Satellite Office
Butuan Lodge
San Franciso Satellite Office
Surigao City Satellite Office
Tandag City Satellite Office
Dinagat Satellite Office

C. In an effort to increase further the revenue, it has been identified that to date, at least 10,000 of the total active membership are merely putting up their savings with the Association and are not availing of our credit facilities. The situation is more of a cost concern as we regularly pay interest. It is therefore imperative to encourage the potential borrowings by these members in order to supplement our income. As these members have already accumulated a substantial amount of savings, it is more likely that everyone is qualified to at least P 100,000.00 amount of loan which can be translated to a total of P 1Billion additional loan amount to be granted per year. Double it if our effort will succeed to convince them to renew at least after 6 months. Therefore, marketing activities will be mobilized and focused to this segment. Branch managers will be pushed to take an aggressive stance in the next five years.

Re-introduction of our loan products, re orientation on the benefits of the members of our Association, lectures, discussion with members, visiting schools, attending teachers meetings and listening to their concerns and suggestions, and coming up with concrete but practical suggestions will be the order for each and everyone.

D. The last five (5) years of the Association showed an increase in the liquidity with an indication of low productivity turn out in terms of capital invested. To further improve the utilization of excess funds, it is deemed wise to explore the purchase of government securities and bonds with a good yield than our present time deposits in our various depository banks. The right mix in the investment of funds from time deposits to government securities shall be pursued with a 40/60 ratio of government bonds/securities vis-à-vis time deposits/special savings deposits.

E. The main reason for most of the members who were lured by the competitor thru their buy out scheme is the maximum amount of loan we are normally approving them which has been at P 150,000.00 with a term of one year in recent years. As a counter measure to this, the Board of Directors approved the increase in the loan limit and management has set the parameters in granting a maximum amount of loan of

P 300,000.00 with likewise extended terms of payments of three (3) years. This will put at par with the rest of the offers being made in the industry thru the Automatic Payroll Deduction Scheme (APDS) of DepEd.

VI. MANAGEMENT COMMITTEE:

The Management Committee is tasked to oversee and implement this business development plan through its regular monthly meeting or a special meeting that may be called to address pressing concerns. It shall report directly to the President who in turn will report the progress of the plan to the Board of Directors.

VII. CONTINUING DEVELOPMENT:

The plan will be updated from time to time as experience dictates, development arises and need occurs.

EFFECTIVITY

This policy shall take effect immediately upon approval of the Board of Directors.

BY AUTHORITY OF THE BOARD OF DIRECTORS

(SGD.) VIRGILIO S. LACSON
President and CEO

BUSINESS RECOVERY AND CONTINUITY PLAN

I. STATEMENT OF POLICY

Management is cognizant of perils consequent to disasters or calamities, whether natural or manmade, catastrophic events, criminal acts and even acts of terrorism, intentional or un-intentional, that will hinder totally if not disrupt fully the operations of each unit/department of operations of the Association and therefore fail, in the delivery of the services we have committed to our members. It shall be the policy of the Association to formulate plans and procedures to immediately restore the disrupted processes and procedures at the most minimal time lost from the time of its occurrence and at the least possible costs to continue its business.

Business Continuity Planning - prepare for and aid in disaster recovery. It is an arrangement agreed upon in advance by management and key personnel of the steps that will be taken to help the office recover should any type of disaster occur. Detailed plans are created that clearly outline the actions that an organization or particular members of an organization will take to help recover/restore any of its critical operations that may have been either completely or partially interrupted during or after (occurring within a specified period of time) a disaster or other extended disruption in accessibility to operational functions. In order to be fully effective at disaster recovery, these plans are recommended to be regularly practiced as well as outlined.

Business Continuity Plan - guards against future disasters that could endanger its long-term health or the accomplishment of its primary mission. BCPs take into account disasters that can occur on **multiple geographic levels-local, regional**, and **national-disasters like fires, earthquakes, or pandemic illness**. BCPs should be live and evolving strategies that are adjusted for any potential disasters that would require recovery; it should include everything from technological viruses to terrorist attacks. The ultimate goal is to help expedite the recovery of the Association's critical functions and manpower following these types of disasters. This sort of advanced planning can help the Association minimize the amount of loss and downtime it will sustain while simultaneously creating its best and fastest chance to recover after a disaster.

II. DISRUPTION RISK MANAGEMENT PERSPECTIVE

1. **Business Resumption Plan -** To continue critical functions at the site of affected areas through work-around until the applications is restored.

2. **Business Recovery Plan -** To recover critical business processes at an alternate site and continue operations until the situation returns to normal.

3. **Contingency Plan -** To manage an external event that has far reaching impact on the business and therefore formulate a disruption effect consequence and minimize the risk of loss in man hours, resources and profit.

III. POLICY OBJECTIVES

Disaster Recovery is the process an organization uses to recover access to their software, data, and/or hardware that are needed to resume the performance of normal, critical business functions after the event of either a natural disaster or a disaster caused by humans. Disaster Recovery plans, often focus on bridging the gap where data, software, or hardware have been damaged or lost, one cannot forget the vital element of manpower that composes much of any organization. A building fire might predominantly affect vital data storage; whereas an epidemic illness is more likely to have an effect on staffing. Both types of disaster need to be considered when creating a DR Plan. It should include in their DRPs contingencies for how they will cope with the sudden and/or unexpected loss of key personnel as well as how to recover their data.

Disaster Recovery Plans are generally part of a larger, more extensive practice known as Business Continuity Planning. DR plans should be well practiced so that the key players are familiar with the specific actions they will need to take should a disaster occur. DR plans must also be adaptable and routinely updated, e.g. if new people/personnel, a new branch office, or new hardware or software are added to an organization they should promptly be incorporated into the organization's disaster recovery plan.

1. To be able to restore and operate disrupted systems and procedures in the event of disaster or calamity within 2 hours to 24 hours from its first impact at the affected location.
2. To define the line of authority in the event a continuity and recovery plan is to be activated as necessitated by disruption caused by mentioned disaster or calamity.
3. To establish and designate core groups who will mobilize the plan.
4. To formulate a detailed plan of action for the immediate deployment of business continuity and recovery procedures until the conditions return to normal situation in the affected area.
5. To be always ready and on guard to respond immediately in case when business operations are affected severely by disaster or calamity.

IV. CLASSIFICATION OF PERIL, DISASTER AND BUSINESS DISRUPTION

1. Natural Calamity/ Disaster
   - Earthquake
   - Typhoon, Hurricane, Tornadoes
   - Flood
   - Fire
2. Hardware and Communications Failure
   - Power outage, Prolonged Brownouts, Blackout
   - Internal or External Sabotage
3. Failure of Supply Chain in the delivery of Funds
   - Depository banks sudden closure, bank holidays, bankruptcy, insolvency
   - Depository banks own system failure
4. Terrorism and Criminal Consequences
   -Bombings
   -Looting/Vandalism
   -Mob Lynch

As the Association attempt to return to business as usual in the aftermath of the foregoing disruptions, the following areas of concern requires a variety of solutions to mitigate the risks that might cause:

-Business Process Failure
-Asset Loss
-Damage to reputation
-Regulatory Liability
-Customer Service Failure

V. DISRUPTION COORDINATING CORE GROUP (DCCG)

The Disruption Coordinating Core Group (DCCG) is hereby created under the direct supervision of and reporting to the **head of the Risk Management Committee of the Association.** Said Committee shall be primarily responsible for the implementation of the Business Recovery and Continuity Plan of the Association. The Disruption Coordinating Core Group is only composed permanently by the section or department heads of the Operations, HRD, Accounting and the EDP/IT Departments. The **Operations Manager** shall be the head of the Core Group with the EDP/IT representative as his deputy. The rest of the aforementioned heads of the different departments shall compose the members of the group. As it is an extreme reality that those appointed members of the Core Group may be themselves affected by such disaster or calamity, causing them to fail to report in their role as the Core Group for the continuity and recovery plan, their assistants next in line shall fill in their place until and after they report for work. The HRD representative of the Core Group is tasked to account for its members who will be ready to discharge the implementation of the plan by immediately reporting to the Core Group head the readiness of the group to put the plan into actions.

Each member of the Core Group will be provided with available Cellular Phones from each service provider (PLDT, GLOBE, SMART, SUN, etc.) in order to explore all the possibilities to immediately communicate with them as the need arises. A separate **Hot Line numbers** will be dedicated for the exclusive use of the reporting unit to relay in case of adversities. These numbers will be posted at all operating business offices of the Association. Report of such disruption will have to be validated by the Head or the Deputy of the Core Group using all available means, i.e., news reports, e-mails, call back, contact to the next nearest office, etc. A validated report will immediately convene the DCCG with the aim of restoring business process at the earliest of 2 hours or the latest of 24 hours. If the present affected office with its present staff will be workable, the recovery and restoration will be done there, otherwise, a new site will be designated. The DCCG will then decide where the staff or required backup personnel, when necessary, will report to restore and continue the disrupted operations.

Until their successors are designated, the following shall be the permanent **Disruption Coordinating Core Group (DCCG):** In Case of Indispensability

Chairman	-	Alternate Chairman
Vice Chairman	-	Alternate Vice Chairman
Members	-	Alternate Members

In order to attain familiarity and proficiency in the written operating procedures, the DCCG will conduct simulation training, orientation and drill among all operating units of the Association to prepare them and be ready as the actual situation arises.

The *DCCG* shall initiate the organization of an EVACUATION BRIGADE TEAM (EBT) from the ranks of volunteer employees who will be called *Marshals* and who will act as the lead in an actual scenario. They will be in the frontline during expected emergency arising from the above mentioned perils and risks. The *EBT will be trained on various aspects of first aid, emergency response and risks evaluation.* A drill (i.e., fire drill, earthquake drill, typhoon or flood) shall be conducted at twice a year to familiarize each and everyone on the proper behaviour and action in case of such an emergency.

VI. BACK UP DATA CENTRE

The EDP/IT of the Association is tasked to maintain the Organizational Data Backup and applications in a remote or off site location away from the Head Office where the wide area connection of our operating systems are currently maintained. This will be in the **third (3rd) Floor of MTMAS Building in Kamias, Quezon City** and designated as the official Back-up Data Centre Site. A second off-site in MTSLA office at *Malabon City* will likewise be established as the Alternate Back-up Data Centre. A complete set of a backup server including all required paraphernalia shall be set up thereon, with full capability to immediately resume operations within 24 hours in case of disruption at the Head Office. It will be fully equipped and operationally ready data centre offering complete *office space, furniture, telephone jacks and basic things in the usual location of the Head Office*.

In such a scenario, the DCCG will direct all affected departments and employees to report in the Back-up Data Centre Site. The restoration of all data and applications will be initiated by them in accordance with the existing Backup Operating Procedures of the Association.

Testing and maintenance of all backup data and applications shall be done at least once every month to test the integrity and effectiveness of the operating procedures as set forth in the Manual. For quality assurance, the EDP/IT shall adopt a continuing study for IT systems in place and its support as well as other aspects of business operations including physical, environmental and personnel whose disruption would affect the operations.

VII. CONTINUING DEVELOPMENT

The plan will be updated from time to time as experience dictates, development arises and need occurs.

EFFECTIVITY

This policy shall take effect immediately upon approval of the Board of Directors.

BY AUTHORITY OF THE BOARD OF DIRECTORS

(SGD.) VIRGILIO S. LACSON
President and CEO

HR RISK MANAGEMENT PLAN

I. OBJECTIVES:

a. Ensure adequate human resources to meet the strategic goals and operational plans of the organization – the right people with the right skills at the right time.
b. Flexibility to manage change
c. Keep up with social, economic and technological trends that impact human resources

II. RISK IDENTIFIED

A. RESIGNATION AND RETIREMENT

Resignation is one of the many challenges an organization is facing, thinking about who will be the next in line after an employee leaves. This is one issue why an organization needs to be thinking and preparing for the succession planning. The most important reason of course is to have competent and qualified staff to carry out our missions, provide services and meet our organizational goals. We need to think about what would happen to those services or our ability to fulfil our mission if a key staff member leaves.

Another reason to focus on succession planning is the changing realities of the workplace. The impending retirement of some employee/s is expected to have a major impact on workforce capacity.

With careful planning and preparation, the organization can manage the changes that result from a generational transfer of leadership as well as the ongoing changes that occur regularly when key employees leave.

Effective succession planning supports organizational stability and sustainability by ensuring there is an established process to meet staffing requirements. **Department Heads** should have an alternative plan strategies and processes in place to ensure that these transitions occur smoothly, with little disruption to the organization.

Risk Assessment

Assessing current and future needs based on strategic plan, goals and objectives, or priority programs and projects

- Match these to the capabilities of the existing workforce

a. People at Risk

All Levels

b. Risk Analysis

Qualitative Risk Analysis
Probability: High
Impact : High

Likelihood and Consequence

- Financial Impact
- No potential employee emerging for succession
- Inadequate training and development resulting in an employee who is not prepared for promotion

Risk Management Control Measures

- Training and developing existing staff. Skills set needed to meet job expectations.
- Move people into different areas for experience and training before they are needed in critical positions.
- Ensure that there is more than one person identified as a potential successor to the person being replaced.
- Proper turnover of work
- Policy on Succession/Forecasting HR requirements
- External recruitment
- Improved management of contingent workers

Communication

- All Levels

Management Action

- Immediate

Monitoring

- Is your plan working?
- Have your risks changed?
- Are staff/members following the risk management plan?
- Do they need retraining on the plan?
- Any changes or updates required?
- Do we need to better communicate the plan?

As people leave and new people assume their responsibilities, the plan will have to be updated to identify the next person to be groomed for promotion.

B. COMPETITION IN HIRING AND RECRUITMENT

Leading companies invest in human capital before anything else. By strengthening the organization's recruitment process, we will be able to attract the talent needed to be competitive. As in business, the key to winning in recruitment is to be better than your rivals at every step of the process.

Like attracting customers, attracting top talent requires planning. In a competitive world where human capital comes at a premium, posting an ad to a job board is no longer enough. We need to start heightening awareness of our vacancies among top candidates.

Risk Assessment

- Recruitment efforts currently done – advertisements used; other tools
- Evaluating the recruitment process
- Competence of Staff

a. People at Risk
All levels
b. Risk Analysis
Qualitative Risk Analysis
Probability: High
Impact : High

Likelihood and Consequences

- Failure to meet targets. Stiff competition in the job market and lack of other avenues or sources of recruitment
- Financial cost. Advertisements of different forms entail cost
- Need for additional recruitment staff
- Hiring unsuitable or unsafe candidates

Risk Management Control Measures

- Fix the bottlenecks. Identify elements that are slowing down recruitment and decrease your time-to-hire. Evaluate tools used like communication, ads and others
- Strategic Planning. Identifying trends, opportunities and threats
- Adopting proactive strategies. Make the best estimate of the probability occurring. Develop a talent tool or pipeline
- Determine the best sources in the job market
- Initiate staffing guidelines, procedures and timelines and ensure compliance thereof

Communication

All Levels

Management Action

Immediate

Monitoring

- Conduct reviews and analyze results
- Regular audit cycle

C. TECHNOLOGY AND TRAINING

The onset of new computer applications poses fear or challenge to most employees. Learning these new techniques requires careful planning as to how these will be taught simply but comprehensive to all. The active participation of IT professionals will play a big role on the employees learning process as they are the experts on technology applications.

Training employees on these new computer applications will increase efficiency thus resulting to productivity beneficial to the organization. This motivates all employees to participate in and protect their organization. It helps generate a sense of belonging and ownership of the organization and at the same time creates an organization-wide attitude of responsibility and diligence towards information security.

In addition, training is an essential element of employee's education on the appropriate use, protection and security of information. It keeps employees and senior management fully updated and knowledgeable in information security, corporate governance, policies and procedures.

Risk Assessment

- Knowledge inventory
- Identifying the people who need the training

a. People at Risk

All Levels

b. Risk Analysis

Qualitative Risk Analysis
Probability: High
Impact : High

Likelihood and Consequences

- Venturing into the unknown. Ignorance or fear of new or changing technology either prevents employees from moving into new areas, or results in facilities when they attempt to.
- New challenges faced by employees; coping up
- Functionality and Performance of the Employee. Gauging the effectiveness of the staff on the new technology
- Productivity. Technology may affect the productivity or output of the staff
- Financial Impact. Cost of Technology and Training
- Frequency of Training. Length or duration of learning new computer applications

Risk Management Control Measures

- A call to action for technology professionals. IT leaders to step up and put themselves and their function at the centre of driving the business forward. Intensify efforts to conduct training.
- Policy. Personnel should learn and know how to use new systems and technologies
- Manage compliance activities. Ensure that all personnel comply with all activities related to technology.

Communication

All Levels

Management Action

Immediate

D. HR OUTSOURCING

- **Risk Management**

Human resources outsourcing firms help the organization minimize risk. Employment and labor laws change regularly, and it can be difficult for employers to remain up-to-date on regulations that affect the workplace. Outsourcing firms employ HR professionals whose purpose is to stay abreast on a variety of centralized and status employment laws. HR staff helps businesses comply with these laws to avoid costly lawsuits brought on by employees. HR also maintains and audit company policies and practices to ensure the organization and its employee's best interests remain protected.

- **Cost Saving**

Outsourcing helps reduce the cost of maintaining nonrevenue-generating back-office expenses. A fully functional human resources department requires additional office space and highly trained and experienced HR staff. More businesses find it more cost-effective to outsource HR functions rather than expand to a larger location to meet the space needs of another department. Furthermore, outsourcing costs are variable and can be reduced when business needs warrant.

- **Efficiency**

Maintaining an efficient and productive workplace is critical. Outsourcing HR functions create greater efficiency within human resources systems. Advanced human resources technology utilized by outsourcing providers help streamline important HR functions, such as payroll, benefit administration and compliance management. Outsourcing helps employers and managers spend less time doing paperwork and more time dedicated to improving the efficiency and effectiveness of the workforce.

- **Employed Development**

Outsourcing HR functions help businesses manage employee performance and development. Providers implement performance management plans to ensure employees comply with company policies and procedures and successfully meet business goals. Outsourcing firms periodically monitor employee performance and report findings to management. This reduces the workload of managers by minimizing the amount of administrative responsibilities they must focus on.

I. Introduction

Most business processes nowadays requires the use of information technology particularly in the automation or streamlining the process. The Association recognizes the use of information technology in the business process which yielded positive results. Unfortunately, such dependency in information technology also incurs risks, like not being able to process transactions in the absence of computers and other related equipments. Occurrence of any type of disruptions to normal operations entails costs to the Association and must be therefore addressed properly. It is only appropriate that risks pertaining to disruptions be mitigated in order to minimize its effect.

The Association hereby requires developing an IT Disaster Recovery Plan that addresses the threat in Information Technology. This document form part of the Association's Business Continuity and Recovery Plan (chapter III of this manual). This will also satisfy the Association's requirements and will serve as a guide by the Management and Staff in the recovery and restoration process of the Information Technology services.

II. Overview

The Information Technology Disaster Recovery Plan documentation contains the steps and procedures to be undertaken by the Association in the event of a disaster. This guide provides the strategies and techniques to undertake that are common to the following;

1. Client/Server Platform
2. Telecommunications Systems

III. DR Plan Approval

Manila Teachers' Savings and Loan Association, Inc. has been reviewed and approved by:

Position/Title	Name	Date

IV. Objectives

This document was developed in order to protect the interest of the management, staff and its members. This aims to achieve the following objectives;

1. To protect the Association computer resources.

2. To provide a plan that will guide all personnel involved on how to be able to respond in the event of a disaster.
3. To be able to restore the computer systems, including all the latest or up-to-date information, as quickly as possible.

VI. Policy Statement

The Association's Information Technology Disaster Recovery Plan must meet the Association's requirements to be able to continue its operations in the event of any disruption. The following must be properly defined and followed:

1. Assignment of personnel and their specific roles to facilitate fast recovery.
2. Resources required to be able to restore to normal operations.
3. Define the scope of coverage of the plan.
4. Training requirements for each personnel involved or included in the recovery process.
5. Simulation of recovery plan.
6. Maintenance and fine tuning of recovery plan.
7. Backup and storage of backup media.

VI. Business Impact Analysis

To be able to properly define the list of priority of each Business Processes that are completely or highly dependent on computers, a business impact analysis for each system had been developed.

For each Business Process listed, components such as the following must be defined:

1. Business Process
2. Effect
3. Resources
4. Level of Criticality
5. Tolerable Downtime
6. Recovery Time Objective
7. Recovery Point Objective

Business Process	Effect	Resources	Level of Criticality	Tolerable Downtime	Recovery Time	Recovery Point
Loan Management System Loan Processing Deposit and Withdrawal	Operations - affects about 50,000 plus members of the Association	Database Server Workstations LAN Connection	High	30 Mins - 48 Hours	30 mins	10 mins
GL System	Accounting Department	Database Server Workstations LAN Connection GL System Application	medium	48 hours	24 hours	24 hours
Journal Voucher/Check Disbursement System	Accounting Department Finance Department	Database Server Workstations LAN Connection VP/CDV System Software SQL Server 2k/2012 Printer	High	30 mins – 48 hours	30 mins	30 mins
Timekeeping and Payroll System	HR - Payroll Employees	Database Server Workstations LAN Connection Timekeeping and Payroll System	High	48 hours	1 hour	24 hours

VII. Preventive Controls

In most cases wherein most of disruptions that occur or has high probability of occurring are often times easily recoverable or can be prevented from happening, in which case, it is more economical to put in place preventive controls or measures and maintaining it on a continuous basis in order to prevent the disaster from happening or minimize its effect. Below are the lists of preventive controls that had been identified:

1. Generators to provide long-term backup power supply
2. Uninterruptible Power Supply (UPS) to provide short-term backup power supply
3. Fire suppression
4. Air-conditioning System

5. Door Access Control
6. Scheduled backup maintenance
7. Off-site backup media
8. Redundant Local Area Network (LAN)
9. Redundant Wide Area Network (WAN)
10. Firewall Installation
11. Anti-Virus Software

VIII. Contingency Strategies

The Association requires fast recovery from any type of disruption; therefore strategies must be put in- place in order to minimize its effect.

Disruption varies as to the extent of its effect and therefore requires that for each type of disruption a specific action must be properly defined.

1. Backup and Recovery

Backup and Recovery strategies must be properly defined in order to be able to resume operation as quickly as possible. The strategies must meet the requirements of the Association and must be designed in accordance with the Business Impact Analysis (BIA).

Backup and Recovery strategies must be defined clearly for each type Business Processes. Procedures and steps to be undertaken must be properly documented. Personnel[s] in- charge to perform such tasks must be properly identified. Roles and responsibilities of the personnel[s] in-charge must be clearly stated.

Backup strategies must conform to the Backup and Retention Policy and the Backup Testing and Recovery Policy of the Association.

2. Off-Site Storage

Backup of critical information, particularly those business processes identified in the Business Impact Analysis (BIA), must have a copy and stored outside of the main facility wherein the business process is being performed/conducted.

Off-Site storage must also conform to the Backup and Retention Policy of the Association.

3. Alternate Site

In the event wherein a disaster prevents the use or utilization of the primary facility, an alternate site must be identified wherein the Association will transfer or shift its operation temporarily until such time that the main facility had been declared to be suitable for operation.

The alternate site, as agreed upon, will be a warm-site. Resources that must be present in the alternate site must be clearly identified and continuously maintained.

Location

The Association has identified that the Disaster and Recovery Site will be located at:

2nd Floor Lacson Commercial
Bldg. Kamias Road, Kamuning,
Quezon City.

List of Items Stored Offsite

It is very important for the following items to be present and ready at all times in order not slow down the recovery process.

1. A copy of the latest Disaster and Recovery Plan
2. A copy of the most recent data backup of the Association
3. A copy of all the installation software and licenses such as but not limited to the following;
    a. Operating System
        Installation disks
    b. Productivity application tools
    c. Anti-Virus installation disks
4. Office Supplies
5. Backup Servers
6. Backup Storage Device
7. Switches and Routers
8. Collapsible Tables and Chairs
9. Telephone or other forms of communication equipment
10. Uninterruptible Power Supply (UPS)
11. Generators

4. **Training**

Effectiveness of each personnel involved in the disaster recovery will require proper training. This will ensure that personnel are prepared, ready and capable of performing such task.

Training will also help personnel to familiarize with his/her role in the recovery process. This will ensure proper coordination with the rest of the team, particularly in the absence of the paper document during the first few hours of the recovery process, which is supposed to serve as their guide. Each member of the team must be familiar with the following and is therefore critical that proper training and exercise must be conducted:

1. Purpose of the Plan
2. Team and Cross Team Coordination
3. Reporting Procedures
4. Security Requirements

5. Team Specific Processes
6. Individual Responsibilities

5. Testing and Simulation

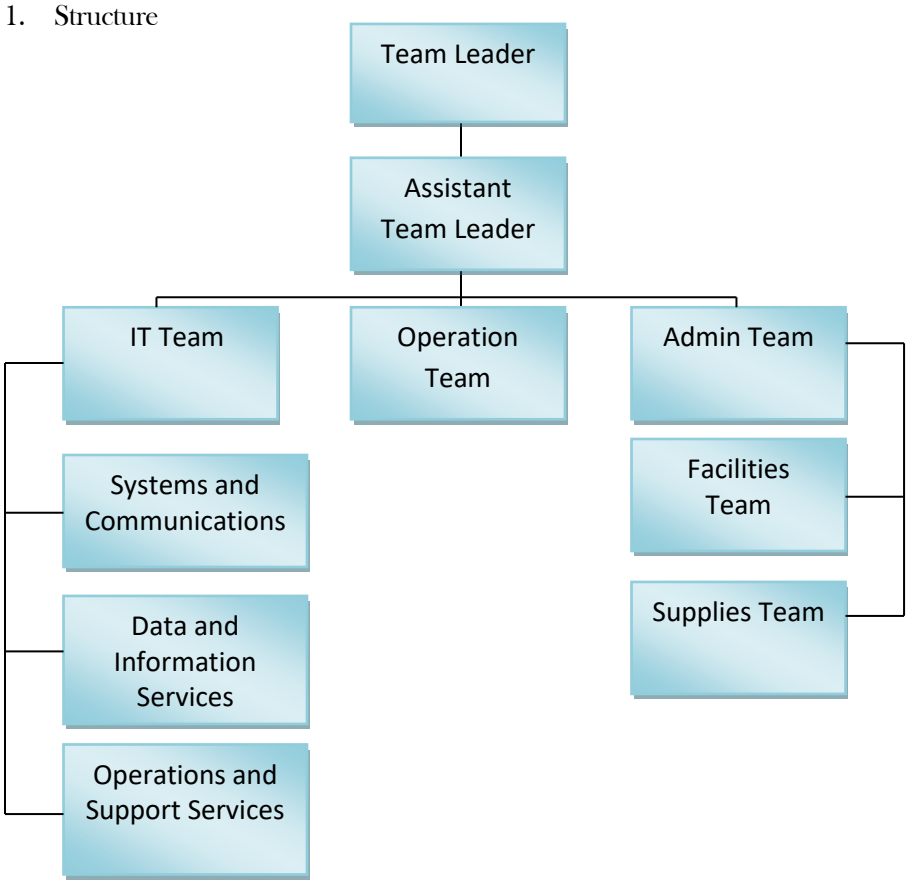
In order to validate the effectiveness of the IT Disaster Recovery Plan, testing and simulation must be conducted on a regular basis.

Such exercise will guarantee the effectiveness of the plan. Also, by performing the exercise, it will help in fine tuning the plan whenever necessary.

Testing and simulation must be done for each business process. Results of the testing and simulation must be documented and submitted to the Risk Management Committee for review

IX. IT Disaster Recovery Team

1. Structure



2. **Roles and Responsibilities**

i. **Team Leader**

a. Heads and supervises the IT Disaster Recovery Team in the event of the disaster
b. Declares a disaster and activates the IT Disaster Recovery Plan
c. Responsible in maintaining, testing and simulation of the Disaster Recovery Plan
d. Coordinates and Informs BCRP Coordinator of the occurrence of the disaster and its current status.
e. Declares that the crisis is over.

ii. **Assistant Team Leader**

1. Assists the Team Leader in the Disaster Recovery.
2. Acts as the Team Leader in the absence of the Team Leader.
3. Coordinates with the rest of the IT Disaster Recovery Team

iii. **Information and Technology Team**

1. **Systems and Communication Services**

a. Reports either to the Assistant Team Leader or Team Leader.
b. Keeps inform either the Assistant Team Leader or Team Leader of the current status.
c. Coordinates with the rest of the IT Disaster Recovery Team.
d. Assesses extent of damage to the voice and communication system and performs recovery strategy appropriate to the disaster.
e. Responsible in preparing/restoring voice and data communication either to the alternate site or at the primary site.
f. Makes necessary recommendations on how to improve recovery plan.

2. **Data and Information Services**

a. Reports either to the Assistant Team Leader or Team Leader.
b. Keeps inform either the Assistant Team Leader or Team Leader of the current status.
c. Coordinates with the rest of the IT Disaster Recovery Team.
d. Assesses extent of damage to the Data and Information and performs recovery strategy appropriate to the disaster.
e. Responsible in restoring data and information either to the alternate site or at the primary site.
f. Makes necessary recommendations on how to improve recovery plan.

3. **Operations and Support Services**
    a. Reports either to the Assistant Team Leader or Team Leader.
    b. Keeps inform either the Assistant Team Leader orTeam Leader of the current status.
    c. Coordinates with the rest of the IT Disaster Recovery Team.
    d. Assesses extent of damage to the Data and Information and performs recovery strategy appropriate to the disaster.
    e. Responsible in restoring data and information either to the alternate site or at the primary site.
    f. Makes necessary recommendations on how to improve recovery plan.

iv. **Operations Team**
1. Advises the affected area of operation regarding the incident.
2. Keeps the affected area informed regarding the incident.
3. Advises the affected area of what to do until such time that the operation goes back to normal.
4. advises the Team Leader or Assistant Team Leader when the systems are already operational.

v. **Facilities Team**
1. Secures and establishes the alternate site whenever the need arises for its use.
2. Coordinates with whole team if the facility, the primary or alternate site, is safe to use.

vi. **Supplies Team**
1. Coordinates with the whole team regarding the requirements needed for disaster recovery before, during and after the event.
2. Responsible for the purchases for the required items by the team.
3. Responsible for coordinating to suppliers/vendors for proper coordination and fast delivery of the needed items.

X. Disaster Declaration

1. Authorized Person to Declare a Disaster or Resume Normal Operations

Name	Title/Position

The following are authorized to declare an Information and Technology Disaster and signal the resumption to normal operations

2. Plan Activation

This plan will be activated in the event of a disaster whether man-made or natural that will cause disruption[s] on normal operations of the Association. Examples of such disaster but are not limited to the following are;

1. Fire
2. Flood
3. Tsunami
4. Typhoon
5. Earthquake
6. Volcanic Eruption
7. Bomb Threats
8. Terrorist Attacks
9. Civil Disorder/Strikes
10. Technology Disaster
    a. Server Breakdown
    b. Communication/Network Breakdown
    c. Virus Attack
    d. Hacking
    e. Power Disruption

3. Resumption to Normal Operations

After containing the threat or the cause of disruption, the recovery team will assess the situation and will announce whether or not the Association can return to its normal operations.

4. Disaster Recovery Key Activities

1. Activating the recovery plan
2. Notifying team leaders
3. Notifying key management contacts
4. Redirecting voice service to an alternate location
5. Securing a new location for the data center
6. Ordering and configuring replacement equipment
7. Network reconfiguration
8. Software and Data reinstallation
9. Keeping management informed
10. Keeping users informed
11. Keeping the members informed

Activities listed may or may not be all performed. Actions to be taken will be based on the kind of disaster the Association is experiencing, thus for each disaster a list of activities or actions to be taken must be defined.

XI. Contact List

Disaster Recovery Team

Designation	Name	Department and	Contact No.
Team Leader	Virgilio S. Lacson	President and CEO	
Asst. Team Leader	Edwin M. German	IT Manager	
IT Operations and Support Services	Kathleen Marco	IT Operations and Support Team Leader	
Data and InformationServices	Rennen G. Ramos	Senior Developer	
Systems andCommunication	Rico Del Rosario	Systems Administrator	
Purchasing/Supplies	Liza Marie Arellano	HR Coordinator	
Operations	Atty. Jonathan Cristobal	Operations Manager	
Building/Facilities	Reyman John Padirayon		

Suppliers and Service Providers

Company Name	Contact Person	Contact Details

I. INTRODUCTION

This manual provides a common starting point for understanding and discussing disasters, disaster management, and disaster preparedness as part of the Association's mission, and discusses the potential scope of disaster preparedness measure. It is appropriate for anyone who has general responsibilities for disaster management and programme implementation. Being prepared for emergencies means taking precautionary measures and knowing what to do if emergency/disaster occur.

- Disaster Plans

Any organization which takes its business seriously will analyze the risks facing it and have a prepared disaster plan. This is not the emergency procedures which an organization has to ensure the safety of the employee/personnel, but the plan which comes into effect once the safety of employee/personnel is guaranteed.

The general objectives of a disaster plan are;

- to anticipate key risk factors and reduce them where possible
- to ensure that staff are well trained (with regular updates) at detecting and responding to incidents and the disasters that they might escalate to and are efficient in the disaster recovery process
- to provide a structure which allows outside agencies (who are briefed to understand the collections special needs) to be called in where necessary
- flexibility, allowing constant revision and improvement, particularly in building on experience gained,
- To get the organization back on its feet and operating as quickly and as safely as possible.

The disaster plan should tie in closely with the procedures adopted by the institution's emergency control organization so that the safety of the disaster recovery team can be monitored. It's clear that within an organization, many of the same people who draft the emergency plan will be involved in the drafting of the disaster recovery plan.

A disaster plan should contain four key elements;

- prevention
- response preparedness
- reaction
- Recovery.

II. DEFINITION

The enactment of Republic Act 10121 otherwise known as the Philippine Disaster Risk Reduction and Management Act of 2010 has laid the basis for a paradigm shift from just disaster preparedness and response to disaster risk reduction and management (DRRM).The DRRM Plan serves as the national guide on how sustainable development can be achieved through inclusive growth while building the adaptive capacities of communities; increasing the resilience of vulnerable sectors; and optimizing disaster mitigation opportunities with the end in view of promoting people's welfare and security towards gender-responsive and rights-based sustainable development.

This is because the underlying causes of people's vulnerability have yet to be fully recognized and addressed. For years, DRR has focused more on efforts around disaster preparedness and response and not

so much in identifying the hazard-prone areas and other factors which contribute to people's exposure to disasters; incorporating risk analysis to development plans; building people's capacities towards sustainable livelihood options; and the like.

III. GUIDING PRINCIPLES IN DISASTER RISK REDUCTION MANAGEMENT

1. Disaster risk management must be a priority
   a. Plans, program and projects must be made
   b. Adequate resources should be allocated
   c. Officials, managers, heads of service and employees should know and feel its importance
2. Risks should be identified and actions about them should be taken
   d. Disaster risks should be identified, needs most
   e. Enhance early warning like;
      Data gathering, planning
      And implementing suggestions
3. A culture of safety and resilience should be created
   f. Training/seminars activities
   g. Relevant information provided
4. Everyone should be prepared and ready to act
   h. Strengthen disaster preparedness

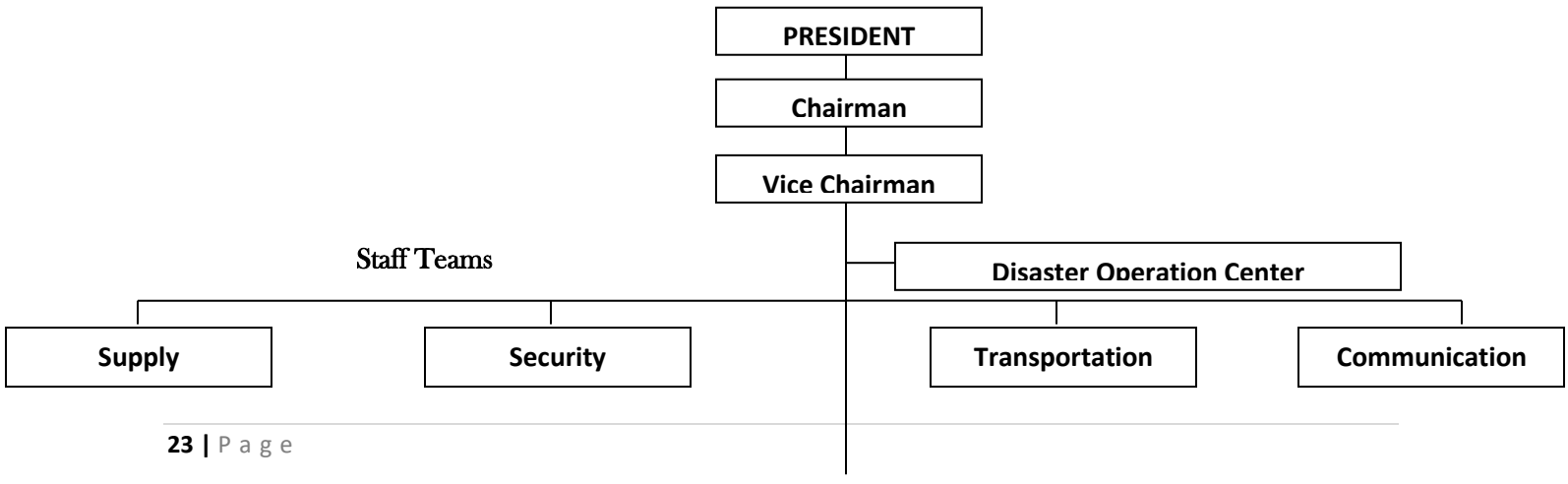
IV. ORGANIZATIONAL STRUCTURE

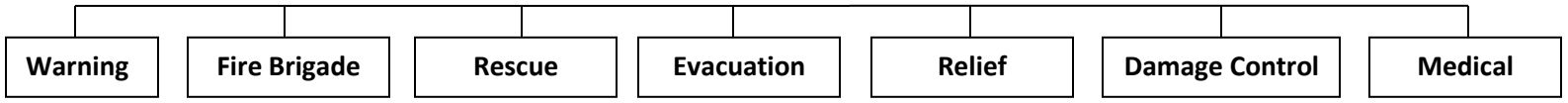
Natural and Human-Induced disasters are becoming more frequent and climate change has further added to the unpredictability of these occurrences as well as their impact on society. The Philippine Government, through the NDRRMC, is therefore faced with the challenge to heighten its vigilance in ensuring that disaster risks are prevented or minimized and it is prepared to address the needs of affected population/environment when disasters or emergencies occur.

Organizational Structure of DRRG, which serves as the principal guide to disaster risk reduction and management efforts to the Association. The Organizational Structure envisions of a safer, adaptive and disaster resilient Filipino communities toward sustainable development.

The basic concept underlying the organization is "protection". This is accomplished by organizing and training small groups of employees for the performance of special tasks. Organization is composes of employee/personnel chosen on a "best qualified" basis.

DISASTER RISK REDUCTION GROUP





V. DUTIES AND RESPONSIBILITIES OF OFFICE DISASTER MANAGEMENT COMMITTEE

1. Chairman

a. Developing the plan to protect life and property and to minimize damage in the event of an emergency or other disaster;
b. Coordinating such planning with the officials of the different branches;
c. Selecting, organizing and training an adequate staff to conduct the emergency operations required;
d. Directing and supervising the activities of the building occupants during an enforced stay, when necessary, in the shelter within the premises.
e. Establish a preparedness plan disseminating to all concern persons and agencies;
f. Assists in planning for and securing the installation and the necessary alarm system and in recruiting or selecting qualified emergency service personnel;
g. Establishes the ***Incident Command System*** as a control point from which activities may be directed in an emergency;
h. Maintains contact with and cooperates with local government units on problems arising in the selection and training of employees in the organization;
i. Insures the appropriate training course be set up and that arrangements are made for obtaining assistance from the National Disaster Coordinating Council (NDCC) and its member agencies';
j. Coordinates arrangements for and directs fire and earthquake drills with the approval and cooperation of all agencies concerned;
k. Arranges for posting on appropriate bulletin boards a roster of personnel who have responsibilities of emergency operations;
l. Establishes primary and alternative evacuations area;
m. Takes all necessary actions to ensure that the organization operates safely and efficiently during emergencies;
n. Exercises command responsibility for the orderly movement of all personnel in the building (including guests and visitors) in accordance with the evacuation route plan;
o. Arranges for and supervises the storage of required supplies and equipment in facility shelter;
p. Conducts periodic inspections of facilities and Offices.

2. Vice Chairman

The Vice Chairman serves as principal assistant to the Chairman and may also serve as one of the leaders of the Office Disaster Management Committee or Operating Teams.

3. Staff Teams

3.1. Security Team

a. Secures vacated building, areas of evacuation centre and disaster operations;

b. Implements and enforces personnel identification in the coordinated areas;
c. Coordinates with the local PNP/Barangay for the security of the areas;
d. Responds to alarm signals or other suspicious activities and reports to authorities concerned;
e. Performs escort duties in the transport of persons, supplies and equipment.

3.2. Supply Team

a. Determines the supply requirements of all action teams;
b. Identifies the sources of such supplies as needed;
c. Receives such supplies and channel the same to the team leaders.

3.3. Transportation Team

a. Determines the transportation needs and requirements;
b. Assigns all available vehicles and transport units;
c. Coordinates with counterpart transport team leaders and local transport groups for use of their facilities.

3.4. Communication Team

a. Receives warning information from the local civil authorities or other authoritative sources;
b. Disseminates such warning to all offices and attached agencies of the Department;
c. Maintains appropriate communication links with offices and personnel;
d. Keeps record of all communications and messages;
e. Organizes equipage and couriers;
f. Coordinates with Local Disaster Coordinating Councils, and concerned government agencies for communications requirements needs.

4. Operation Teams

4.1. Warning Team

a. Ensures that all occupants are oriented on the meaning of different signals and alarms;
b. Organizes warning teams for specific sections, floors, wings, buildings and areas;
c. Provides adequate warning devices and equipment;
d. Coordinates with LGUs and Local Disaster Coordinating Council for joint warning dissemination;
e. Coordinates with local civil defence and other response agencies/units for receipts of authoritative warning information.

4.2. Relief Team

a. Receives evacuees/victims from the evacuation service leader;
b. Provides temporary shelters for displaced persons/evacuees during emergency;
c. Informs the DRRG Chairman on the status of disaster relief activities;
d. Coordinates with other relief and response agencies, non-government organization, foundation, and people's organizations.

4.3. Fire Brigade Team

a. Organizes fire-fighting teams/brigades for initial fire instructions;
b. Provides fire-fighting instruction through available sources (local fire department);

c. Assures that fire fighter know their stations locations of fire fighting equipment in the area;
d. Deploys fire fighting personnel to fire areas.
e. Check/inspect fire fighting equipment is properly installed in all offices.

4.4. Rescue Team

a. Locates/removes injured or trapped persons in the area;
b. Organizes and trains the rescue teams provided for in the facility plan;
c. Obtains appropriate equipment for rescue operations.

4.5 Medical Team

a. Arranges with government health agencies, Philippine Red Cross (PRC) or other sources for first aid and medical self-help training;
b. Supervises the selection of first aid or medical treatment areas in shelters and elsewhere;
c. Directs first aid or medical self-help operations and controls access to medical supplies;
d. Establishes policies and rules governing the emergency treatment of ill/injured personnel;
e. Maintains adequate sanitation and hygienic standard and matters relating to emergency health;
f. Inspects the storage and handling of goods and drinking water in shelter areas within the building.

4.6 Damage Control Team

a. Establishes a plan to attend to mechanical devices, ventilation, water, gas and steam valves power switches and others;
b. Dispatches individuals or teams at the sound of emergency alarm to prearranged control or directed action;
c. Deploys personnel after fire or any emergency to correct damage with requires assistance;
d. Maintains physical facilities and evacuation centres and assess damages in the area.

VI. HUMAN-MADE / INDUCED HAZARDS

Human-made hazards are threats having an element of human intent, negligence, and error and involving a failure of a system.

A. Technological Hazards

1. Structure Collapse

Often caused by engineering failures such as under-design of structural components, by corrosion attack and by aerodynamic flutter of the deck.

- **Preparedness and Mitigation**

(What to do before)

a. Conduct a periodic general check on the conditions of the buildings thru the assistance of Engineers
b. Repair of rehabilitate structure to put them in good condition

- **Response**

  (What to do after)

  a. Vacate the building immediately
  b. Apply first aid, in case of injuries/casualties and bring the victim to the nearest hospital for medical treatment.

- **Rehabilitation Phase**

  (What to do after)

  a. Secure the area
  b. Evaluate and assess the damages to authorities for proper action
  c. Recommend for approval of the demolition of the condemned buildings.

2. Fire

Composed of three elements; heat, fuel and oxygen which when combined will result to a chemical reaction called burning.

2.1. Building Fire – Cause by:

a. System overloading e.g. octopus wiring/illegal connection
b. Overloading of appliances
c. Faulty electrical wirings and connections
d. Carelessness of users.

- **Preparedness and Mitigation**

  (What to do before)

  a. Post floor/evacuation plan in strategic locations
  b. Make fire extinguishers and alarm available.
  c. Educate by means of demonstration to employees on the proper use of fire extinguishers
  d. Maintain proper signage for fire exit
  e. Clear and free fire exits from obstruction
  f. Make sure that the public address systems are load, clear and functional
  g. Conduct regular inspections and safety checks of electrical outlets
  h. Assign personnel who will regularly check possible areas when fire may start such as stock room and computer laboratory
  i. Maintain safety plan and education program to preserve the building and protect personnel from fire.

- **Response**

  (What to do during)

1. Prior to the impact

- **DO's**

  a. Sound the alarm
  b. Advice fire department
  c. Fight the fire
  d. Drop, crawl and go when fire breaks outs
  e. Seek the nearest exit not blocked by fire
  f. Close windows and doors as you escape from the scene
  g. Evacuate
  h. Conduct inventory of employees.

- DONT's
    a. Do not panic
    b. Do not run
    c. Do not use the elevators
    d. Do not jump out from an upper floor

- Post Impact
    a. Seek medical assistance when injured
    b. Never return inside the building once outside
    c. Find your way out of the building for fresh air when smokes build up.

➢ Rehabilitation Phase
(What to do after)
    a. Coordinates with the Bureau of Fire and local engineering office for building assessment
    b. Conduct inventory of personnel and equipment, fixtures and facilities
    c. Report damage/s to proper authorities.

➢ How to Eliminate Electrical Fires

1. Check regularly electrical installations and have all open wirings, damaged sockets, switches and other destroyed electrical fixtures changes or repaired immediately. These are the common source of sparkling and arching, which often times become the source of destructive fires.
2. All electrical installations, repairs and changes shall be undertaken by a competent electrician.
3. Do not overload your electrical circuits by profusely putting extra lights or appliances.
4. Do not be replace blown fuses with pennies, wires or any metal to short circuit the current. Lighting circuits should be provided with fuses of limited amperage.
5. Use only approved types of electrical appliances and equipment. If not improve them.

➢ How to Use a Fire Extinguisher
1. Pull off the safety pin placed at the right side of the lever.
2. Hold the hose and aim the nozzle at the flame and keep a safe distance away from it.
3. Squeeze the upper and lower levers together to make it functional.
4. Sweep the nozzle during burst to prevent the rapid spread of fire and to keep it from affecting other things.

➢ Evacuation

Evacuate immediately if one is in a building. In case of fire, the smoke is usually more dangerous than the flames. If one will not be able to extinguish flames, do not panic, do the following:

1. Sound the alarm.
2. Report to Fire Department immediately by phone or the fastest means.
3. Evacuate the premise calmly.
4. In a smoke-filled room, crawl low under smoke. Keep crawling with head closest to the floor to avoid inhaling smoke. Oxygen is still present one foot above the ground. Cover your mouth with a wet clothes/handkerchief if possible. Swing your arms left and right alternatively while crawling to avoid hurting your head.
5. If the stairs cannot be used, leave the building at once through the fire escape or evacuation device, usually installed in the balcony.

6. Do not worry about your personal appearance or your personal possessions or valuable. Evacuate quickly and do not attempt to return.
7. If your clothes catch on fire, drop cover roll. Drop on the ground in prone lying (face on the ground) position, cover your face with your two hands and roll back and forth to stop the fire.

VII. NATURAL CALAMITY/DISASTER

A. EARTHQUAKE

An earthquake (also known as a quake, tremor or temblor) is the perceptible shaking of the surface of the Earth, which can be violent enough to destroy major buildings and kills thousands of people Earthquakes, is unpredictable.

1. Emergency Kit and Disaster Plan are Important

Because earthquakes happen without warning, being prepared in advance is critical to minimize damage to property and loss of life.

WHAT TO DO:

- Before an Earthquake
  a. Familiarize yourself with your place of works or residence.

  b. Develop an emergency plan. Preparedness can help reduce anxiety and minimize injury.

  c. Put together an emergency kit. Your kit should include non-perishable food, water, first aid supplies, flashlights, camping supplies (stove, battery-powered lantern, etc.), extra batteries, blankets and any personal items you may need (medications, toiletries, clothing).
- During an Earthquake
  a. Stay away from glass windows and furniture that could potentially fall over.

  b. Get under a study table or desk and do the "Duck, Cover, and Hold", to avoid being hit by falling object.

  c. Never to attempt to go out, wait until the shaking stops. Run/walk (in an orderly manner) as fast as you can.

  d. Do not use elevator, use stairways.

  e. Do not panic, remain calm.

  f. Do not jump from a building (if inside the building).

- After an Earthquake
  a. Stay calm,

  b. Check yourself by any injuries.

  c. Check for injured or trapped people in the building.

d. Check yourself and others for injuries. Provide first aid/seek medical help for anyone who needs it.

B. TYPHOON

Typhoon is a type of tropical cyclone, which is a general term for a circulating weather system over tropical waters.

WHAT TO DO:

- Before Typhoon:

1. Pack foods (can goods, biscuits, candies, chocolates).
2. Keep flashlights, candles and battery-powered radios within reach.
3. Keep your radio on to listen to the latest weather announcements. Store fresh batteries in case of emergency.
4. Evacuate from low-lying beaches or other locations which may be swept away by high tides or floods. Leave early if your only passage to high ground is over a road.
5. Store water as water service may be cut off or there may be leakage in water pipes that may cause diarrhea when drunk.
6. Double check everything that may be blown away or turn loose. Flying objects are dangerous during typhoons.

- During a typhoon:

1. Stay inside the building and keep updates with the latest weather forecast.
2. If safe drinking water is NOT available, boil water for at least 20 minutes, and then place it in a container with cover.
3. Do not wade through flood waters to avoid electrocution and water-borne diseases.
4. Stay away from low-lying beaches or other locations which may be swept away by tides or waves.
5. Check everything that may be blown away or turn loose. Flying objects are dangerous during typhoons.
6. Do not use gas or electrical appliances that were submerged during flood.
7. Be calm when going to an evacuation centre. Close all windows and turn off main power switch before leaving. Put important appliances and belongings on a high ground. Avoid roads leading to the river and areas prone to land-slide.
8. Don't panic, just stay calm. Your ability to handle an emergency will be a good example to others.

- After Typhoon:

1. Be sure that the building is safe and stable before you enter.
2. Beware of poisonous animals like snakes that may have entered the building.
3. Watch out for live wires or outlet immersed in water and report damaged electrical cables and fallen electric posts to authorities.

POWER FAILURE

Like any other part of the infrastructure, electrical power to the building can fail, either as an isolated incident (e.g., tripped circuit breakers) or as part of a larger event (scheduled outages, regional power outages or natural disasters). Power outages result in health & safety issues due to the loss of heating/cooling, reduced illumination, computer impairments, damage to sensitive equipment, and patient care disruptions. Just because power lines are damaged does not mean they are dead. Every downed power line is potentially energized and dangerous until utility crews arrive on the scene to ensure power has been cut off. Downed power lines, stray wires, and debris in contact with them all have the potential to deliver a fatal shock.

- Power Failure – Preparing Ahead of Time

Identify hazardous equipment that should be turned off after power fails because it might cause injury when restarted after power returns. Unless there has been an order to evacuate the building, assign an employee to turn off power or unplug to all hazardous equipment in the work area, such as shop machinery, after a power failure.

- Power Failure - Office

a. All welding, soldering, hot plates, coffee warmers, etc should cease immediately and not be left unattended until surfaces have cooled to a safe temperature. Turn power off to the hot work device.
b. Switch off electrical equipment to prevent unexpected or sudden start up when power is restored. Office equipment that should be switched off includes copiers, printers, computers, monitors, microwaves, and coffee pots. This does not apply to fridges and freezers.
c. Turn off all light switches. The voltage may fluctuate and damage lights that are on. Do not use candles or other type of flame for lighting.
d. Avoid ignition sources such as lighters, cigarettes, and candles.
e. Set all equipment and appliance switches to the OFF position. This is to avoid tripping the circuit breakers, blowing fuses, or damaging equipment from power surges when normal power is restored.
f. Do not use elevators during a power outage. It may become inoperative and unable to return to the primary floor without normal power.
g. If it becomes necessary to evacuate the premises during a power failure, be sure to protect all valuables and make sure that all equipment is safe when the power comes back on. Leave building and go to the assigned assembly place.
h. Assist disabled persons in exiting the building.
i. Never enter a flooded basement if electrical outlets are submerged. The water could be energized
j. Do not turn power off if you must stand in water to do so. Call your electric utility, and have them turn off power at the meter.
k. Before entering storm-damaged buildings, make sure electricity and gas are turned off.
l. Do not use water-damaged electronics before properly restoring them. Electric motors in appliances should be cleaned and reconditioned before use. It may be necessary to replace some of your appliances and electronics. Have your water-damaged items inspected and approved by a professional before using them.

m. If you clean-up outdoors after a storm, do not use electronic equipment when it is wet out.
n. If you are driving and come along a downed power line, stay away and keep others away. Contact emergency personnel or your utility company to address the downed power line.
o. If you do come in contact with a downed power line, do not leave the car. Wait for utility and emergency professionals to make sure the power line is de-energized before exiting the car.

- While the Power is Off

Do not conduct experiments or work with hazardous materials (biological, chemical or radiological) during power outages.

a. Ensure experiments, equipment, machinery or apparatus are stabilized or safe.
b. Cap volatile materials in fume hoods and close the sash. Do not use laboratory facilities during the shutdown or enter areas that have storage of material that require mechanical ventilation.
c. Check equipment on emergency power to ensure that it is running properly. Do not connect items not intended to be on emergency power during a disruption period.
d. Reschedule experiments due to limited availability of lighting, hand washing, toilets, air conditioning, medical gases, and vacuum.
e. Disconnect equipment that runs unattended, and turn off unnecessary lights and equipment. This will reduce the risk of power surges and other unforeseen damage or injury that could result when the power comes on unexpectedly.
f. Avoid ignition sources such as Bunsen burners, candles, lighters, cigarettes, or strikers during power outages.

- When Normal Power is Restored

a. Reset or restart equipment. Ensure that equipment is returned to a safe operation mode.
b. Do not enter a flooded basement unless you are sure the power is disconnected.
c. Do not use flooded appliances, electrical outlets, switch boxes or fuse-breaker panels until they have been checked and cleaned by a qualified electrician.
d. Switch on the main electric switch (before, check to ensure appliances, electric heaters, TVs, microwaves computers, etc. were unplugged to prevent damage from a power surge).
e. Give the electrical system a chance to stabilize before reconnecting tools and appliances. Turn the heating-system thermostats up first, followed in a couple of minutes by reconnection of the fridge and freezer. Wait 10 to 15 minutes before reconnecting all other tools and appliances.
f. Turn on the water supply. Close lowest valves/taps first and allow air to escape from upper taps.
g. Check food supplies in refrigerators, freezers and cupboards for signs of spoilage. If a freezer door has been kept closed, food should stay frozen 24 to 36 hours, depending on the temperature. When food begins to defrost (usually after two days), it should be cooked; otherwise it should be thrown out or composted.
h. Restock your emergency kit so the supplies will be there when needed again.

C. VOLCANIC ERRUPTION

Know beforehand where the active volcanoes are in your area. If so, be prepared at all times. Volcanic eruptions happen with early warnings unlike earthquakes that are sudden. Before the volcano erupts there are warning signs such as rumbling sounds, continuous emissions of steam, increasing temperature around the volcano that results to withering of plants around and unusual behaviours of animals and earthquakes. There are dangers that volcanic eruptions pose to people so it is important that they know how to handle situations before, during and after volcanic eruptions to avoid serious problems.

- **Here are precautionary measures before volcanic eruptions:**

a. If you run a business located in the area of volcanoes, create a business continuity plan(see page 30) for ensuring that staff can get to safety and for protecting stock, equipment, and any other business essentials.

b. A volcano can cause severe property damage. Review and if necessary purchase insurance to make sure you have the right kinds and amounts of coverage. **Put together an emergency supply kit.** This kit is something that anyone living in a volcano zone should have prepared at all times. The kit should include such items as a first aid kit, food and water supplies, a mask to protect against ash, a manual can opener, a flashlight with extra batteries, any necessary medications, sturdy shoes, goggles or other eye protection, store as much food, water and a battery-powered radio. Ensure that everyone knows where the emergency supplies that prepared are located.

c. Prepare all necessary things to bring once evacuated is needed. Those in danger zones are warned when to evacuate.

d. Volcanic eruption have ash falls so be prepared for masks or anything to cover nose and mouth.

- **Here are precautionary measures during volcanic eruptions:**

a. Avoid all low-lying places because lava flows and mudflows are more likely to pass them.
b. Seek cover in case of ash falls rock falls.
c. Use masks and cover your mouth and nose to avoid breathing in ashes.
d. Close all doors and windows to avoid ashes from getting inside.
e. Always stay indoors.
f. Stay in the evacuation centre until further instructions. Do not attempt to leave the place unless told to do so.

- **Here are precautionary measures after volcanic eruptions:**

a. Clean everything around the building and check all damages incurred.
b. Use masks while cleaning ash and other debris.
c. Wait for further announcements related to the volcano activities.
d. Make sure that the building is still safe for everyone.

D. TERROR ATTACK

Terrorism is commonly defined as violent acts (or threat of violent acts) intended to create fear perpetrated for a religious, political, or ideological goal, and which deliberately target or disregard the safety of non-combatants.

- **Be cautious to these Suspicious Behavior/Circumstances:**

a. People in buildings or areas who do not appear to be conducting legitimate business.
b. People monitoring areas, buildings or entrances.
c. Unauthorized people in restricted, sensitive or private areas.
d. Persons taking photographs of critical facilities.
e. Persons asking detailed information about physical security and/or information with no apparent need for that information.
f. People wearing clothing not consistent with the weather conditions (bulky coat in warm weather etc.)
g. Abandoned parcels or other items in unusual locations or high traffic areas.
h. Individual attempting to access utility locations (water, electrical, petroleum, telecommunications, information systems).
i. Multiple persons who appear to be working in unison, committing the above.

- **Be Alert to:**

a. Abandoned Vehicles
b. Vehicles Parked Near Buildings or Public and Common Areas
c. Unexpected/Unfamiliar Delivery Trucks
d. Unfamiliar Vehicles Parked For Long Periods
e. Vehicles Containing Unusual/Suspicious Parcels or Material
f. Vehicles Arriving and Being Left Behind at Odd Hours
g. Substances Leaking or Spilling from Vehicles

- **Hostage Defense Measures**

a. Survive with honour--this is the mission of any hostage.
b. If your duties may expose you to being taken hostage, make sure your family's affair is in order to ensure their financial security. Make an up-to-date will and give appropriate powers of attorney to your spouse or to a trusted friend.
c. If you are taken hostage and decide not to resist, assure your captors of your intention to cooperate, especially during the abduction phase.
d. Regain your composure as quickly as possible after capture, face your fears, and try to master your emotion.
e. Take mental note of the direction, time in transit, noise, and other environment factors that may help you identify the location.
f. Note the numbers, names, physical characteristics, accents, personal habits, and rank structure of your captors.
g. Anticipate isolation and terrorist efforts to confuse you.

h. Try to mentally prepare yourself for the situation ahead as much as possible. Stay mentally active.
i. Do not aggravate your abduction; instead, attempt to establish a positive relationship with them. Do not be fooled by a friendly approach-it may be used to get information from you.
j. Avoid political or ideological discussions with your captors; comply with their instruction, but maintain your dignity.
k. Do not discuss or divulge any classified information that you may possess.
l. Read anything you can find to keep your mind active.
m. Eat whatever food is offered to you to maintain your strength.
n. Establish a slow, methodical routine for every task.
o. When being interrogated, take a simple, tenable position and stick to it. Be polite and maintain your temper. Give short answers, talk freely about nonessential matters, but be guarded when the conversation turns to substantial matters.
p. I forced to present terrorist demands to authorities, in writing or on tape, do only what you are told to do. Avoid making a plea on your behalf.

- **During rescue phase:**

a. Drop to the floor.

b. Be quiet and do not attract your captors' attention.

c. Wait for instructions.

d. Rescue forces will initially treat you as one of the terrorists until you are positively identified as friend or foe. This is for your security. Cooperate, even if you are initially handcuffed.

e. Once released, avoid making comments to the news media until you have been debriefed by the proper authorities.

E. FLOOD

- **BEFORE A FLOOD**

When flooding is forecast:

- **Be alert.**
  a. Monitor your surroundings.
  b. Flash floods develop quickly. Do not wait until you see rising water.
  c. Get out of low areas subject to flooding
  d. If driving, do not drive through flooded roadways

- **Assemble disaster supplies.**
  a. Drinking water – Fill clean containers.
  b. Food that requires no refrigeration or cooking.
  c. Cash.
  d. Medications and first aid supplies.
  e. Clothing, toiletries.

f. Battery-powered radio.
g. Flashlights.
h. Extra batteries.
i. Important documents: insurance papers, medical records, bank account numbers.

- Be prepared to evacuate.
  a. Identify places to go.
  b. Identify alternative travel routes that are not prone to flooding.
  c. Plan what to do with your pets.
  d. Fill your car's gas tank.
  e. If told to leave, do so quickly.

- Review your Family Disaster Plan.

  a. Discuss flood plans with your family.
  b. Decide where you will meet if separated.
  c. Designate a contact person who can be reached if family members get separated. Make sure every family member has the contact information.

- Protect your property.

  a. Move valuables and furniture to higher levels.
  b. Move hazardous materials (such as paint, oil, pesticides, and cleaning supplies) to higher locations.
  c. Disconnect electrical appliances. Do not touch them if you are wet or standing in water.
  d. Bring outside possessions indoors or tie them down securely. This includes lawn furniture, garbage cans, and other movable objects.
  e. Seal vents to basements to prevent flooding.

➢ DURING A FLOOD

- Be alert.
  a. Monitor your surroundings.
  b. Make sure your vehicle has enough fuel.
  c. Follow recommended routes. DO NOT sightsee.
  d. Avoid disaster areas. Your presence might hamper rescue or other emergency operations and put you at further risk.
  e. Watch for washed out roads, earth slides, and downed trees or power lines.
  f. Be especially cautious at night, when it is harder to recognize flood dangers.
  g. If the vehicle stalls, abandon it.
  h. If water rises around your car, leave the vehicle immediately. Climb to higher ground as quickly as possible.

- NEVER drive through flooded roadways. STOP! Turn Around Don't Drown.
  a. The roadbed may be washed out.
  b. You can lose control of your vehicle in only a few inches of water.
  c. Your car may float. Vehicles can be swept away by less than 2 feet of water.

d. Do not drive around a barricade. Turn around and go another way!

- **Get to high ground – Climb to safety!**
  a. Get out of low areas that may be subject to flooding.
  b. Avoid already-flooded areas and do not attempt to cross flowing water.
  c. Stay away from power lines and electrical wires.

- **Evacuate immediately, if you think you are at risk or are advised to do so!**
  a. Act quickly. Save yourself, not your belongings.
  b. Move to a safe area before access is cut off by rising water.
  c. Families should use only one vehicle to avoid getting separated and reduce traffic jams.
  d. Shut off water, gas, and electrical services before leaving.
  e. Secure your home: lock all doors and windows.
  f. If directed to a specific location, go there.

- **Never try to walk or swim through flowing water.**
  a. If flowing water is above your ankles, STOP! Turn around and go another way.
  b. If it is moving swiftly, water 6 inches deep can knock you off your feet.
  c. Be aware that people have been swept away wading through flood waters.
  d. NEVER allow children to play around high water, storm drains, creeks, or rivers.

- **Shut off the electricity at the circuit breakers.**

If someone falls in or is trapped in flood water:

a. Do not go after the victim!
b. Use a floatation device. If possible throw the victim something to help them float, such as a spare tire, large ball, or foam ice chest.
c. Call emergency hotlines. Call for assistance and give the correct location information.

➢ AFTER A FLOOD

- **Wait until it is safe to return.**
  a. Monitor local television and radio stations.
  b. Do not return to flooded areas until authorities indicate it is safe to do so.
  c. Do not visit disaster areas following a flood. Your presence may hamper urgent emergency response and rescue operations.

- **Travel with care.**
  a. Follow recommended routes. DO NOT sightsee.
  b. Watch for washed out roads, earth slides, and downed trees or power lines.
  c. Stay away from downed power lines.

- **If a building was flooded, check for safety before entering.**
  a. Do not enter a building if it is still flooded or surrounded by floodwater.
  b. Check for structural damage. Inspect foundations for cracks or other damage.
  c. Turn off any outside gas lines at the meter tank.
  d. Do not enter a building that has flooded until local building officials have inspected it for safety.

- Use extreme caution when entering buildings.
  a. Wear sturdy shoes. The most common injury following a disaster is cut feet.
  b. Use ONLY battery-powered lighting. Flammable material may be present.
  c. Look for fire hazards (such as damaged gas lines, flooded electrical circuits, or submerged furnaces).
  d. Check for gas leaks. If you smell gas or hear a blowing or hissing noise, open a window and quickly leave the building. If possible turn off the gas at the outside main valve. Call the gas company.
  e. Report broken utility lines to appropriate authorities.
  f. Check for electrical system damage (sparks, broken or frayed wires, or the smell of burning insulation). Turn off the electricity at the main circuit breaker if you can reach it without stepping in water.
  g. Examine walls, floors, doors, windows, and ceilings for risk of collapsing.
  h. Watch out for animals that might have entered with the floodwaters.
  i. Let the building air out to remove foul odors or escaping gas.

- Take pictures of the damage, both of the building and its contents, for insurance claims.

Get professional help.

  a. Seek necessary medical care. Do not neglect minor wounds or illnesses.
  b. Food, clothing, shelter, and first aid are available from Red Cross.
  c. If the gas has been turned off for any reason, it must be turned back on by a professional.
  d. Have an electrician check the electrical system and appliances.
  e. Wells should be pumped out and the water tested for purity before drinking.

- Your home is no longer a safe place.
  a. Throw away medicine, food, or water that had contact with floodwaters (including canned goods).
  b. If water is of questionable purity, boil drinking water for 10 minutes.
  c. Restrict children from playing in flooded areas.
  d. Keep windows and doors open for ventilation.
  e. Pump out flooded basements gradually (removing about 1/3 of the water volume each day) to avoid structural damage.
  f. Keep the power off until an electrician has inspected the system for safety. All electrical equipment should be checked and dried before being returned to service.
  g. Clean and disinfect everything that got wet.
  h. Service damaged sewage systems as soon as possible.

- When making repairs, protect your property from future flood damage.
  a. Follow local building codes.
  b. Use flood-resistant materials and techniques.
  c. Elevate electrical components above the potential flood height.
  d. Elevate utilities (washer, dryer, furnace, and water heater) above the level of anticipated flooding.
  e. Consider elevation of the entire structure.
  f. Install a backflow valve in the sewer system.

➢ Flood Safety Precautions

- **Before**

a. Know the following terms: - Flood Watch—Flooding possible in a certain designated area. – Flood Warning—flooding imminent or already reported.
b. Learn to recognize environmental clues such as heavy rains, topography and flood history of the region.
c. Know your elevation above flood stage and the history regarding flooding of your location.
d. Learn first aid and CPR at your local Red Cross chapter or community organization.
e. Keep on hand a battery-operated flashlight and radio.
f. Learn evacuation routes.
g. Keep vehicle fuelled since power failure may render service stations inoperable.

- **During**

a. Avoid areas subject to sudden flooding.
b. Do not attempt to cross a stream where water is above your knees. When in doubt, don't try it.
c. Do not try to drive over a flooded road. The water can be much deeper than it appears and you could be stranded or trapped.
d. Do not try to drive around police barricades.
e. Stay away from drains and ditches.

- **After**

a. Do not eat fresh food that has come in contact with flood waters.
b. Boil drinking water before using.
c. Report broken gas, electrical and water lines immediately.
d. Do not handle electrical equipment in wet areas.
e. Do not sightsee. Your presence could impede relief efforts as well as endanger yourself.
f. Cooperate with local officials. Respond to requests for assistance from local police, fire fighters and relief workers. Community participation is critical to effective disaster relief.