TANZANIA SCOUTS ASSOCIATION

EMEGENCY MANAGEMENT POLICY AND PROCEDURES

Schedule of Amendments and Approval

Document Number	Revision	Approval Reference	Date
TSA/DOC/018	Creation	5th Ordinary Meeting of the National Executive Committee	4th June, 2016

TABLE OF CONTENTS

APPROVAL OF THE POLICY

This is an official EMERGENCY MANAGEMENT POLICY AND PROCEDURES (EMPP) for Tanzania Scouts Association, having been presented to the National Executive Committee and approved. As thus, we members of Executive Committee of Tanzania Scouts Association hereby commit that we will abide by this Policy and Procedures document from date of endorsement.

Thus signed on this day ________of __________________ 2016 in Dar es Salaam.

______________________________ **Chief Commissioner**	______________________________ **National Executive Chairperson**
______________________________ **National Executive Commissioner**	______________________________ **Honorary Secretary**

FORWARD

To insert forward statements by the Chief Commissioner

1 Purpose and Scope

Emergencies and critical incidents in the workplace can affect people physically and

Psychologically, and affect Business (activities) continuity of TSA.

The purpose of this policy is to ensure TSA prepares for and effectively responds to emergency situations and critical incidents through the appropriate use of resources. The prevention and effective management of emergency situations and critical incidents can assist to minimise the negative impact of an unexpected event.

This policy applies to all staff, Members, volunteers and visitors of Association.

2 Definitions

An emergency is an unplanned or imminent event that affects or threatens the health, safety or welfare of people, property and infrastructure, and which requires a significant and coordinated response. The defining characteristic of an emergency event or situation is that usual resources are overwhelmed or have the potential to be overwhelmed.
Emergencies may be a specific event with a clear beginning, end and recovery process, or a situation that develops over time and where the implications are gradual rather than immediate.

Emergency management is the coordination of an emergency response and management of recovery. The aim of emergency management is to minimize physical and psychological impacts on all parties and to minimise damage to assets, operations, reputation and staff productivity.

A critical incident is an unexpected traumatic event, involving personal or professional threat, which evokes extreme stress, fear or injury. Providing appropriate supports following a critical incident is part of emergency management.

A traumatic event is one in which a person experiences, witnesses or is confronted by experiences that involve actual, threatened or perceived death or serious injury and/ or threat to own or others physical and emotional integrity. The person's response may then include intense fear, feelings of helplessness and horror, which impact on their sense of 'self'.

Complex trauma refers to a condition resulting from multiple exposures to one or more traumas. When repeatedly exposed to traumatic stress, disruptions can occur in brain structure and function, central and autonomic nervous system arousal, endocrinological and immunological function. These biological disruptions interact with psychological, emotional, cognitive and spiritual processes.

Critical Incident Debriefing (CID) is a preventative health measure to minimise the impact of traumatic events and the development of major psychological health problems such as Post Traumatic Stress (PTS) Disorder.

Disaster is serious disruption of the functioning of a community or society causing widespread human, economic or environmental losses which exceed the ability of the effected community/society to cope using its own resources.

Evacuation is an operation whereby all or part of a particular population is temporarily relocated, whether individually or in an organized manner, from an area in which a disaster or emergency is imminent or has occurred.
Risk is the probability of harmful consequences or expected losses (deaths, injuries, property, livelihoods, economic activity disrupted or environment damaged) resulting

from interactions between natural or human- induced hazards and vulnerable conditions.

Risk Assessment refers to a methodology to determine the nature and extent of risk by analyzing potential hazards and evaluating existing conditions of vulnerability that together could potentially harm exposed people, property, services, livelihoods and the environment on which they depend.

Hazard is a potentially damaging physical event, phenomenon or human activity that may cause loss of life or injury, property damage, social and economic disruption or environmental degradation.

Disaster Management committee is Sub Committee of Executive Committee whose role is to set policy direction for planning, mitigation, preparedness, emergency response, recovery, and Business (activities) continuity. The committee has authority to take actions required to achieve an effective response to an emergency on behalf of EXCO.

Emergency Response Teams are working groups composed of individual from all volunteering to conduct the frontline operations of an emergency response, under the direction of the ACC DM at the National level, at the Regional and District level under the co-ordinator of Disaster.

Functional Area Recovery Management (FARM) Team are working groups composed of individual staff (either employed staff or volunteer) who are working or conversant in the operational area affected by the disaster which has disrupted TSA internal operations. The FARM team is responsible for planning of recovery in their respective area affected by a disaster,

Business Continuity Management (BCM) Team is the same as **Disaster Management committee** but is more specifically for the scope of TSA internal operations (business) continuity.

3 Abbreviations

TSA	Tanzania Scouts Association
EXCO	Executive Committee
CC	Chief Commissioner
DCC	Deputy Chief Commissioner
ACC(s)	Assistant Chief Commissioner(s)
ACC DM	Assistant Chief Commissioner responsible for Disaster Management
NEC	National Executive Commissioner

4 Principles

Emergency management planning is being prepared for events or incidents that stretch our ability to cope beyond normal day-to-day capacity.

The Association is committed to the protection of staff, members, and visitors during emergencies.

TSA swiftly and effectively responds to emergency situations, with the foremost goals of preserving life, protecting the organisation's property, and restoring operations as quickly as possible.

Critical incidents can be a threatening experience and appropriate supports are required to minimise long term effects arising from exposure to the trauma.

5 Outcomes

Emergency situations are prevented as far as practical.

The negative impacts of emergency situations and critical incidents are minimised through effective management.

6 Functions, Duties, Responsibilities and Delegations

6.1 National Scouts Council

~~Approves the TSA's Emergency Management Policy and Procedures.~~ Seeks periodic assurance from executive committee that Strategic Emergence Management Framework has been implemented and is operative.

6.2 National Executive Committee

Approves the TSA's Emergency Management Policy and Procedures.

6.3 Chief Commissioner

Responsible for the implementation of TSA Strategic Emergency Management Framework, including resourcing, planning, training, testing, monitoring review of the emergency management preparedness and evaluation.

6.4 Assistant Chief Commissioner - Disaster Management

The Assistant Chief Commissioner Disaster management is responsible for the overall management of emergency. In addition, the Acc Dm is responsible for:

- Coordinating the members of a Disaster Management Committee and

- Proving ongoing oversight of the Emergency Response plan
- Implementing the Emergency Response plan in an emergency
- Coordinating the Emergency Response Teams.
- Completing a formal investigation of an emergency event in a timely manner and marking recommendation to the disaster management committee
- Ensuring that he/she and appropriate others complete formal training in emergency management.

6.5 Disaster Management Committee

6.5.1 Responsibilities

The **Disaster management committee or Business Continuity Management Team** is responsible for:

- Developing, implementing and maintain the Emergence Response plan / Functional Area Recovery Management (FARM) plans
- Ensuring the technical reliability of the Association, response plans and Business (Activities) continuity plans.
- Following up on recommendation made by the ACC DM.
- Initiating and coordinating an annual emergency exercise or simulation
- Issuing directives and protocols for preparedness, emergency response and recovery.
- Delegating recourses responsible for emergency response

6.5.2 Disaster Management vis a vis Business Continuity Team

The term Disaster Management Committee will be more applied when the extent of disaster has affected the TSA external community while Business Continuity Management will be more used for the extent of disaster affecting the TSA internal operations. For the external community, TSA role will be that of Supporting Agency.

6.6 Emergency Response Teams and Functional Area Recovery Management Teams

The **Emergency Response Teams** are responsible for:

- Talking action in an emergency under the direction of the Assistant Chief Commissioner Disaster Management.
- The actions handled by Emergency Response Teams are of broader nature going to affected areas outside TSA internal operations.

- To participate effectively in the National Disaster as stated on the **TANZANIA EMERGENCE PREPAREDNESS AND RESPONSE PLAN(TEPRP)** on page no. 18,19 and 20

The **Functional Areas Recovery Management Teams** are responsible for:

- Development and support of individual Functional Areas Recovery Management (FARM) Team Plans for recovery of TSA internal operations.
- Testing essential element of preparedness for responding to a disaster on TSA internal operations.

6.7 Delegations of Authority

The CC delegates authority to the ACC DM to take all steps necessary to protect life, prevent or limit further injury, prevent or limit harm to the environment and Association in fracture and assets, and to protect the TSA core business and research in the lead up to, during and directly after an emergency event.
During an emergency event, the ACC DM may sub-delegate this authority to the Emergency Response team Leader.

7 Risk Management

All members, staff and volunteers are trained in disaster and emergency response procedures at induction

Emergency evacuation drills are undertaken in all sites **annual** under the instruction of **ACC DM**.

Disaster and emergency management plans are reviewed annually and/or following the event of a disaster or emergency situation.

As far as possible, traumatic events are prevented, and the impacts of trauma are minimised following traumatic events.

8 Policy Implementation

All staff and members have access to and are familiar with policies and procedures relating to disaster emergency management.

All staff and members have information which outlines actions to follow for various disaster and emergency situations, and are supported to undertake training for specific roles in emergency and critical incident.

9 Policy Details

TSA identifies, prevents and manages disaster and emergency situations within its sphere of responsibility and influence, until the arrival of appropriate emergency services.

A range of emergency situations may occur on the premises with the potential to impact on the safety of staff, members, visitors, assets, operations (activities) of TSA and external community including:-

- Fire
- Gas or water leak
- Vehicle and other accidents
- Chemical, radiation or biological spill
- Bushfire
- Storm
- Earthquake
- Bomb threat
- Civil disorder or illegal occupancy
- Hostage or terrorist situation
- Death
- Robbery
- Physical (including sexual) assaults.

9.1 Risk Assessment

TSA uses risk assessment processes to identify and control barriers to effective emergency management. Details for risk management and assessment are further covered in the TSA's ***Risk Management Policy and Procedures***.

Staff, members and visitors are expected to behave in a way which minimises the risk of emergencies occurring.

9.2 Preparedness

The ***Emergency Checklists & Procedures*** (***Appendix A***) supports the Association to prepare for potential disaster and emergency situations, and is reviewed on **quarterly basis**. Disaster and Emergency management plans are reviewed **annual** basis.

All staff, members and visitors are provided with training to ensure they are familiar with implementation of disaster and emergency management plans.

All staff, members and visitors familiarise themselves with emergency evacuation procedures, including their responsibilities and the emergency evacuation assembly point.

All fire safety activities undertaken by the Association are recorded and reviewed to identify gaps in training, knowledge, equipment or processes. Fire activities include, but are not limited to, fire safety training, drills and exercises, records of maintenance and inventories of equipment kept.

Where relevant, all staff, students and volunteers familiarise themselves with techniques to minimise physical and emotional harm from other people.

9.3 Response

When a disaster or emergency situation arises, the primary aim of the response is to ensure the safety of all people on the premises, preserve life and protect property.

TSA initiates recovery and aims to restore operations as quickly as possible.

The availability of critical incident debriefing is an essential component of the Association's approach to emergency management.

When required; supportive counselling is provided to visitors, staff, and members who are affected by an emergency or critical incident within two hours of the event (for defusing and mobilisation) and then within 48 to 72hours (for critical incident debriefing).

10 Emergency and Critical Incident Procedures

Staff, members, and visitors who experience a critical incident related to their involvement with **TSA** should immediately inform where possible **CC/DCC**. If this is not possible they should immediately inform **ACC DM**.

10.1 A Critical Incident Report:

- is to be completed by the ACC DM involved in the incident or notification of the incident.
- is to contain as much information as possible and indicate the people directly involved in the incident.

The Committee who receives the report will ensure that the person(s) identified in the critical incident receives all appropriate support.

The **Disaster Management Committee (DMC)** in conjunction with **Emergency Response Teams** will assess the Critical Incident and implement a plan of action to follow up the Critical Incident.

Where required, a meeting will be organised to determine issues and responsibilities relating to:-

- Assessing risks and response actions
- Liaison with emergency and other services
- Contact with the affected person's relatives and other supports
- Liaison with other organisations
- Counseling and supporting staff, members, volunteers, and visitors not directly involved in, but affected by, the incident.
- Media management (if required)
- Where appropriate **TSA** may be required to provide support to the family in the form of:-
    a. hiring interpreters
    b. making arrangements for hospital/funeral/memorial service/repatriation
    c. obtaining a death certificate
    d. assisting with personal items and affairs including insurance issues

TSA will conduct a review of actions arising from the above meeting to ensure:-

- Follow up such as de-briefing, counseling and prevention strategies have been completed.
- Relevant people have been informed of all outcomes from the incident
- A recommendation as to the response to the critical incident is documented and included in the quality improvement cycle.
- Further follow up required is documented and responsibilities allocated to appropriate staff.

10.2 Critical Incident Debriefing (CID)

Critical Incident Debriefing (CID) will occur within 48 - 72 hours after the incident.

Debriefing may include individual and group counseling, where the aim is to:
- Decrease feelings of isolation
- Provide people affected by the incident with a facilitated session to assist them to normalise their thoughts and feelings. Groups assist people to explore their differing perspectives of the incident and share their similar thoughts and feelings.

There will usually be an initial counseling session, followed up with one or more debriefing sessions.

Initial counseling will occur as soon as possible after the incident, preferably immediately or within a few hours. Depending on the type or severity of the critical incident, initial defusing may include:-
- A short factual statement about what is known about the incident, the possible effects on those involved, what is being done for them and what is going to happen in the future, eg.; planned debriefing sessions.
- Information on acute stress response (what is happening to people now) and how people can care for themselves.
- An arrangement for a structured debriefing session within 48-72 hours.
- The provision of different levels of service for those differently affected
- Referrals to various resources including counselors

TSA will maintain confidentiality to ensure that:-
- Only a record of when and where a debriefing took place will be kept; and
- No information will be released without the agreement of the individual or group.

10.3 Evacuation

In the event of an alert to evacuate - either verbal, automatic alarm or manual alarm and the threat is immediate, all staff, members, and visitors:
- Proceed along designated routes to the designated assembly area(s)
- Ensure assistance is provided to people with disabilities and/or special needs
- **ACC DM** to collect visitor sign-in and staff attendance registers and direct people to the assembly point.
- **ACC DM** to check attendance at assembly area against the attendance registers.
- Remain at the assembly area until advised by the [insert position] and/or emergency personnel that it is safe to return to premises.

10.4 Emergency Checklists and Procedures

The Emegency Checklists and procedures provided under ***Appendix A*** covers the following:

Checklist #01 - Bomb Threat Procedures

Checklist #02 - Cyber Security Threat Assessment
Checklist #03 - Cyber Security Checklist 20
Checklist #04 - Handling Suspicious Parcels or Letters
Checklist #05 - Prevention and Response to Workplace Violence
Checklist #06 - Threat of fire
Checklist #07 - Hold-up 25
Checklist #08 - Earthquake
Checklist #09 - Flood
Checklist #10 - The Evacuation “GO BOX”

11 Communications

Communication with the wider TSA community will be undertaken in accordance with the TSA’s Constitution and system described in the Internal and External Communications Policy.

Only the following people are authorized by TSA to speak to the media in relation to an incident or Emergency:

- The Chief Commissioner or Deputy Chief Commissioner
- ACC DM by permission of CC or
- The National Executive Commissioner

12 Recovery Procedures

TSA's emergency management recovery arrangements shall be effectively integrated with Business (activities) Continuity Management (BCM) and IT Disaster Recovery arrangements as and when the Association becomes more automated.

In addition to Business Continuity Management (BCM) and IT Disaster Recovery arrangements, TSA will develop effective plans and procedures that promote holistic recovery of the Association and its communities.

12.1 Hazard Analysis, Impact, Mitigation And Recovery Actions

This section analyzes hazards that TSA operations/ functions could face, their mitigation measures and recovery procedures/actions to be taken inline with Functional Area Recovery Management (FARM) Team plans in case a real disaster occurs.

The table herein below summarizes the risks and subsequent recovery procedures.

Risk	Identify the hazards that the business could face including natural, technological disasters, biological, terrorism, civil emergencies and other business interruptions.
Probability	The likelihood of the risk occurring (high, medium, low).
Impact	- Will the impact on our business/operations be high, medium or low? - The human impact (injuries and /or losses). - Property impact (Physical damage to building structure, machines, computers, etc). - Business impact (cost to restore damage + profit lost due to business interruption + fixed cost) - The findings of the impact (High, Medium, Low) as analyzed in Attachment -3
Likely Scenario	The most likely reasons for problems/hazard/disaster to occur.
Functions Affected	Specific functions affected by the disaster.
Action	- What to do when the interruption occurs. - Recovery actions to be taken in line with the FARM Team plans.
Responsibilities	- Who takes what actions - Key BCM and FARM Teams (personnel) responsible for execution of the plans.
Mitigation	- What is TSA doing to minimise the risk before it happens. - Specifically address those tasks/ investments and resources necessary to eliminate or reduce the impacts of specific hazards.
Constraints	The practicalities of dealing with the risk
Resources	- The implications for costs, staffing, facilities etc - Internal resources available for immediate access during emergency or business disruption (e.g. fire extinguisher, powerbackup, etc.) - external resources available upon request/ through contract (e.g. local emergency management office, hazardous materials response, hospitals, utilities, etc.)

12.2 Total or Partial Building Loss – TSA Office

Risk	**Total or Partial– TSA Office**
Probability	Low
Impact	Medium to High, depending on the scope of damage.
Likely Scenario	Fire, bomb threat (terrorist), earthquake etc.
Functions Affected	All
Action	- Contact nominated agency to assess damage and availability and timing of alternate locations (alternate / recovery) site - Contact all TSA staff and suppliers to arrange alternate locations and contact details - If documents have been destroyed see '*Documents Lost'*. - If documents have been damaged, see '*Fire or Water Damage to Documents'* - Move TSA business operations (staff) to available designated recovery site / backup site with phone access and preferably networked PC's. - Inform all business units, stakeholders and public - Initiate this Recovery by applying appropriate FARM Team Plans (Disaster Recovery Standard Operating Procedures)
Responsibilities	- CC and ACC DM - NEC to contact nominated agency - FARM Team to coordinate contacting all staff and suppliers - Other FARM Teams of affected areas
Mitigation	- Alternate arrangements will be made at any Local Association nearby.
Constraints	*The Emergency Checklists & Procedures override these instructions if there are any conflicts*
Resources	Cell Phones; TSA Laptop(s)at staff residences; backups at alternate (recovery) site

12.3 Unavailability of Internet/ Email/ Website

Risk	**Unavailability of Internet/ Email/ Website**
Probability	Medium
Impact	High
Likely Scenario	- Problem with the service provider internet back bone or the broadband line being disturbed/ disrupted. - Problem in the hosting servers of email & website provided by external partner
Functions Affected	- Business units sending requests over the Internet including accessing the Email system. - Receipts of information from stakeholders. - Feedback messages from website. - Any other business units using email communication and website publication.
Action	- Contact Business Units by phone and ask that all communications be by phone, on paper or in person. - Matter is taken up with the concerned service provider to know the reasons for un-availability and down time duration - Avail laptop(s) with alternate modems/adapters to access Internet for small downloads and uploads of files. - Request Fax reports - Send the driver/messenger to collect information - When the concerned service is available again, then resume normal services
Responsibilities	- NEC, ACC responsible for ICT - Heads of affected functional unit (ACCs) coordinate the FARM team plans
Mitigation	- Some TSA laptops have been installed with modem/adapters from alternate service providers.
Constraints	Since this service is provided by third party vendor, estimation of real down time may be difficult.
Resources	- External Modem/adapters to activate fallback internet connection - Phone/ Fax

12.4 Unavailability of Phone/Fax Connectivity

Risk	**Unavailability of Phone/Fax Connectivity**
Probability	Low
Impact	High
Likely Scenario	Phone system or phone line problems with service providers
Functions Affected	- NEC Office - Business units requesting phone/ fax services
Action	- Contact Business Units to inform that all communications be in person or through any other alternate mode. - Matter is taken up with the concerned service provider to know the reasons for un-availability and to know the down time duration - Send the messenger/driver to collect the required information - Use emails
Responsibilities	- NEC and FARM Team - Heads (ACCs) of affected functional unit coordinate the FARM team plans
Mitigation	mobile phone; email and fax if applicable
Constraints	
Resources	email; mobile phone

12.5 Hardware - Computer/Telecom/Office Equipment Problems

Risk	Hardware - Computer/Telecom/Office Equipment Problems
Probability	Low
Impact	Medium to High depending on the nature of the problem
Likely Scenario	Malfunctioning PC, printer, scanner, CD burner, projector, PABX, Computer server, racksetc
Functions Affected	Any
Action	- Business units are informed about the problem - For PC's and printers, contact NEC / FARM Team; switch to another PC or printer if available. - For the CD Burner, contact the NEC / FARM Team; arrange use of another CD Burner in the meantime. - For other TSA equipment (computer server, scanners, data projector) contact the supplier or manufacturer. - Maintain the Service Support Agreement with the service provider for machines which are out of warranty period. - When the hardware problem is resolved resume normal operations.
Responsibilities	- FARM Team responsible for ICT - FARM Team affected - PC user is responsible to switch to another available PC and escalate the problem to NEC / ACC DM / ACC responsible for ICT.
Mitigation	- Service agreements for mission-critical equipment and SW
Constraints	Dependency on service provider can impair our business operations
Resources	Phone, fax and email etc

12.6 Missing Incoming/Outgoing Mail

Risk	**Missing Incoming/Outgoing Mail**
Probability	Low
Impact	High
Likely Scenario	Incoming or outgoing mail reported overdue or missing.
Functions Affected	Incoming or outgoing couriers, ad hoc or scheduled; potentially any business operation.
Action	Contact affected business unit and / or sender to get full description of parcel, delivery method, addressee, times and dates. Check with the one involved in the dispatch and look in allsatchels, empty mailbags and trolleys. **<u>Incoming</u>** Check at main reception (ask all staff on duty at likely delivery time) ***and Tender Box*** Check all other reception areas Ask courier company **<u>Outgoing</u>** Check with Document resource personnel at all likely sites **<u>If still not found</u>** Put notice on staff bulletin board/memo, consider broadcast email Repeat some of these actions over two or three days if necessary – most parcels turn upthe next day at the correct destination
Responsibilities	- FARM Team responsible for HQ (NEC)
Mitigation	- Collecting documents from source offices should be carried to TSA office in a dedicated mailbag - Distributing documents from source offices should be carried to TSA office in a dedicated mailbag - Attached priority tags on important mails (eg payment instructions) - Maintenance of inward/outward register
Constraints	- Absence of secured delivery mechanism - Some of the incoming and outgoing services are provided by third party.
Resources	email, phone, mail register

12.7 Documents Lost – Electronic (Specific Documents)

Risk	**Documents Lost – Electronic (Specific Documents)**
Probability	Low
Impact	Varies Low to High
Likely Scenario	Document accidentally deleted
Functions Affected	All electronic and paper-based document related activities
Action	Immediately: - Contact Head of Department/Unit (ACC) to log problem and if necessary request recreation from backup if applicable. - Advise all affected business units. - If problem cannot be fixed by recreation from backup, investigate ways and need to recreate from paper files, or from individual staff members or suppliers (involve all stakeholders)
Responsibilities	FARM Team of affected area
Mitigation	Electronic documents are stored in a shared folders in the filed server.
Constraints	It can take time to organize a recovery
Resources	Backup; File Server, CD's

12.8 Documents Lost – Hardcopy (Specific Document, File or Box)

Risk	**Documents Lost – Hardcopy Specific Document, File or Box)**
Probability	Medium
Impact	Low to high
Likely Scenario	Important document got lost/damaged due to various means ie fire, water, inadvertently shredded, theft, etc.
Functions Affected	The affected business/Unit and the TSA as a whole where applicable.
Action	- Determine the last known person involved with document. - Check at likely sites. - Contact individual staff members who may have knowledge of the documents concerned. - If document is irrevocably lost, discuss impact with stakeholders, issue statement of search and loss signed by CC. - Assess damage on affected document
Responsibilities	FARM Team of affected area
Mitigation	Use fireproof file cabinets Some documents eg Contracts are scanned to CD, and copies are held by business units and other soft copies saved in File Server
Constraints	Depending on external factors
Resources	Backup; File Server, CD's

12.9 Fire or Water Damage to Documents

Risk	**Fire or Water Damage to Documents**
Probability	Low
Impact	Medium
Likely Scenario	Fire damage plus water damage from sprinklers and hoses; or stormwater damage. Water damage is usually the most serious outcome of a fire.
Functions Affected	Business Units using files.
Action	- If water problem occurs when TSA staff are present and is in a TSA controlled area, putpolytarps over affected shelves. - Assess damage (may require input from business units) – if not manageable in house, contact external services to get quotes on removal, drying and cleaning. *Drying should begin within 24 hours to minimise damage.* - Advise all business units of extent of problem and likely delays - If documents are lost, see *Documents Lost – Hardcopy*
Responsibilities	- Senior TSA staff member present to coordinate and escalate if required.
Mitigation	
Constraints	- Polytarps only useful if water is in limited area under TSA control and problem occurs while TSA staff present. - Cost for use of commercial recovery specialists.
Resources	Polytarps, email, phones

12.10 Power Unavailable

Risk	**Power Unavailable**
Probability	Low
Impact	High
Likely Scenario	lights or power points only or all 240v power failure
Functions Affected	All, main impact if outage is long.
Action	- Total power outage means lights, phones or computers. - Find out extent and likely duration of problem – contact TANESCO for main power. - Use the rechargeable flashlights in the TSA area at night, if required in office. - If the outage is long, acquire a standby generator to be connected to service TSA office
Responsibilities	NEC / FARM Team of affected area
Mitigation	-
Constraints	Fall back Standby generator not working/available
Resources	phone, mobile phone, rechargeable flashlights, generator

12.11 Vehicle Unavailable

Risk	**Vehicle Unavailable**
Probability	Low
Impact	Low
Likely Scenario	- Due to accident - Seized/repossessed/impounded - The TSA's vehicle booked to go for specific delivery/collection, unavailable at last minute
Functions Affected	All business Units.
Action	- Hiring of alternate vehicles - Take appropriate actions to make the vehicle available in the future.
Responsibilities	NEC / FARM Team
Mitigation	Finalize arrangement with rental car company Use personal vehicle .
Constraints	No allocated budget
Resources	phone, staff, cash, vehicle and drivers

12.12 Employee Unavailable

Risk	High
Probability	Low
Impact	Business discontinuity
Likely Scenario	Sickness, death, disappearance etc.
Functions Affected	Employee's Department/ unit
Action	-Substitute employee to take over the duties -Report to appropriate channels in case of disappearance
Responsibilities	NEC / FARM Team of affected Department/unit
Mitigation	-To have more than one personnel for every position -To have clear, detailed and updated operational manuals in every Directorate / Unit -To have succession plan in every section
Constraints	-Low manning level
Resources	-Human resource budget

13 Emergency Contact Numbers

Organisation	**Phone / Address**
Police	112
Crime Stoppers Police	111
Fire Brigade	112
Ambulance	112
Anti Corruption Bureau	113
TANESCO	CALL CENTER (HQ) 0768 985 100

Appendix A : Emergency Checklists & Procedures

Checklist #01 : Bomb Threat Procedures

- If you receive a bomb threat by phone, instruct employee(s) to get as much information from the caller as possible. Keep the caller on the line and record everything that is said.

- If you are notified of a bomb threat referring to a delivered package, do not touch any suspicious packages. Clear the area around the suspicious packages and notify the police immediately.

- At the same time, <u>emergency warning procedure </u>should be implemented, so others can notify law enforcement, building management and staff.

- Initiate shutdown and <u>emergency evacuation procedures.</u>

- At meeting place, verify the evacuation of all employees and visitors

<u>Question to Ask the Caller</u>

1. When is the bomb going to explode?
   …………………………………………………………………..……………..

2. Where is the bomb?
   ………………………………………………………………………………….

3. What does it look like?
   ....

4. What kind of bomb is it?
   ……………………………………………………………………….….

5. What will cause it to explode?
   …………………………………………………………………..…………..

6. Did you place the bomb?
   …………………………………………………………..…………..……

7. Why did you place the bomb?
   ……………………………………………………………………………………

8. Where are you calling from?
   ……………………………………………………………………..……...

9. What is your address?
   ……………………………………………………………………………………

10. What is you name?
………………………………………………………………………………….

If voice is familiar, who did it sound like?
…………………………………………………………………………………………….

Were there any background noises?
…………………………………………………………………………………………….

Telephone number call received at
…………………………………………………………………………………………..

Person receiving call ……………………………………………………………………..

Any additional remarks…………………………………………………………………..

CALL POLICE 112 IMMEDIATELY!

Checklist #02 : Cyber Security Threat Assessment

SECURITY CHECKLIST	Yes	No
PHYSICAL SECURITY		
1. Is your computing area and equipment physically secured? 2. Are there procedures in place to prevent terminal from being left in a logged-on state, however briefly? 3. Are screens automatically locked after 10 minutes idle? 4. Are modems set to Auto-Answer OFF (not to accept incoming calls)? 5. Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)? 6. Does your staff wear ID badges? 7. Do you check the credentials of external contractors? 8. Do you have procedures for protecting data during equipment repairs? 9. Is waste paper binned or shredded? 10. Do you have procedures for disposing of waste materials? 11. Do your policies for disposing of old computer equipment protect against loss of data (e.g. by reading old disks and hard drives)? 12. Do you have policies covering laptop security (e.g. cable lock or secure storage)?		
ACCOUNT AND PASSWORD MANAGEMENT		
13. Do you ensure that only authorized personnel have access to your computers? 14. Do you require and enforce appropriate passwords? 15. Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default password)? 16. Are your computers set up so that staff entering passwords cannot be viewed by others?		
CONFIDENTIALITY OF SENSITIVE DATA		
17. Are your exercising responsibilities to protective sensitive data under our control? 18. Is your most valuable or sensitive data encrypted?		
DISASTER RECOVERY		
19. Do you have a current business continuity plan?		
SECURITY AWARENESS AND EDUCATION		
19. Are you providing information about computer security to your staff? 20. Are employees taught to be alert to possible security breaches?		

Checklist #03 : Cyber Security Checklist

This is an example of a threat checklist using 0-5 rating scales for impact and likelihood.

IMPACT SCALE	LIKELIHOOD SCALE
0 Impact is negligible	0 Unlikely to occur
1 Effect is minor; major agency operations are not affected.	1 Likely to occur less than once per year
2 Agency operations are unavailable for a certain amount of time, costs are incurred, public/customer confidence is minimally affected.	2 Likely to occur once per year
3 Significant loss of operations; significant impact on public/customer confidence.	3 Likely to occur once per month
4. Effect is disastrous; systems are down for an extended period of time; system need to be rebuilt and data replaced.	4 Likely to occur once per week
5 Effect is catastrophic; critical systems are offline for an extended period; data are lost irreparably corrupted; public health and safety are affected.	5 Likely to occur daily

Threats	Impact (0-5)	Likelihood (0-5)	Total (Impact x Likelihood)
GENERAL THREATS			
Human error:			
1. Accidental destruction, modification, disclosure, or incorrect classification of information			
2. Ignorance: Inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge			
3. Workload: Too many or too few system administrators; highly pressured users.			
4. Users may inadvertently give information on security weakness to attackers.			
5. Incorrect system configuration			
6. Security policy not adequate or not enforced.			
SABOTAGE			
1. Dishonest: Fraud, theft, embezzlement, selling of confidential agency information.			
2. Attacks by “social engineering?” • Attackers may uses telephone to impersonate employees to persuade users/administrators to give username/password/modem numbers, etc. • Attackers may persuade users to execute Trojan horse programs			
3. Abuse of privilege/trust			
4. Unauthorized use of “open” terminals/PCs			
5. Mixing of test and production data or environments			
6. Introduction of unauthorized software or hardware			
7. Time bombs: Software programmed to damage a system on a certain date			
8. Operating system design errors: Certain systems were not designed to be highly secure			
9. Protocol Design errors: Certain protocols were not designed to be highly secure. Protocol weaknesses in TCP/IP can result in:			

• Source routing: DNS spoofing, TCP sequence guessing, unauthorized access. • Hijacked sessions and authentication session/transaction replay; data is changed or copied during transmission. • Denial of service, due to ICMP bombing, TCP-SYN flooding, large PING packets, etc.			
10. Logic bomb: Software programmed to damage a system under certain conditions.			
11. Viruses in **programs**, documents, e-mail attachments.			
IDENTIFICATION/AUTHORIZATION THREATS			
1. Attack programs masquerading as normal programs (Trojan horses)			
2. Attack hardware masquerading as normal commercial hardware			
3. External attackers masquerading as valid users or customers			
4. Internal attackers masquerading as valid users or customers			
5. Attackers masquerading as helpdesk/support personnel			
RELIABILITY OF SERVICE THREATS			

Threats	**Impact (0-5)**	**Likelihood (0-5)**	**Total (Impact x Likelihood)**
1. Major natural disasters: fire, smoke, water, earthquake, storms/hurricanes/tornadoes, power cuts, etc.			
2. Minor natural disasters, of short duration, or causing little damage.			
3. Major human-caused disasters: war, terrorist incidents, bombs, civil disturbance, dangerous chemicals, radiological accidents, etc.			
4. Equipment failure from defective hardware, cabling, or communications system.			
5. Equipment failure from airborne dust, electromagnetic interference, or static electricity.			
6. Denial of service: • Network abuse: Misuse of routing protocols to confuse and mislead systems. • Server overloading (processes, swap space, memory, “tmp” directories, overloading services). • E-mail bombing • Downloading or receipt of malicious Applets, ActiveX controls, macros, Postscript files, etc.			
7. Sabotage: Malicious, deliberate damage of information or information processing functions:- • Physical destruction of network interface devices, cables, • Physical destruction of computing devices or media • Destruction of electronic devices and media by electromagnetic radiation weapons (HERF Gun, EMP/T Gun) • Theft • Deliberate electrical overloads or shutting off electrical power. • Viruses and/or worms. Deletion of critical system files.			
PRIVACY THREATS			
1. Eavesdropping: • Electromagnetic eavesdropping/Van Eck radiation.			

• Telephone/fax eavesdropping (via “clip-on”, telephone bugs, inductive sensors, or hacking the public telephone exchanges. • Network eavesdropping: Unauthorized monitoring of sensitive data crossing the internal network, unknown to the date owner.			

Threats	**Impact (0-5)**	**Likelihood (0-5)**	**Total (Impact x Likelihood)**
Network eavesdropping: Unauthorized monitoring of sensitive data crossing the Internet, unknown to the date owner. • Subversion of DNS to redirect e-mail or other traffic. • Subversion of routing protocols or redirect e-mail or other traffic. • Radio signal eavesdropping. Rubbish eavesdropping (analyzing waste for confidential documents, etc.			
INTEGRITY/ACCURACY THREATS			
1. Malicious, deliberate damage of information or information processing functions from external sources.			
2. Malicious, deliberate damage of information or information processing functions from internal sources.			
3. Deliberate modification of information.			
ACCESS CONTROL THREATS			
1. Password cracking (access to password files, use of bad (blank, default, rarely changed) passwords).			
2. External access password files, and sniffing of the network.			
3. Attack programs allowing external access to systems (back doors visible to external networks)			
4. Attack programs allowing internal access to systems (back doors visible to internal networks)			
5. Unsecured maintenance modes, developer backdoors.			
6. Modems easily connected, allowing uncontrollable extension of the internal network.			
7. Bugs in network software which can open unknown/unexpected security holes. (Holes can be exploited from external networks to gain access. This threat grows as software becomes increasingly complex).			
8. Unauthorized physical access to system.			
REPUDIATION THREATS			
1. Receivers of confidential information may refuse to acknowledge receipt.			
2. Senders of confidential information may refuse to acknowledge source.			
LEGAL THREATS			
1. Failure to comply with regulatory or legal requirements (e.g. to protect confidentiality of employee data).			
2. Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (e.g. incitement to racism, gambling, money laundering, distribution of pornographic or violent material).			
3. Liability for damages if an internal user attacks other sites.			

Checklist #04 : Handling Suspicious Parcels or Letters

Be wary of suspicious packages and letters. They can contain explosives, chemical or biological agents. Be particularly cautious at your place of employment. Some typical characteristics postal inspectors have detected over the years, which ought to trigger suspicion, include parcels that:-

- Are marked with restrictive endorsements, such as “Do not x-ray” or ‘do not share the content with others’
- Have protruding wires or aluminum foil, strange odors or stains.
- Are of unusual weight, given their size, or are lopsided or oddly shaped.
- Are marked with any threatening language or have inappropriate or unusual labeling.
- Have excessive postage or excessive packaging material such as masking tape and string.
- Are addressed to someone no longer with your organization or are otherwise outdated.

With suspicious envelopes and packages other than those that might contain explosives, take these additional steps against possible biological and chemical agents.

- Place suspicious envelopes or packages in a plastic bag or some other type of container to prevent leakage of contents. Never sniff or smell suspect mail.
- If you do not have a container, then cover the envelope or package with anything available (e.g., clothing, paper, trash can, etc.) and do not remove the cover.
- If you are at work, report the incident to your supervisor, who should notify other authority without delay.

Checklist #05 : Prevention and Response to Workplace Violence

- Establish an atmosphere of awareness and encourage employees to report suspicious activity or behavior, strangers, unexplained events, unscheduled deliveries or suspicious mail;

- Maintain strict hiring policies that include background checks;

- Establish Staff Code of Conduct with zero tolerance to gross misconduct (reference to Staff Regulations;
- List prohibited conduct;

- Monitor current employees' behaviours;

- Train supervisors how to recognize and resolve problems;

- Maintain a working environment that is open to communication and respectful to all employees; and

- Balance a violence-free workplace with employee rights.

- If you find yourself struggling to wade through these complicated laws, you may want to consult an employment law attorney.

- Institute appropriate security procedures to prevent attacks on the facility or your employees, by restricting access to your facility and incorporating crime prevention techniques;

- Establish a procedure to alert management and staff and law enforcement of a potential threat ("panic button," intercom, code word)

- Ensure all employees understand the Emergency Evacuation Procedures

Checklist #06: Threat of fire

In the event of a fire:

- Trigger the fire alarm, if it's available.
- Contact fire emergency services.
- Alert the CC or ACC DM
- Evacuate people from the immediate area of the fire behind a rated fire door or outside the building
- Fight the fire with existing equipment if safe to do so
- if it is safe to do so, close all doors and windows and turn off power supply before leaving the premises.

Checklist #07: Hold-up

In the event of a hold-up situation:

- Assume the offender is armed and that any firearms are loaded
- Comply with instructions given by the offender, doing no more or less than what you are told to do, and answer all questions asked
- Do not attempt to disarm or apprehend the offender
- Take mental notes of details about the offender and any items that are touched by the offender
- If it is safe to do so, raise the alarm

Immediately after the incident:

- Lock access doors to secure the area and prevent people from approaching
- Notify the police immediately
- Notify CC/DCC or ACC DM
- Attend to the post-incident needs of staff, members and visitors affected by the incident.

Checklist #08: Earthquake

In the event of an earthquake:

If you are indoors:

- Remain indoors and seek shelter under strongly constructed tables, desks or door frames
- Keep away from windows, fixtures, furniture, and items that may become unstable
- Evacuate the premises if it is safe to do so.

If you are outdoors:

- Move quickly away from buildings, electrical structures and flammable products
- Proceed to designated assembly area if safe to do so.

After the earthquake:
- Check attendance at assembly area against the attendance registers
- Respond to injured people
- Check for gas leaks, power failure and any other hazard
- Turn off electricity, gas and water if it is safe to do so
- Prevent entry to premises if unsafe
- Contact and liaise with emergency services if required
- Notify CC/DCC or ACC DM.

Checklist #09: Flood

In the event of a flood:
- Do not enter the flood waters
- Eliminate potential electrical hazards
- Place high value equipment and records away from impending floodwaters if it is safe to do so
- Stay in a safe location while it continues to offer protection
- Evacuate staff, members and visitors as for the above evacuation procedures.
- Contact and liaise with emergency services if required
- Notify CC/DCC or ACC DM.

Checklist #10 : The Evacuation "GO BOX"

The "Go Box" contains copies of important documents essential for the business to continue to operate. It should be stored in a fire-proof secure container/cabinet in an alternate location. Below are recommended items; however, each business unit should discuss and specifically designate the contents of their "Go Box".