Section 15 – Managing Risks and Protecting Vital Records

Contents

Main Things to Remember about Managing Risks and Protecting Vital Records

- Your vital records will be small in number.
- Identify them and protect them.
- Remember to exchange older security copies for current versions as necessary.
- Have a plan for accessing the security copies in the event of an emergency – and practice it.

Introduction

UN Policy on Vital Records

ARMS recommends that all UN departments, field missions, offices away from HQ and other UN identities which contribute to the UN recordkeeping system should have a system in place to manage vital records so they are safe and available in the event of a disaster or emergency. The system should include:

- Senior management authorisation and support of the vital records programme
- Designation of a staff member (ideally an Information Management Officer) who is responsible for implementing the policy
- A register of those records which are vital to the office's continued operation as well as those records which are vital to the UN's continuing operation and credibility in the event of an emergency
- Identification, analysis and management of the whole range of risks posed to the office's records
- A plan and procedures to protect vital records which takes into consideration the cycle of currency and allows for the on-going maintenance of the protection programme
- A set of plans for the recovery and reconstruction of vital records in the event of a disaster
- Regular review of the vital records register and the vital records management programme

Managing vital records management is the part of the recordkeeping programme which ensures that those records which are crucial to continue operations are identified and available in the event of a disaster. All UN field missions and offices should develop procedures to identify and manage their vital records as part of overall disaster recovery and business continuity planning. The plans of individual units should be unique to their precise range of business functions and specific to the local geography. However, the local plans should be consistent with and complementary to the UN's greater overall disaster recovery and business continuity planning. This section deals primarily with the vital records and disaster planning that you need to do at the local level. In managing your vital records you must collaborate with ARMS and with the appropriate staff in CITS or ITSD to ensure that you comply with the aims and procedures of the UN's Disaster Recovery Planning.

Vital Records Plan

A vital records plan sets out how vital records are protected prior to a disaster and how, if there is a disaster, they can be accessed. You need to have in place a number of elements which come together to make a comprehensive plan. These elements are covered in detail in this section of the Toolkit, they are:

- Identification of your vital records
- Identification of disaster types you need to protect them from
- Deciding on a strategy for protecting your vital records
- Planning the procedures for accessing vital records in the event of a disaster

You need to develop these four elements into a formal written plan for your team. The plan needs to be cleared with your management as well as with ARMS. Your team must be familiar with the plan and their roles and responsibilities for both maintaining the vital records management programme and for implementing the plan in the event of an emergency or disaster. The checklist Constituents of a Vital Records Plan at the end of this section below gives details of what the plan should include.

You will also need to test your plan and if necessary amend it in the light of how it performed in the test. You'll also need to periodically re-survey your vital records to ensure that new or changed record series are covered.

Identifying your Vital Records

The first step in establishing a vital records programme is to identify the records that your field mission or office needs in order to:

- continue to operate under other than normal conditions
- protect the rights of the UN and its staff
- protect the rights of individuals directly affected by UN actions

A good way to begin to identify your vital records is by identifying your unit's most crucial business functions. These will fall into two broad categories: the functions that need to be carried out to restore minimal operations, and the functions that have to continue to meet UN obligations and primary goals. In assessing the work of your office you must involve operational staff (your colleagues), but remember that decisions about crucial functions are essentially strategy and policy decisions and should be taken by your senior management in consultation with ARMS and the UN Business Continuity team.

Once the crucial functions have been identified, you can identify the records that support those functions. You will also need to identify what date span the records need to cover to ensure that in the event of an emergency you have all the records you need but no more. Some vital records will have limited currency, for example staff contact lists, so you need to ensure you have the most up to date version. Remember that vital records may be originals or copies, for example a directive from UNHQ which is vital to the establishment and maintenance of a field mission. You will be looking to keep the number of vital records to the bare minimum required for the resumption of operations – remember that at some point following an emergency or disaster you will be able to access copies of many records from other UN entities and from UN stakeholders.

Remember that:

- most of your vital records will probably be active, because you will need access for vital on-going operations
- it may also be necessary to specify the originals of some records as vital for legal reasons (e.g. contracts for which only the original provides proof of the agreement)

Only 2-4% of an organisation's records are likely to be vital and if you don't keep your vital records programme concise it will become difficult to manage.

You can gather this data on your vital records in a simple form such as the one below:

Vital Records Survey Form

Responsible Official:

Title:

Unit:

Section:

Office / Division:

Department:

Record series title	Function supported	Required for restoration ☑	Required for continuation ☑	Master or copy	Medium	Location of master if not held	Cycle of Currency	Volume

Some Examples of Vital Records

In identifying your vital records, ensure you include all, and nothing but, the ones which are crucial to starting and effectively continuing the field mission's or office's work. You are looking for records which support mission-critical operations but remember this will be specific to your field mission and office as the selection of vital records depends on the nature of the mission, its current phase of operations, and its functions and responsibilities. You may also need to think through whether the records you would need in the event of an emergency might depend upon the nature of the emergency/disaster itself. You are looking therefore for all key documents which are still active, or those which are inactive but which are required for continuity of an essential business process. For UN field missions this will broadly include:

- Records of territorial boundaries and demarcations
- Multilateral treaties
- Memoranda of understanding
- Medical and personnel files of international and locally-recruited civilian staff, police and military observers
- Records necessary to protect legal and financial status
- Records necessary to preserve the rights and obligations of citizens
- Records held in trust to preserve the rights and obligations of citizens
- Records identified as necessary to protect UN assets
- Financial records which facilitate continuing solvency and accounting/finance functions (records of monies owing, account status and statements, account access authorities, current staff payroll and benefit details, records allowing access to emergency funding)
- Records which authorise and support the field mission's most fundamental responsibilities and essential activities (policy documents, contracts, ownership records, delegations and authorisations, directives/instructions from UN HQ, records relating to the establishment or structure of the office, records which amend, repeal, or revoke policy/authorisation records, key source documents in the operational framework, such as deeds, agreements with host country and local government organisations)
- Some records of an administrative nature (key operating procedures, licences, permits, timetables, insurance policies)
- Records relating to buildings, doors, safes, sprinklers, alarm systems; personnel lists; building plans; evacuation plans, security clearance records)
- Vital objects which are needed in an emergency, but which are not hardware (e.g. building keys)

Once you have identified your vital records you should enter them into a register or document them in some way so that the whole team knows which records are vital, who creates them, how they are protected and how they can be accessed in an emergency. The checklist Identifying Vital Records at the end of this section will help you in this task.

Identifying Records Vital to the UN

Some of your records may be vital to the UN's overall business continuity. In this case, ARMS and the UN Business Continuity team will work with you to ensure those records are identified and a protection and recovery plan is in place.

Defining and Planning for Disasters

In planning to protect your vital records, you must think through the kinds of disaster and emergency that could potentially affect your team and its work. The difference between an emergency (not to be confused with the kind of humanitarian emergencies that the UN deals with) and a disaster is primarily scale. You could probably deal with an emergency without additional financial or human resources. A disaster will require money, personnel with specialised skills and contracted services to recover from.

Although missions should have an overall plan and procedures for dealing with emergencies and disasters, we are primarily concerned here with mitigating the impact of a disaster on recordkeeping. The first thing you need to do is identify the potential risks to your office's records. Examples include:

- Sustained power cuts
- Civil insurrection
- Peaceful demonstration
- Outbreak of military conflict
- Natural disaster (flood, adverse weather, earthquake etc)
- Man-made disaster (fire, explosions, terrorist attack)

Once you have identified the sort of risks that are possible, you can begin to assess their likelihood and map out a scenario which will help you to mitigate their impact on recordkeeping and the work which relies upon the records. You should also think this through from the perspective of what work needs to be done in the immediate aftermath of the emergency or disaster and which records are needed to support it.

For example, if you suffer sustained power outage and you have no generators you will have difficulty in accessing computer records. It may be that there are paper copies of the records which can support your team's work whilst the power problem is addressed. However, if you have complex computer records such as databases, financial systems etc. they are unlikely to be copied in their entirety onto paper. You will need to think which parts of those records are needed in the short term to support the field mission's work and decide whether it is feasible to print out portions of the system or database. For example, the recent accounts which give income, expenditure and account balances. In this scenario only a small portion of your vital records will come into play.

Another example is the kind of disaster where you and the team are not able to access any records because the office is inaccessible due, for example, to military action or adverse weather conditions. In this scenario you will need to make arrangements for copies of the vital records to be available elsewhere.

You can use the table Risk Identification and Assessment Tracking at the end of the section to help you map out the various risk scenarios and to identify the type of plan(s) that you will need to have in place to deal with each kind of disaster or emergency. Although you need to have a set of procedures in place for each possibility, many of the elements will be the same or similar so you are in effect picking and mixing from a finite pool of actions.

The table is not exhaustive, and you will also need to consider whether your field mission/office is vulnerable by nature of your work. For example, if there is any particular reason that the UN, or the particular UN function which is being carried out, is unpopular and might be deliberately targeted by certain factions. You also need to consider technical vulnerability. Reliance on technology is a risk for any organisation but you need to think to what degree your operation relies on technology and how technological failure will affect your work.

The Toolkit section Emergency Preparedness for a Mission Records Storage Facility gives full details on how to develop, maintain and implement a disaster recovery plan.

Protecting Vital Records

Once you have identified and registered your vital records you need to work out how to protect them in case of a disaster or emergency. There are a number of options for protecting vital records:

- Preventative measures
- Heavy-duty protection to originals on-site
- Relying on computer back-ups

You may decide you need to have a range of measures in place to protect your vital records. You will certainly want to combine preventative measures with at least one of the other options. Another factor which has a bearing on which method you choose is whether the vital records are frequently referred to or if they are less current but need to be kept to provide evidence of rights or responsibilities.

Preventative Measures

It is good recordkeeping practice to ensure that all records, not just vital records, are secure and as protected from possible threats as is reasonably possible. Hopefully, most measures will already be in place, but it is good practice to audit the situation on a regular basis to ensure that you are taking all possible care to ensure that no preventable disaster occurs. You can use the checklist of preventative measures given at the end of this section to identify which are most applicable to your mission and to ensure that you have the necessary measures firmly in place.

Extra Protection for Master Vital Records On-site

Even if you have good disaster prevention measures in place, you should also have a way of protecting vital records. You may decide that protecting masters or originals in your office is the only viable option. In that case you need to think how you can give vital records additional or optimal protection. This might include:

- Locking vital records (of any media) away in a safe or at least a lockable cupboard or desk drawer
- Storing vital records (of any media) in fire-proof safes, or at least in something that affords additional protection from fire
- Storing vital records (of any media) in bomb-proof storage

Remember that all vital records will have a fairly limited currency and they need to be regularly replaced with the up to date version. You need to include this in your procedures.

Relying on Computer Back-ups

Many vital records will be created or received in digital formats and be subject to the ITSD or CITS regime of backing up in case of system failure. It is possible to rely on these back-ups in the event of an emergency but you must remember that the aim of a back-up system is to enable them to reconstruct the whole of the system in the event of computer system failure. Their priorities are not to restore the small number of vital records and it may not be possible for them to identify and isolate your vital records as a matter of priority. However, if your team decides that this is the only option for protecting your vital records, you should work with ITSD to agree on priorities for restoration of the system and records so that the vital records are accessible as soon as possible. This may mean maintaining a store of copies of the vital records discretely so they can be easily identified and restored in the event of a disaster.

It is also important to remember that all digital records require not just the records themselves but also operating systems and application software in order to access them in case of an emergency so systems data and/or software will also need to be protected and made available.

Copying and Dispersing to another Location

The most reliable and effective way of protecting vital records is by copying them and dispersing (or sending) them off-site to another controlled location. If you can identify and control a location that is far enough away from your office, but can be accessed in the event of an emergency, you should opt for this method of protection.

Information Box

Requirements for Controlled Location away from Office

The location and premises must:

- Be secure from access by all but authorised personnel
- Have the same rigorous disaster prevention measures that are in place in your office accommodation
- Be able to accommodate storage of vital records in the full range of media that you require
- Protect the records from adverse environmental conditions for their whole lifetime (which may be quite short but may also be very long)
- Afford access to vital records regardless of medium
- Allow internet, telephone and other communication methods

Ideally the vital records storage facility should be owned and managed by the UN but if this is not possible the contractor should be carefully vetted and the contract should carefully specify ownership of records, storage conditions and security as well as requirements for access to and restoration of the records in the event of a disaster.

When establishing your vital records dispersal programme, you need to take into consideration the possibility that some types of record are routinely copied and dispersed as part of the UN or your office's everyday work. The ITSD computer back-up programme has already been discussed but there are other records which may be sent to other UN departments, field missions, organizations or even member states, copies of which could be obtained within an acceptable timeframe in the event of a disaster. Use the checklist below to ensure all records on your vital records list or register are adequately protected.

Information Box

Copying and Dispersing Vital Records

For each vital record/record series ensure that at least one of these actions must be in place:

- It is backed up regularly and is it readily accessible in the event of a disaster
- A copy is sent to UNHQ/DPKO
- A copy is sent to the host member country or other friendly stakeholder
- The original is with UNHQ/DPKO
- The original is with the host nation or other stakeholder
- Staff have copies on laptops or other storage such as digital media or paper files which are usually kept out of the office

If copies are routinely made and stored elsewhere than the office, it is possible to put in place some procedures which ensure that copies are made and protected and that they can be restored and accessed in the event of a disaster. Although this option may seem very attractive as it is not going to be as resource demanding as a separate vital records copying and dispersal programme, it may not be effective or reliable enough.

Use the checklist Copying and Dispersal Information Required for Vital Records at the end of the section to ensure that you have adequate copying and dispersal information for each vital record/record series identified in the register.

Copying and Dispersal Programme Procedures

Procedures for the copying and dispersal programme need to include:

- Set schedules for copying and transporting vital records off-site which are monitored to ensure these tasks are carried out promptly and diligently
- Secure transportation from your office to the off-site facility; drivers should sign in and out
- Tracking copies that are sent off-site, labelling them clearly to indicate the number/amount, the date of transfer, a reference to relate them to the vital

record register, whether the record is an amendment to a record already off-site (and which record) and the office of origin (this could be done via a transfer form)

- Issuing a receipt which matches the transfer form and is signed to confirm that the record(s) arrived off-site
- The form should include room to indicate any necessary action concerning expired vital records (e.g. destruction) which could be confirmed with a signature when it is done
- A master inventory of all vital records that are off-site
- A copy of the inventory needs to be kept safely, but available for reference by the office in the event of an emergency
- Removing records from off-site storage as they cease to be vital and updating the inventory accordingly
- Ensuring that vital records are destroyed in accordance with the retention schedule pertaining to originals.

Emergency Operation Sites

Your mission will have a contingency plan for emergency situations. Your mission Information Management Officer needs to ensure that the records perspective is clearly included.

In the event of a disaster you may not be able to operate in your office so you need to make some arrangements for alternative premises. It may be possible to use the same premises as are used to store your vital records, or you may be able to find something else that is suitable far enough away from the office in case the area affected by the disaster is fairly large. At the very least you should approach real estate agents so they know your requirements if you need to find somewhere at short notice. If you are able to have alternative premises standing ready, there are two ways of fitting them out:

1. A working duplicate of all systems and equipment, known as a hot site. This can be run by a commercial organisation, such as specialists in disaster recovery services
2. An empty shell with utilities, air conditioning and communications lines; a place where compatible equipment and systems can be made available to read and process vital records. This is known as a cold site and again can be run by a commercial organisation

In the Event of a Disaster

If you are unlucky enough to suffer a disaster and you have no disaster plan in place, shock may well prevent you from operating efficiently. A disaster plan will save you time because you ensure that you can respond as you will have information and resources at hand to get up and running again.

Information Box

Action in the Event of a Disaster

In the event of a disaster:

- Access a copy of the emergency plan
- Confirm that the office is now acting under emergency conditions (this should be confirmed by senior management)
- Gather the disaster team together and decide what recovery scenario is required depending on the nature of the disaster
- Contact staff to ensure all are safe and to tell them what they need to do
- Set up an emergency operations site
- Recall (and if necessary reconstitute) vital records and ensure that they are issued to appropriate staff
- Ensure that the office is structurally sound and it is safe to return
- Depending on the nature of the disaster, make arrangements to salvage any non-vital records

☑ Checklist: Constituents of the Vital Records Plan

- □ The vital records policy
- □ Objectives, justification and scope of the programme
- □ Details of roles and responsibilities
- □ Organisational chart and staff contact details
- □ Details of the vital records register
- □ The vital records programme: details and procedures for protecting vital records (including preventative measures, cycles of currency etc), storage requirement and locations (including contact details), together with any forms and other documentation
- □ Details and procedures for retrieving, restoring and salvaging vital records as necessary in the event of a disaster, together with any forms and other documentation
- □ Specifications for equipment requirements
- □ Details of an emergency operations centre if the office is not accessible/usable
- □ Specific scenarios for different types or intensity of disaster
- □ Details of the review and audit cycle

☑ Checklist: Identifying Vital Records

- □ Identify the functions that need to be carried out to restore minimal operations
- □ Identify the functions that are required to continue to meet UN obligations and primary goals
- □ Identify record series which support crucial functions
- □ Specify currency cycle for each vital record series
- □ Consult operational staff
- □ Gain senior management support and input into strategic and policy issues
- □ Consult ARMS
- □ Consult UN Business Continuity team
- □ Specify whether original or copy of record is created elsewhere in UN

☑ Checklist: Disaster Prevention Measures to Protect Vital Records

Measure	Tick	Notes
Staff Awareness and Training:		
Train staff to be aware of threats to vital records	□	
Train staff in preventative measures to protect vital records	□	
Ensure that new staff are properly trained to follow vital record protection procedures and to ensure unnecessary disasters are prevented	□	
Security (Facilities):		
Establish good locking up procedures	□	
Install automatic security alarms	□	
Install locks on all doors, windows and skylights	□	
Install bars and/or toughened glass around windows	□	
Conduct regular facility and security inspection of records storage areas, including off-site inactive and vital records facilities	□	
Control all building keys	□	
Supervise non-staff in building	□	
Security (IT):		
Lock rooms with computers at night	□	
Ensure good, up to date fire wall is in place	□	

☑ Checklist: Disaster Prevention Measures to Protect Vital Records

Measure	Tick	Notes
Ensure good, up to date virus protection is in place	□	
Limit access to computer systems with passwords	□	
Use data encryption where necessary/appropriate	□	
Use auxiliary generators and surge protectors	□	
Employ due care when handling floppies, tapes etc	□	
Fire:		
Ensure compliance with all fire regulations	□	
List and ensure all flammable liquids in separate, locked metal cabinets or store rooms	□	
Keep storage areas clean and tidy	□	
Ban smoking in areas where records are kept or used	□	
Check electrical wiring regularly	□	
Appoint a staff fire warden and devise a fire safety plan	□	
The local authority fire officer should tour with fire prevention staff to point out vulnerable areas	□	
Discuss how best to protect/salvage records in event of fire	□	
Install fire alarms, smoke detectors and heat detectors as appropriate	□	

☑ Checklist: Disaster Prevention Measures to Protect Vital Records

Measure	Tick	Notes
Drill staff in raising the alarm and evacuation procedure	□	
Ensure that shelving is strong, stable, non-flammable (including paint)	□	
Flood:		
Mains supply, heating and drainage water pipes should not cross areas where records are stored	□	
Roofs should be pitched, not flat	□	
Flood alarm systems should be installed	□	
Check water penetration points regularly	□	
Inspect and maintain gutters and drains	□	
Check humidity levels regularly – a rise can mean water penetration	□	
Ensure taps are always turned off	□	
Turn off water at mains when the building is not occupied, with an automatic over-ride for fire	□	
Use good quality, well-made boxes and other equipment for storage: make sure that highest shelves are not used for storage but act as a roof (to protect the records from water)	□	
Bottom shelf should be 6” (15cm) above the floor (to minimize water damage caused by flooding)	□	
Storage:		
Don’t store records in basements (prone to flooding) or top floors (can be	□	

☑ Checklist: Disaster Prevention Measures to Protect Vital Records

Measure	Tick	Notes
excessively hot in summer and risk of leaks).		
Building work on own or neighbouring buildings, office moves etc (periods of high risk to records)	□	
Liaise with building contractor to obtain clear picture of work undertaken	□	
Check insurance - both builders and UN office's	□	
During roof repairs protect records with polythene sheeting	□	
Check for blocked drains if demolition work occurs adjacent to your building	□	
If moving use own staff as much as possible	□	
Protect records while waiting to move/be put away – e.g. raise off floor onto pallets, cover	□	

☑ Checklist: Copying and Dispersal Information Required for Vital Records

- □ Details of the method of copying (remember that the copy does not need to be in the same medium or format)
- □ Procedures for copying which include validation of copies to ensure reliability in case they are relied upon as records/evidence of actions and decision
- □ Frequency of copying and dispersal
- □ How often the record needs to be replaced by a more current record
- □ What procedures are in place to destroy copies when they are no longer vital
- □ What equipment, software, hardware etc is needed to restore and access the records and what contingency arrangements are in place to obtain it in the event of a disaster
- □ Any special security/access mechanisms that need to be in place to protect sensitive or personal records

Table: Risk Identification and Assessment Tracking

Type of disaster or emergency likely to occur	Type of plan required			Vital records identified	Vital Records Restoration Plan in Place
	Severely affects field mission/ office (backup site required for operations)	Affects field mission/ office to degree that normal operations are disrupted	Impact such that field mission/ office can cope without major emergency/ disaster outlay		
Natural causes: Fire					
Water/chemicals used to extinguish fire					
Flood					
Volcanic eruptions					
Earthquakes					
Tornadoes					
Heavy storms					
Snow					
Lightning					
Hail					
Cyclones/high winds					
Tidal waves					
Electrical storms					

Table: Risk Identification and Assessment Tracking

Type of disaster or emergency likely to occur	Type of plan required			Vital records identified	Vital Records Restoration Plan in Place
	Severely affects field mission / office (backup site required for operations)	Affects field mission / office to degree that normal operations are disrupted	Impact such that field mission / office can cope without major emergency / disaster outlay		
Insect invasions					
Building or equipment failure or malfunction: Leaky roofs					
Broken pipes					
Defective wiring/switches					
Faulty machinery/equipment					
Broken heating/cooling systems					
Electrical outages and malfunctions					
Acts of deliberate destructiveness: Theft					
Espionage					
Vandalism					
Terrorism					

Table: Risk Identification and Assessment Tracking

Type of disaster or emergency likely to occur	Type of plan required			Vital records identified	Vital Records Restoration Plan in Place
	Severely affects field mission / office (backup site required for operations)	Affects field mission / office to degree that normal operations are disrupted	Impact such that field mission / office can cope without major emergency / disaster outlay		
War					
Public disorder					
Human error, carelessness: Smouldering cigarette					
Open window					
Unattended stove					
Negligent storage of flammable chemicals					
Careless computer key stroke					
Misfiling					
Unauthorised access due to inadequate security					
Misuse					
Alteration					

Other Relevant Toolkit Sections

- Section 13 – Emergency Preparedness for a Mission Records Storage Facility

Forms

- Vital Record Survey Form

Glossary

Business Continuity: the process of assessing likely disasters which are a risk to the business and putting together a plan to mitigate those risks. Vital records management and disaster planning are part of business continuity.

Disaster: an unexpected and negative event, man-made or natural, or a combination, that damages the organisation's assets (information, property etc) and ability to operate normally.

Disaster recovery: the operation of restoring record collections and related operations after a disaster.

Emergency: an unexpected adverse event that causes limited localised damage and requires staff to carry out procedures outside of everyday duty parameters to prevent further damage and recover or rehabilitate assets.

Vital Records: those records which, in the event of a disaster, are essential for the recovery of vital operations and the ongoing business of an organization. Without its vital records the organization cannot function effectively.

Vital Records Programme: a management regime for vital records which includes preventative and protection measures and procedures, retention requirements and locations, staff and service provider contact details together with documentation.

Frequently Asked Questions (FAQs)

What is a Disaster Recovery Plan?

A written plan (sometimes called an Emergency Plan) which sets out:

- the precautions and procedures to minimise the risks and effects of natural and man-made disasters such as fire, flood, earthquake, terrorism etc.

- the steps to be taken to resume business in the event of a disaster

the personnel, equipment and processes necessary to recover, secure and make available the vital records in the event of disaster.

What about our archives? Aren't they vital records?

Record series which your retention schedule designates for permanent retention in the UN Archives are not necessarily vital records, although more current portions of them may be. Nevertheless, you should also be looking to protect your archival records, and more detail on how to do this is given in the Toolkit section Emergency Preparedness for a Mission Records Storage Facility.

What is the difference between an emergency and a disaster?

An emergency is an unexpected adverse event that causes limited localised damage and requires staff to carry out procedures outside of everyday duty parameters to prevent further damage and recover or rehabilitate assets. Examples include broken water pipes, computer crashes and power cuts. A disaster is much more serious and debilitating than an emergency. It is an unexpected and negative event, man-made or natural, or a combination, that damages the UN's assets (information, property etc) and ability to operate normally. Examples include a fire which destroys the premises and contents, a hurricane which prevents the facility from being used for an extended period of time, civil disturbance or military action which prevents access to the office.