"The City of Heritage"

ULUNDI
MUNICIPALITY

# INFORMATION TECHNOLOGY

# Physical and Environmental Security Policy

## Table of Contents

# 1. Introduction

The term physical and environmental security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Physical and environmental safeguards are often overlooked but are very important in protecting information. Buildings and rooms that house information and information technology systems must be afforded appropriate protection to avoid damage or unauthorised access to information and systems. In addition, the equipment housing this information (e.g. filing cabinets, data wiring, laptop computers, portable disk drives, etc.) must be physically protected. Equipment theft is of primary concern, but other issues should be considered, such as damage or loss caused by fire, flood, and sensitivity to temperature extremes.

# 2. Objectives

The goal of the Physical and Environmental Security Policy is to ensure the prevention of unauthorized physical access, loss, damage or interference to Ulundi Municipality's premises and infrastructure, or interruptions to its critical operations, using physical and environmental controls appropriate to the identified risks and the value of the assets protected. As such, the main objectives of this policy are to:

i) To prevent unauthorised access, damage and interference to business premises and information.
ii) To prevent loss, damage, or compromising of assets and interruption to business activities.
iii) To prevent compromising or theft of information and information processing facilities.

# 3. Scope

This policy applies to aall individuals within the Ulundi Municipality that are responsible for the installation and support of information resources, individuals charged with information resources security, and data owners.

## 3.1. Policy and Procedures

### 3.1.1. Physical Security Controls

- Security policy applies to full and part time employees, contractors, vendors, consultants and externally employed people who require Server Room access

- It is essential that critical information is housed in secure areas, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference, commensurate with the identified risks.
- The following guidelines and controls will be considered and implemented where appropriate:
- Security perimeters are to be clearly defined.
- A manned reception area or other means to control physical access to the site or building should be in place.

- The server room shall be kept locked by the IT Manager and the Systems Administrator, and the keys shall be kept as follows:

    - One set in the strong room in the Off-site storage location, Civic Centre;
    - One set with the IT Manager;
    - One set with the Financial Manager and Chief Financial Officer

- Access to sites and buildings should be restricted to authorised personnel only.
- Visitor's time of entry and exit to secure areas recorded.
- Access rights to secure sites will be reviewed and updated regularly.

### 3.1.2. Securing Offices, Rooms and Facilities

a. A secure area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes. The selection and design of secure areas must take into account the possibility of damage from fire, flood, explosion, civil unrest, and other forms of natural or man-made disaster. Consideration must also be given to any security threats posed by neighbouring premises, i.e. leakage of water from other areas.
b. Fallback equipment and backup media must be sited at a safe distance to avoid damage from a disaster at the main site.

### 3.1.3. Equipment Siting and Protection

a. Equipment must be sited or protected to reduce risks from environmental threats and hazards, as well as opportunities for unauthorised access.

b. Protection of equipment (including that used off-site such as notebook computers for example) is necessary to reduce the risk of unauthorised access to data and to protect against loss or damage.

c. As such, the following controls must be considered:

- Equipment must be sited to minimise unnecessary access into work areas.
- Controls must be adopted to minimise the risk of potential threats including:
  - Theft
  - Fire
  - Explosives
  - Smoke
  - Water (or supply failure)
  - Dust
  - Vibration
  - Electrical supply interference (or supply failure)
- Smoking is generally covered by applicable legislation- where this may be interpreted as not being applicable; smoking in the proximity of information processing facilities is expressly prohibited.
- Over and above provisions that may be contained in the conditions of service, the use of alcohol (or other forms of substance abuse in secure areas or in the proximity of information processing facilities is expressly prohibited.
- Consumption of food or beverages in secure areas or in the proximity of information processing facilities should be discouraged where possible.
- Other items prohibited from the Server Room:
  - Combustible materials such as paper and cardboard (except reference manuals as needed)
  - Explosives and weapons
  - Hazardous materials
  - Alcohol, illegal drugs and other intoxicants
  - Electro-magnetic devices that could cause interference with computer and telecom equipment
  - Radioactive materials
  - Photographic or recording equipment (other than backup media)

### 3.1.4. Power Supplies

a. Key equipment must be protected from power failures and other anomalies. A suitable electrical supply conforming to the equipment manufacturer's specifications must be assured. To do so may require one or more of the following:

- Multiple feeds to avoid a single point of failure in the power supply,
- Uninterruptible Power Supply (UPS), and/or
- Backup generation facilities.

b. A UPS to support orderly shutdown or continuous running is necessary for equipment supporting business-critical operations. Contingency plans must cover the action to be taken in the event of failure of the UPS. UPS equipment must be regularly checked to ensure adequate capacity and tested in accordance with the manufacturer's recommendations.

c. Emergency power switches must be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting should be provided in case of main power failure. Lightning protection may be necessary in certain buildings and lightning protection filters should be fitted to all external communications lines.

### 3.1.5. Generator

A backup generator should be considered if processing must continue in case of prolonged power outage. If installed, procedures must be implemented to regularly test generators in accordance with the manufacturer's recommendations. An adequate supply of fuel should be available to ensure that the generator can function for prolonged periods. Due consideration must be taken when sitting such facilities, particularly with regard to fuel supply and replenishment thereof, to minimise possible risks to information processing facilities.

### 3.1.6. Cabling Security

a. Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.

b. As such, the following controls should be considered:

- Power and telecommunications lines into the Server Room should be underground, where possible, or subject to adequate alternative protection.

- Network cabling should be protected from unauthorised interception, or damage, through (for example) the use of conduit or by avoiding routes through public areas.
- Power cables should be segregated from communications cables to prevent electromagnetic interference.
- Cables should be clearly marked and neatly arranged in cable racks.

### 3.1.7. Air Conditioning

- Air conditioning is provided throughout the room. The temperature in the Server Room should not go below 10°C (50°F) or above 28°C (82°F) in accordance with best practice. Use good quality racks to protect equipment, maximize efficient use of space, and support the efficient distribution of chilled air.
- Humidity in server rooms should be between 40% and 60% rH. Too dry will result in the build-up of static electricity on the systems. Too humid and corrosion will start slowly damaging your equipment resulting in permanent equipment failures.

### 3.1.8. Dust Prevention

- The Server Room should remain dust free at all times, therefore packing or unpacking of equipment should take place outside the room. Items can be unpacked in another room prior to introduction into the computer room with the help of staff.
- Cardboard and other items that can generate dust and are easily combustible should remain outside the Server Room. Waste bins are available throughout the Server Room for all other items of waste.
- The Server Room should be cleaned on a weekly basis every.

### 3.1.9. Fire Detection and Fire Extinguishers

- The Server Room should be fitted with a fire detection system linked to audible and visual alarms (colored red) placed throughout the Server Room. If an alarm is activated leave the room immediately at the designated exit points and exit the building. Users should then go the designated meeting point. For small incidents fire extinguishers are placed throughout the Server Room alongside instruction signs.
- FM200® gas can be used in fire extinguishers. It is a colorless gas which is liquefied under pressure for storage, it has a low toxicity level and is super-pressurised with Nitrogen to 24.8bar (360psi) which makes it safe for use in the fully automatic mode in occupied areas. It rapidly extinguishes most commonly found fires through a combination of chemical and physical mechanisms. FM200® is immediately available

to protect most hazards. It is effective in the protection of data processing, telecommunications and electronic equipment as well as most flammable liquids and gases.

### 3.1.10. Equipment Maintenance

a. Equipment must at all times be correctly maintained to ensure continued availability and integrity, compliance with warranty provisions and protection of the municipality's investment.
b. As such, the following controls must be considered:

- Equipment must be maintained in accordance with the manufacturer's recommendations according to the manufacturer's recommended service intervals and specifications.
- Only authorised maintenance personnel may carry out repairs and service equipment.
- Records should be kept of all suspected or actual faults and all preventive and corrective maintenance.
- Appropriate procedures and controls must be applied when equipment leaves municipal premises for maintenance (in particular, the confidentiality and security of data that may be stored in the equipment must be considered). Also, stringent recording procedures must be applied in order to track the whereabouts of the equipment.

### 3.1.11. Environment Monitoring

A number of monitoring equipment should be put in place to report on issues affecting the Server Room environment. These include:

- **Ambient room monitoring**

  - Ambient room monitoring is the environmental monitoring of the room for its humidity and temperature levels. Temperature and humidity sensors are typically deployed in: potential "hot zones" inside the server room and near air conditioning units to detect failure of such systems.
  - Smoke and Fire environmental monitoring in the server room is also essential.

- **Water & Flooding Monitoring**

- Water leakage is a less known threat for server rooms. The fact that most server rooms have raised floors makes the risk even bigger as water seeks the lowest point.

- **Rack Level Monitoring**

  - American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends no less than 6 temperature sensors per rack in order to safeguard the equipment (top, middle, bottom at front & back of rack).

- **Network and Application Monitoring**

  - Whilst intrusion detection from network traffic from an outside source is very important, there is also a need for network monitoring. Network monitoring software can send alerts when the network goes down or becomes unavailable from hardware failure.

### 3.1.12. Secure Disposal or Re-Use of Equipment

a. Information security can be compromised through careless disposal or re-use of equipment. Storage devices containing sensitive information should be physically destroyed or securely overwritten, rather than simply using the standard 'delete' function which effectively resets the file size to zero without destroying the data.
b. In cases of extreme sensitivity, it may be necessary to overwrite the disk up to seven times to ensure that the data is irrecoverable.
c. Final disposal of information processing equipment, in common with all municipal movable assets, is subject to the provisions of any other applicable policies and/or procedures.

### 3.1.13. General Controls

Information and information processing facilities must be protected from disclosure to or modification by unauthorised persons, or theft. Effective controls must be implemented to minimise the risk of loss or damage.

### 3.1.14. Clear Desk and Clear Screen Practices

a. It is recommended that "clear desk" and "clear screen" practices become the norm at all municipal premises, so that removable media and information contained in paper reports are not visible or accessible to unauthorised persons. Information storage

media left on desks is also more likely to be damaged in the event of a disaster and to reduce the risk of unauthorised opportunist access to facilities.

b. The following controls should be considered and implemented where appropriate:

- Paper documents and computer media should be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside of working hours.
- Sensitive or critical business information should be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.
- Personal computers and computer terminals must not be left logged on when unattended and should be protected by key locks, screensavers with passwords or other controls when unattended.
- Personal computers and computer terminals must not be left switched on overnight. The normal switch on and “boot up” process also carries out certain housekeeping functions that are necessary for optimum functioning.
- Sensitive or classified information, when printed, should be cleared from printers immediately. Persons who regularly need to print such documents should consider a personal printer rather than using shared facilities, where appropriate.

#### 3.1.15. Removal of Property

a. Equipment, information or software must not be taken off-site without proper authorisation.
b. Where necessary and appropriate, equipment should be logged out and logged back in when returned.

## 4. Enforcement

Non-compliance, violation and disregard of this policy by any Ulundi Municipality employees, consultants and temporary staff shall result in disciplinary action and sanctions against the individual concerned and such sanctions may lead to termination of the individual’s employment contract, depending on the circumstance and the gravity of the transgression. In the event of Ulundi Municipality incurring financial loss as a result of non-compliance, violation and/or disregard of this policy, Ulundi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the individual and this shall be in addition to the disciplinary action that Ulundi Municipality would have taken against the individual.

## 5. Approvals

The table below provides necessary approvals of this policy.

| Approver | Signature | Date |
|---|---|---|
| Chairman of the Council | | |
| Chairman of the Audit and Risk Committee | | |
| Ulundi Municipal Manager | | |