CAPE WINELANDS DISTRICT
MUNICIPALITY • MUNISIPALITEIT • UMASIPALA

# PHYSICAL ENVIRONMENTAL SECURITY POLICY

**POLICY ADOPTED BY COUNCIL ON 25 JULY 2013**
**AT ITEM C.14.1**

## Table of Contents

1. INTRODUCTION .......... 3

2. ACCESS .......... 3

   2.1 Restricted/Sensitive .......... 3

   2.2 Operational .......... 4

3. USAGE .......... 4

   3.1 Restricted/Sensitive .......... 4

   3.2 Operational .......... 4

4. PHYSICAL SAFEGUARDS .......... 4

   4.1 Restricted/Sensitive .......... 4

5. RECORD KEEPING .......... 5

   5.1 Restricted/Sensitive .......... 5

6. CONTINGENCY .......... 5

   6.1 Restricted/Sensitive .......... 5

7. GUIDELINES .......... 5

## 1. INTRODUCTION

1.1 The security and environment surrounding the server room must be of the highest standards and consistency.

1.2 The equipment in the server room are –

1.2.1 Sensitive to environmental issues.

1.2.2 Affected by temperature, moisture and dust, just to mention a few.

1.2.3 Valuable for both their replacement cost and the critical services they deliver.

1.2.4 Represent one of the major risk/opportunities of the Cape Winelands District Municipality (CWDM) and equivalent contingency plans.

1.3 The security and environmental issues are dealt with from two perspectives, namely restrictive/sensitive and operational. Striking a balance between these two items manages the risks while promoting efficient and consistent operations.

## 2. ACCESS

### 2.1 Restricted/Sensitive

2.1.1 New or refurbished server rooms will be locked at all times using a programmable locking mechanism capable of being monitored remotely.

2.1.2 Access to the server room will be restricted by key, code or electronic card.

2.1.3 An auditable process for issuing keys, codes, and/or cards shall be documented.

2.1.4 If keys are used, it will be stamped "*Do Not Duplicate*".

2.1.5 If access codes are used they will be changed at least every six (6) months.

2.1.6 The Manager: Information Technology shall maintain a list all personnel having access.

2.1.7 Means of entry shall be provided on a strict "need to have" basis as determined by the Manager: Information Technology and approved by the Senior Manager: Strategic Support Services.

2.1.8 Guests will be required to sign a guest log and be escorted at all times.

### 2.2 Operational

2.2.1 The Manager: Information Technology will maintain a list of all personnel having access.

2.2.2 If used, keys will be stamped "*Do Not Duplicate*".

2.2.3 If access codes are used they will be changed at least every six (6) months.

2.2.4 The $CO^2$ fire suppression system stays activated and must be de-activated on entry and reactivated upon exit of the server room.

## 3. USAGE

### 3.1 Restricted/Sensitive

3.1.1 There shall be no eating, drinking, or smoking allowed in the server room at any time.

### 3.2 Operational

3.2.1 There shall be no eating, drinking, or smoking allowed in the server room at any time.

3.2.2 The server room will be available 24/7.

## 4. PHYSICAL SAFEGUARDS

### 4.1 Restricted/Sensitive

4.1.1 Servers shall be located in a room designed for housing server computers and ancillary equipment (secured server room managed by the Manager: Information Technology).

4.1.2 Such room shall be totally enclosed and physically separate from space designed for any other purpose and have appropriate environmental and fire/water hazard detection/suppression/prevention and controls.

4.1.3 Provision for staff to perform server operations may be located within the server room.

4.1.4 Wiring shall be routed in the server room away from personnel working areas and in a manner that allows for cable identification and maintenance.

4.1.5 There shall be no external signs making the server room identifiable.

4.1.6 Display devices shall be located so that the information displayed is not visible from outside the room.

4.1.7 All detection and monitoring devices shall be tested on a regular basis as recommended by the manufacturer.

4.1.8 Fire suppression must be tested in compliance with fire safety requirements and in a manner that does not disrupt operations.

4.1.9 The occurrence of testing shall be documented.

4.1.10 Cleaning supplies shall not be stored in the server room.

## 5. RECORD KEEPING

### 5.1 Restricted/Sensitive

5.1.1 Documentation of all repairs and modifications to the physical components related to security (e.g., doors, hardware, locks) shall be maintained for a period of six (6) years.

## 6. CONTINGENCY

### 6.1 Restricted/Sensitive

6.1.1 A sufficient uninterruptible power supply shall be in place and be of sufficient capacity to enable a normal shutdown in the event of power failure.

6.1.2 A backup plan shall exist in case of an air-conditioning failure.

6.1.3 Provision shall be made for physical access in support of restoration of services and data by authorized personnel in the event of a disaster.

## 7. GUIDELINES

7.1 Server rooms should be locked at all times using a multi-factor access control system capable of being audited and monitored remotely.

7.2 The guest log and the access log should be reviewed by the Manager: Information Technology at least monthly.

7.3 The guest log and the access log, if any, should be reviewed by the Manager: Information Technology at least monthly.

7.4 There should be at least one (1) fire alarm inside and one outside the server room.

7.5 The server room must have at least one (1) water detector and one (1) smoke detector.

7.6 Emergency power-off switches should be inside the server room. Switches may be placed outside the server room if adequately secured.

7.7 The server room should be above the entry level of the building.

7.8 Provision for surveillance of entry points and the server room should be made.

7.9 A pre-action, dry pipe suppression system should be in place.

7.10 The Fire Services Division and the Occupational Health and Safety Officer should conduct inspections on a regular basis.

7.11 In the case of an emergency, systems should be able to be shut-down quickly to prevent significant data loss.

7.12 A backup plan should exist in case of an air-conditioning failure.

7.13 An electronics-safe fire extinguisher should be prominently located inside the server room.