DIRECTORATE OF ICT

ICT ENVIRONMENTAL CONTROL PROCEDURES

Contents

Preamble
Data Centers are found in almost all organizations. These data centers host the service environment and electronic data and forms the Service Fabric of the organization. Due to the sensitivity nature of these implementations, it is imperative to guide on the proper mechanisms for access, management, security disaster recovery, value add and growth.

Purpose and Objectives
The purpose of the document is to provide the organization with guidelines and procedures relating to access control, environment control and operations of Service Fabric.

Scope of Application
This procedure is applicable to County Government of Meru employees granted privilege access to

Data Centre and cabinet rooms, service providers and consultants, and any other entity.

Legal framework
- ICT Policy

Procedure Content

Back ground
The vulnerability of business critical information systems and the data they contain within the Data Centre makes the site a high value asset, which requires a high degree of protection. A range of security measures are therefore in place to protect employees, information and physical assets, along with the reputation of County Government of Meru and interested third parties with equipment in the Data Centre.

1. **Entry Systems and Access Control**

Access shall be controlled via Biometrics fingerprint system and all doors shall be fitted with sensors to detect unauthorized or prolonged opening.

Staff and visitors shall not adjust or otherwise tamper with door fittings. Any suspected faults with doors, lights or any security equipment should be reported to Director ICT immediately.

Any person requiring access to the Data Centre shall sign the log book located and be accompanied and escorted by authorized staff during office hours.

Tailgating into restricted areas is prohibited. Care shall therefore be taken by all authorized staff to prevent these. During deliveries, authorized staff shall supervise such work at all times.

2. **Access after hours**

Security Services shall be responsible for access control and security of the Data Centre outside normal working hours. In case where contractors require access to Data Centre after hours, Security Services shall be responsible to provide such access and protection.

The Head of ICT or the Infrastructure manager will authorize the use and changes to be made in the Data Centre.

3. Close Circuit Television (CCTV)

Internal, entry and exits area of the Data Centre shall be monitored by a closed circuit television (CCTV) to capture all Data Centre activities.

4. Safety

This outlines the safety observed in the datacenter and in addition to this safety precautions shall be applied in conjunction with County Government of Meru Occupational health and Safety

5. Signs and Information

Safety signs and information shall be posted at access points to the Data Centre and cabinet rooms. General notices shall also be posted around the Data Centre providing detailed information on first aid, emergency contacts and general Health and Safety issues.

6. Health and safety Considerations

No one should attempt to lift heavy equipment without suitable help.

No one should attempt to lift equipment in and out of racks unaided, particularly where height makes the task more dangerous.

Ear defenders shall be made available and be worn if working in the Data Centre for periods longer than 30 minutes.

Anyone working in the Data Centre for prolonged periods should let staff know of their presence. Users are advised to take regular breaks from working to avoid adverse effects from temperature and noise levels in particular.

Flexible safety barriers shall be available and be used to lift up raised floor tiles.

7. Emergency Exits and Fire Alarm Procedures

When the fire alarm is triggered at the Data Centre, normal emergency procedures shall be followed as stipulated by County Government of Meru emergency evacuation procedures. Lifts shall not be used, only emergency stair ways shall be used.

8. Fire Detection and Fire Extinguishers

Fire and smoke detection system shall be fitted and linked to audible and virtual alarms.

If an alarm is activated the Data Centre shall be evacuated immediately to avoid gas inhalation and the incident shall be reported to Security Services and Director ICT.

9. Electrical Safety

Only qualified electrical technicians shall have access to electrical systems, IT staff and other personnel should contact the relevant electrical personnel when encountering electricity problems.

Request shall be authorized by the Director ICT

Use of Data Centre and Active Points

1) **Hours of Operation**

The Data Centre will be operated during office hours to authorized personnel between 8 am to 5 pm.

Access afterhours for maintenance purposes will be authorized and delegated by the Director ICT

2) **Equipment delivery**

Delivery of equipment shall be supervised by authorized personnel upon approval by the ICT Management

3) **Control of Equipment**

No unused equipment and spares shall be left at the Data Centre.

Alternate storage facility shall be available for such purpose.

Prohibited Items

The following items are prohibited from the Data Centre:

- Combustible materials such as paper and cardboard (except reference manuals as needed).
- Food and drink.
- Tobacco products.
- 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).

Cables and Wiring

Cables and wires shall be structured and labelled when running under the raised floor, wall, and equipment racks.

Environment

1. **Air Conditioning**

Under floor air conditioning shall be provided in the Data Centre. It shall deliver enough cooling per rack in accordance with design specification.

Service shall be done at least three times a year by a reputable maintenance service provider for Air dale equipment. Certificate for maintenance performed shall be submitted to the Department.

2. **C02 Fire Extinguisher**

The datacenter shall be fitted with C02 fire extinguishers

3. Power and Lighting Provisioning

Two single phase power sockets shall be available in each rack and shall be fed directly from the main switch.

Adequate power light shall be available to ensure that all equipment in the Data Centre are clearly visible.

This is backed up with the main generator, power backups and second generator

Lights shall be switched off when no access to the Data Centre is required.

4. UPS Provisioning

All major equipment at the Data Centre shall be powered on by a UPS system, should the AC power goes down. The UPS system should sustain power to those devices for at least 5 minutes to allow graceful shutdown.

Service shall be done at least annually by a reputable maintenance service provider for APC Galaxy equipment. Certificate for maintenance performed shall be submitted to the Department.

5. Temperature and Humidity

Temperature and Humidity monitoring devices shall be implemented and set to monitor deviations against baseline set according to standard recommended.

6. Environment Monitoring

A number of monitors shall be put in place to report on issues affecting the Data Centre environment. Monitoring system shall report to designated IT and Security personnel monitoring shall include:

- Temperature and Humidity alarms.
- Fire and Smoke Detectors.
- UPS malfunctioning or discharge during normal AC power operation.
- Daily monitoring.

7. Dust Prevention

The Data Centre shall be well ventilated to prevent dust from affecting equipment.

Equipment to be installed in the Data Centre shall be dust freed outside before introduced.

8. Waste Disposal and Cleaning

Cardboard and other items that can generate dust and that are easily combustible should remain outside the Data Centre.

Waste bin shall be available outside the Data Centre main entrance for easy disposal of other items of waste.

9. Change and Configuration Management

The Director ICT is responsible for all changes that shall take place at the ICT Environment.

All changes to be made shall be requested to and authorized by the Director ICT in accordance with **Change and Configuration Management Plan.**

The Director ICT or person assigned will monitor and review the Data Centre access log book on a regular basis.

Administration of the Policy
County Government of Meru and ICT Directorate is responsible for enforcing these procedures and continuously ensuring monitoring and compliance.

Procedure Review
This document shall be reviewed Bi-annually.

Default
Non-compliance of this policy shall constitute violation of the policy and shall be treated in terms of the departmental disciplinary code and procedure policy.

Inception Date
This policy comes into effect from the date of approval by Cabinet

Enquiries
Enquiries about these procedures should be directed to the County Government ment of Meru ICT Office.

Document Title	**ICT Data Centre Physical Access and Environmental Control Procedure**
Compiled By:	County Government of Meru ICT Directorate …… ……. Director ICT Date
Qualified by:	…… ……. …Head Of Infrastructure…… Date
Adopted by:	…… ……. Head Of ICT Date
Approved by:	…….. .. …..……. Chief Officer – Finance, ICT & Planning Date