Trusted Partner in Healthcare

ICT POLICY

November 2016

Table of Contents

Revision Notice

Second version November 2016

First version as by September 2013

Copyright

© CMST 2013. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorization of CMST.

Contact Details

Any queries concerning the content of this Policy may be directed to the Chief Executive Officer, CMST Head Office, Mzimba Street, P/Bag 55, Lilongwe. Tel: +265 1753910, email: cmst@cmst.mw

Foreword

The Central Medical Stores Trust (CMST) exists to efficiently procure, store and distribute medicines and medical supplies to the population, a mandate that directly impacts on promoting the population's health gain.

In pursuing this mandate, CMST is largely reliant on Information Communication and Technology (ICT). For that reason, this Policy is to direct proper management of ICT related matters to promote good practices and eliminate challenges that could befall ICT operations, and ultimately misalign CMST's mandate.

In this document, CMST exhibits its willingness to handle ITC in the most effective manner. In doing so, the Policy details recommended measures against unprofessional conduct in dealing with ICT matters.

The Policy has the blessings of the Board of Trustees and it is my belief and urge that CMST Management, staff and all stakeholders will support its implementation.

To ensure that all users start out on the same page in implementing the Policy, comprehensive awareness on use of the document shall be arranged.

By use of this Policy, all ICT matters are to be handled professionally in a manner aligned to other CMST policies or other national and international ICT policies and laws to which CMST or the Malawi ICT industry subscribe.

CMST is thankful to the Ministry of ICT for providing overall guidance in aligning the CMST ICT Policy to the national ICT policy provisions. It is through such alignment that CMST is assured of meeting its objectives while not departing from the larger national goals on ICT.

Signed

Preface

The Central Medical Stores Trust (CMST) is aware of its delicate operating environment where ICT can pose both advantages and challenges.

It is therefore CMST's proactive measure to come up with a Policy around which to set a regulated ICT environment within which risks can be foreseen and averted.

The Policy's priority areas include the controlling of access to information and systems; developing and maintaining software; data management; reporting and responding to information security incidents; applications systems management and combating Cyber Crime.

It is expected that staff and all concerned persons contribute to the successful implementation of the Policy.

The Policy therefore also details what is to happen in terms of non-compliance.

Signed

Definition of Terms

Access Control Standards	Rules which an organization applies in order to control access to its information assets.
Cybercrime	Criminal activity which uses network access to commit a criminal act.
Hacker	A highly skilled computer expert who uses computers to gain unauthorized access to data.
Information Security	Sometimes shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
Techno-vandalism	Term used to describe a hacker or cracker who breaks into a computer system with the sole intent of defacing and or destroying its contents.
Workstations	A special computer designed for technical or scientific applications

Acronyms

CEO	Chief Executive Officer
CHAM	Christian Health Association of Malawi
CMST	Central Medical Stores Trust
ICT	Information and Communication Technology
IS	Information Security
UPS	Uninterruptible Power Supply

CMST Mandate

The Central Medical Stores (CMS) existed by Government's General Notice Number 125/1968 of the Finance and Audit Act to operate as a commercially oriented Treasury Fund with the purpose of purchasing, storage and distribution of medicines and medical supplies for the public health facilities. In August 2011, CMS obtained "Trust Status" and became the Central Medical Stores Trust (CMST) under the CMST Trust Deed of 2010.

Why a public Trust?

A Public Trust is foreseen to judiciously and efficiently estimate and procure the medical and pharmaceutical demands of the population through proper public procurement, storage and proficient distribution of the medicines and medical supplies to user facilities.

Vision

To be the choice public sector supplier of efficacious, good quality, affordable and safe medicines and medical supplies in Malawi.

Mission Statement

To ensure continuous, uninterrupted and adequate supply of approved quality and affordable medicines and medical supplies to the health facilities in Malawi.

Core Values

a) Customer Orientation

b) Innovation

c) Integrity

d) Teamwork

e) Diversity and Equal Opportunity

Introduction

This document contains formal statements of the rules by which those who are given access to CMST's systems, data, information and assets must abide.

CMST core functions are to procure, warehouse, sale and distribute medicines and medical supplies to public health facilities in Malawi.

The main purpose of this ICT Policy is to inform all users or members of staff of the Trust of the obligatory requirements for protecting data, information and physical ICT assets at CMST and provide a framework from where users of various systems and processes can conduct themselves on the resources made available to them.

Objectives

The objective of this policy is to continuously provide secure data, information and well managed systems In order to achieve the three main core functions which are:

1. To help maintain systems that would help to procure medicines and medical supplies for the health facilities

2. To help maintain good systems for warehousing of medicines and medical supplies to meet international standards

3. To help in selling and distributing the medicines and medical supplies to various Public and Christian Health Association of Malawi (CHAM) health facilities.

Policy Goals

1. To define organizational roles and responsibilities with regard to ICT.

2. To give direction on how users can conduct themselves when working with CMST's ICT assets, documents, and systems and how they can protect the same from damage, abuse and theft.

3. To offer a secure working environment for the users of CMST ICT services and help maintain systems that can be used in decision making at corporate, functional and operational levels of the Trust.

ICT Assets

The assets to be protected shall include the following:

1. All technical configurations of the networking devices and computer systems.

2. Hardware assets

3. Data assets

Users and Clients Covered by this Policy

1. Users shall include:

    1. All personnel employed under the Trust who have access to IT equipment. Companies/individuals contracted by CMST

    2. CMST equipment or facilities that:

        a. take output from CMST systems
        b. give input into CMST systems

    3. CMST Clients with ability to access CMST's equipment.

4. External Support Companies

2. Clients shall include:

   All Government health facilities and those with working agreement with Ministry of Health CMST Suppliers

The CMST ICT Security Directive

1. The Board of CMST shall supports the information security principles and statements expressed in this ICT Policy and CMST staff members shall comply with these principles at all times.

2. CMST is highly reliant on information technology (IT) to support its business processes, and as such, the ICT facilities used to input, process, store transmit and disseminate CMST information are viewed as important as other resources of CMST such as money, physical assets and facilities.

Information Security Governance and Responsibilities

1. The heads of section of CMST have the overall accountability for making sure that data, information, are secure and under their control.

2. The ICT section shall act as an implementation agent for the agreed rules and procedures. The section can enforce implementation and compliance of rules through ICT techniques. However where this cannot be possible, compliance of procedures will be done by user departments.

The ICT Department shall:

1. Oversee the implementation of information security controls across CMST.

2. Review incidents from non-compliance to ICT policy for collective action.

8. The Human Resources and Administration Section shall orient new employees about the ICT Policy, as part of the recruitment process.

9. All access rights therefore will have to go through a formal procedure where a Head of Department agrees and signs for the rights to be granted.

Policy Review

10.This policy shall be reviewed every 2 years or as and when significant changes occur.

Non-Compliance

11.Non-compliance with this ICT Policy shall lead to disciplinary action as stipulated in the CMST's Terms and Conditions of Service.

POLICIES

Section 1: Combating Cyber Crime

Policy 1.1: Defense Against Virus Attacks

Policy Statement

1.1.1 The head of ICT department shall ensure that anti-virus software is deployed across all computer platforms with regular virus definition updates All employees are mandated to scan their machines on a daily basis.

1.1.2 Proper punitive measures shall be leveled against a member of staff that spreads a virus through their computer or flash disks in line with the terms and conditions of service

Policy 1.2: Defense Against Hackers, and Techno-Vandalism

Policy Statement

CMST shall deploy appropriate protective systems and devices for the protection of Information and Systems.

Policy 1.3: Responding to Virus Incidents

Policy Statement

ICT Section shall timeously respond to virus incidents and perform regular reviews according to laid out procedures

Policy 1.4: Internet Usage

Policy Statement

Internet shall be used for work related purposes

Policy 1.5: E-Mail

Policy Statement

CMST e-mail messages, including backup copies, shall be subject to official inquiries, such as the Office of Inspector General and Auditors requests involving litigation and other official investigations.

Section 2: Controlling Access to Information and Systems

Policy 2.1: Network Management and Access Control Standards

Policy Statement

Access to Network devices shall be restricted to CMST ICT authorized personnel.

Policy 2.2: Securing Unattended Workstations and Servers

Policy Statement

All CMST employees shall ensure control against unauthorized access and use to their computer equipment.

Policy 2.3: Managing Passwords

Policy Statement

All employees shall adhere to procedures and best practice guidelines in the selection, use and management of passwords.

Policy 2.4: Physical Access into CMST Server Rooms

Policy Statement

All CMST server rooms shall remain a protected area from unauthorized access.

Policy 2.5: Server Rooms Usage

Policy Statement

2.5.1 All server rooms shall not be used as offices

2.5.2 No food shall be taken or stored in the server rooms

Section 3: Developing and Maintaining Software

Policy 3.1: Developing and Maintaining Software

Policy Statement

ICT department shall be responsible for development and maintenance of software in the event that there is no capacity development and maintenance shall be outsourced

Section 4: Data Management

Policy 4.1: Data Backup

Policy Statement

The ICT department shall perform data backup, retention, testing and restoration for servers, computers and networking devices configurations.

Policy 4.2: ICT Disaster Recovery

Policy Statement

CMST shall have a disaster recovery plan and site for its assets

Section 5: Hardware

Policy 5.1: ICT Hardware

Policy Statement

All ICT hardware shall be procured and installed by authorized ICT personnel

Policy 5.2: Equipment Testing

Policy Statement

All ICT equipment shall be comprehensively tested by ICT personnel before deployment.

Policy 5.3: Continuous Power Supply to Critical Equipment

Policy Statement

ICT Department shall ensure that an Uninterruptible Power Supply source is installed to all critical equipment to ensure the continuity of services during power outages.

Policy 5.4: Printing

Policy Statement

5.4.1 CMST printers shall be used for CMST business.

5.4.2 Allocation of standalone printers shall be limited to executive management and managers unless with approval from the CEO.

Policy 5.5: Using Portable Storage Device and Removable Media

Policy Statement

Portable storage devices and removable media shall not be allowed on CMST computers.

Section 6: Reporting and Responding to Information Security Incidents

Policy 6.1: Reporting Information Security Incidents

Policy Statement

Employees shall exercise vigilance for possible security activities and promptly report incidents to the IT manager.

Policy 6.2: Responding to Information Security Incidents

Policy Statement

The ICT Department shall respond to all reported information security incidents.

Section 7: Change Control

Policy 7.1: Change Control

Policy Statement

All changes to systems and hardware shall be executed through a change control process

Section 8: Application Systems Management

Policy 8.1: System Operation

Policy Statement

ICT Department shall ensure that all users are familiar with the systems application management

Policy 8.2: Systems Access

Policy Statement

ICT Department shall ensure that all users are given access rights into the system applications.

Policy 8.3: Systems Reports

Policy Statement

ICT Department shall produce relevant system audit reports when necessary

Policy 8.4: Responsibilities and Accountability

Policy Statement

All users shall be responsible and accountable for actions performed in the systems.

ICT POLICY APPROVAL

Approved by the Board

_____ _____

Chairperson Secretary