Part 3: Information Security-ICTA-3.003:2023

DRAFT

© ICTA 2023- All rights reserved Third Edition 2023

The ICT Authority is a State Corporation under the State Corporations Act 446

www.icta.go.ke

REVISION OF ICT STANDARDS

In order to keep abreast of progress in industry, ICT Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Chief Executive Officer, ICT Authority, are welcome.

©ICT Authority 2023

Copyright. Users are reminded that by virtue of Section 25 of the Copyright Act, Cap. 12 of 2001 of the Laws of Kenya, copyright subsists in all ICT Standards and except as provided under Section 26 of this Act, no Standard produced by ICTA may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from the Chief Executive Officer.

ICT AUTHORITY

Telposta Towers 12th floor. Kenyatta Avenue P.O. Box 27150-00200, Nairobi Kenya Tel.: +254 20 2089061
Web:http://www.icta.go.ke
Email:standards@ict.go.ke

DRAFT

DOCUMENT CONTROL

Document Name:	Information Security Standard
Prepared by:	Government Information Security Technical Committee
Edition:	ThirdEdition
Approved by:	Board of Directors
Date Approved:	
Date of Operationalization:	
Next Review Date:	After 3 years

DRAFT

TABLE OF CONTENTS

FOREWORD 7
1. INTRODUCTION 8
2. SCOPE 8
2.1 Application 8
3. NORMATIVE REFERENCES 8
4. TERMS AND DEFINITIONS 9
4.1. Abbreviations 11
4.2. Sub domains 12
5. LEADERSHIP AND ACCOUNTABILITY 12
5.2 Roles and Responsibilities 13
5.3 Contacts with Authorities and Special Interest groups 13
5.4 Information Security in Project Management 13
6. HUMAN RESOURCES SECURITY 13
6.1 Background Screening 13
6.2 Terms and Conditions of Service 13
6.3 Termination or Change of responsibilities 14
6.4 Information Security Awareness, Public Education and Training 14
6.5 Disciplinary Process 14
7. SYSTEMS AND APPLICATIONS SECURITY 14
8. COMMUNICATION SECURITY 16
8.2 Information Transfer 17
9. RISK MANAGEMENT 18
9.1 Information Asset Management 18
9.2 Information Classification and Sharing 20
9.3 Business Continuity Management 20
9.4 Threat and Vulnerability Management 22
10. OPERATIONAL SECURITY 22
10.1 User End-point Device Security 22
10.2 Collection of Evidence 24
10.3 Protection Against Malware 24
10.4 APIs and Interoperability 25
10.5 Virtualization 25

DRAFT

11. ACCESS CONTROL 25
11.1 Access control policy 26
11.2 Access control to program source code 27
11.3 Identity management 27
11.4 Privileged access rights 28
11.5 Management of Authentication Information 28
11.6 Review of user access rights 29
11.7 Removal or adjustment of access rights 29
11.8 Information access restriction 30
11.9 Child Online Protection 30
11.10 Data Masking 30
11.11 Secure log-on procedures 30
11.12 Use of privileged utility programs 31
11.13 Change Management 31
11.14 Incident Management 32
11.15 Physical and environmental security 35
11.16 Cloud security ..... **Error! Bookmark not defined.**
12. CRYPTOGRAPHY 36
12.1 36
Cryptographic controls 36
12.2 Key Management 36
12.3 Digital Signatures 36
12.4 E-Commerce 37
13. SUPPLIER RELATIONSHIPS 38
13.1 Supplier Relationships 38
13.2 Supplier service delivery management 39
14. COMPLIANCE 40
14.1 Identification of applicable legislation and contractual requirements 40
MCDA shall institute mechanisms to review and monitor changes to, regulatory or contractual and ensure compliance. 40
14.2 Intellectual property rights 40
14.3 Protection of records 40
MCDAs shall establish guidelines on secure management of records throughout the document life cycle. 40
14.4 Privacy and protection of personally information 40

DRAFT

15. APPENDIX I: Compliance Checklist for information Security 41
16. Appendix II: Guidelines 58

DRAFT

FOREWORD

The ICT Authority has the mandate to set and enforce ICT standards and guidelines across all aspects of information and communication technology including Systems, Infrastructure, Processes, Human Resources and Technology for the public service. The overall purpose of this mandate is to ensure coherent and unified approach to acquisition, deployment, management and operation of ICTs across the public service in order to achieve secure, efficient, flexible, integrated and cost-effective deployment and use of ICTs.

To achieve this mandate, the Authority established a standards committee to identify the relevant standard domains and oversee the standards development process. The committee consulted and researched broadly among subject matter experts to ensure conformity to acceptable international and national industry best practices as well as relevance to the Kenyan public service.

For example, the ICT Security Standard, which falls under the overall Government Enterprise Architecture (GEA), has therefore been prepared in accordance with KEBS standards development guidelines which are, in turn, based on the international best practices by standards development organizations including ISO.

The Authority's Directorate of Programmes and Standards has the oversight role and responsibility for management, enforcement and review of this standard. The Directorate shall carry out quarterly audits in all the Ministries, Counties, and Agencies (MCA) to determine compliance to this Standard.

The Authority shall issue a certificate for compliance to agencies upon inspection and assessment of the level of compliance to the standard. For non-compliant agencies, a report detailing the extent of the deviation and the prevailing circumstances shall be tabled before the Standards Review Board who shall advise and make recommendations to remedy the shortfall.

The ICT Authority management, conscious of the central and core role that standards play in public service integration, fostering shared services and increasing value in ICT investments, shall prioritize the adoption of this standard by all Government agencies. The Authority therefore encourages agencies to adhere to this standard in order to obtain value from their ICT investments.

Stanley Kamanguya, OGW
Chief Executive Officer
ICT Authority

DRAFT

1. INTRODUCTION

Data and Information are assets that, like other important government assets, are essential to Government and its operations and consequently need to be suitably protected in order to ensure information confidentiality, integrity and availability. This is especially important taking into consideration the increase in interconnectivity of government departments and systems. As a result, government information is now exposed to a growing number and a wider variety of threats, risks and vulnerabilities.

Information systems security standards aim at guiding in the setting up of appropriate controls that will ensure the protection of information from a wide range of threats in order to ensure continuity in government operations, minimize risk, and maximize return on government IT investments.

The following set of standards guide in the implementation of suitable set of controls, including policies, processes, procedures, organizational structures, software and hardware functions to ensure information security is achieved. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific IT security and operational objectives of the government are met.

Information Security is based on the following five elements:

- Confidentiality - ensuring that Information is only accessible to those with authorized access
- Integrity - safeguarding the accuracy and completeness of Information and processing methods
- Availability - ensuring that authorized Users have access to Information when required
- Compliant Use - ensuring that MCDA meet all legal and contractual obligations
- Responsible Use- ensuring that appropriate controls are in place so that Users have access to accurate, relevant and timely Information but that Users of MCDA ICT resources do not adversely affect other Users or other Systems.

2. SCOPE

This ICTA Standard establishes security guidelines for Ministries, Counties and Agencies as custodians of public information and data. The standard is based on a risk management approach and requires MCDA to implement policies and procedures that are proportionate to their level of risk, after conducting and documenting a risk assessment.
The objective is to provide a consistent approach to managing information security risks across Government in line with the Government Enterprise Architecture guiding principles.

2.1Application

This standard will be applicable to the following:

- Central Government of Kenya
- County Governments
- Constitutional Commissions
- State Corporations

3. NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. All standards are subject to revision and, since any reference to a standard is deemed to be a reference to the latest edition of that standard, parties to agreements based on this standard are encouraged to take steps to ensure the use of the most recent editions of the standards indicated below. Information on currently valid national and international standards can be obtained from Kenya Bureau of Standards.

DRAFT

- ISO/IEC 27002:2022- Information Security, Cybersecurity and Privacy Protection-Information Security Controls
- Center for Internet Security Controls Version 8
- The computer Misuse and Cybercrime Act 2018
- Data Protection Act 2019

For the purposes of this ICTA Standard, the following definitions, abbreviations and symbols apply:

4. TERMS AND DEFINITIONS

Asset	Anything that has value to the MCDA.
Administrative Privileges	The highest level or rights granted to the user of a computer, application system or database or network, it is the ability to make major changes to a system.
Application Security	Application security is the use of software, hardware, and procedural methods to protect applications from external threats from development, deployment to maintenance.
Availability	The property of being accessible and usable upon demand by an authorized entity
Business continuity planning	A plan to enable a businessto continue offering critical services in the event of a disruption and tosurvive an interruption to activities.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Cloud computing	On-demand availability of computer data storage and computing power system resources without physical presence management by the user. This mainly defines data centers available to many users over the Internet.
Cryptography	Securing information by applying mathematical concepts and a set of rule-based calculations called algorithms that to transform messages in ways that are hard to decipher with an objective is to protect confidentiality, authenticity or integrity of the information.
Data Masking	A data security technique in which a dataset is copied but with sensitive data obfuscated.
Data Security	Data security refers to protective measures that are applied to prevent unauthorized access to computers, databases and websites that may cause data corruption.
Digital signature	A mathematical technique used to validate the authenticity and integrity of a message, software or digital document
Disaster Recovery Planning	A set of human, physical, technical andprocedural resources to recover, wwithin a defined time and cost, an activityinterrupted by an emergency or disaster
Duress alarm	Is a method for secretly indicating that an action is taking place ‘under duress’.

Electronic commerce	Thebuying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions. It is the buying and selling produce by electronic means such as by mobile applications and the Internet.
Email Security	Email security refers to the collective measures used to secure the access and content of an email account or service.
Hardware Security	Hardware security refers to the collective measures deployed to secure the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system.
Incident Management	The process of describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence of ICT incidences.
Information Asset	Any device or media used to store information in any form.
Information Backup	The creation of a copy of computer data and stored in a different location so that it may be used to restore the in the event of a data loss event
Information Classification	A process in which organizations assess data that they hold and the level of protection it should be given, usually classified in terms of confidentiality.
Information Security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Information security incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Information Security Management System (ISMS)	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security NOTE: The management system includes MCDA's structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
Integrity	The property of safeguarding the accuracy and completeness of assets
Key management	The process of administering or managing cryptographic keys. It involves the generation, creation, protection, storage, exchange, replacement and use of specific security keys and with another type of security system built into large cryptosystems, enables selective restriction for certain keys.

DRAFT

Malware	Software that is intentionally designed to cause damage to a computer systems and infrastructure.
Network Security	Network security refers to any activities designed to protect the usability, reliability, integrity, and safety of your network and data.
Physical Security	The protection of building sites and equipment (and all information and software contained therein) from theft vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee).
Remote working	All forms of work outside of the office, including non-traditional work environments, such as those referred to as "tele-working", "telecommuting","flexible workplace", and "virtual work" environments.
Residual risk	The risk associated with an action or event remaining after natural or inherent risks have been reduced by risk controls
Risk acceptance	Decision to accept a risk
Risk analysis	Systematic use of information to identify sources and to estimate the risk
Risk assessment	Overall process of risk analysis and risk evaluation
Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk management	Coordinated activities to direct and control an MCDA with regard to risk
Risk treatment	Process of selection and implementation of measures to modify risk
Threat Management	Management of potential incidents caused by anything/anyone capable of acting against an asset in a manner that can result in harm.
Vulnerability Management	Setting up controls against a weakness in the design, implementation, operation orinternal control of a process that could expose the system to adverse threats

4.1. Abbreviations

API	Application Program Interface
DKIM	Domain Keys Identified Mail
DMARC	Domain based Message Authentication Reporting and Conformance
GEA	Government Enterprise Architecture
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Standards Organization
IS	Information Security
IT	Information Technology

DRAFT

MCDA	Ministry, Counties, Departments and MCDA
OS	Operating System
PCI-DSS	Payment Card Industry – Data Security Standard
PKI	Public Key Infrastructure
SDLC	Software Development Life Cycle
SPF	Sender policy Framework
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN's	Virtual Local Area Networks
WAF's	Web Application Firewalls

4.2. Sub domains

a. Leadership And Accountability
b. Human Resources Security
c. Systems and Applications Security
d. Communication Security
e. Risk Management
f. Operational Security
g. Access Control
h. Cryptography
i. Supplier Relationships
j. Compliance

5. LEADERSHIP AND ACCOUNTABILITY

MCDAs shall establish sufficient governance structures in line with the GOK IT Governance Standard clause 6 and 7.3.3 (b).

5.1 Information Security Policies

5.1.1 Enterprise Information Security Policy

MCDAs shall developan enterprise information security policy which sets out management direction and support for information security. The policy shall be approved by management, published, communicated to and acknowledged by personnel and third parties.
MCDA shall take into consideration the business strategy & requirements, legal statutory regulatory and contractual requirements, risk and threat landscape when deriving the enterprise information security policy.

The enterprise information security policy shall contain: -
a) Definition of information security, and information security objectives framework
b) Assignment of responsibilities to the relevant information security management roles
c) Commitment to implementthe applicable to information security requirements
d) Procedures for handling deviations and exceptions
e) MCDA shall review information security policies at planned intervals and when significant changes occur.

5.1.2 Issue Specific Security Policy

The enterprise information security policy shall be supported by issue specific information security policies, to address distinct needs of certain target groups within an MCDA.

DRAFT

5.2 Roles and Responsibilities

MCDAs shall:

5.2.1 establish define and allocate information security roles and responsibilities in line with the GoK ICT Governance standard 7.3.3(b).
5.2.2 Segregate conflicting duties and areas of responsibilities to reduce the risk of fraud error and bypassing of information security controls.

5.3 Contacts with Authorities and Special Interest groups

MCDAs shall establish contacts with relevant Authoritiesand special interest groups to facilitate appropriate flow of information and to ensure that information security incidents are promptly reported and responded to in order to minimize the impact of information security incidents and ensure business continuity.

5.3.1 MCDA shall maintain contacts with Law enforcement, Regulatory bodies, Supervisory authorities and Service providers.
5.3.2 MCDA Information Security function shall maintain contact with specialist security forums and professional associations

5.4 Information Security in Project Management

Information security objectives shall be included in all project's objectives being implemented by the MCDA.

5.4.1 MCDA shall ensure the protection of confidentiality, integrity and availability of project information.
5.4.2 MCDA shall identify, address and manage information security risks at all stages of projectmanagement.

6. HUMAN RESOURCES SECURITY

6.1 Background Screening

MCDAs shall:

6.1.1 MCDA shall conduct background verification checks on all candidates for employment in accordance with relevant laws, regulations and ethics.
6.1.2 MCDA shall ensure that personnel have necessary competence and trusted to perform the security role assigned
6.1.3 MCDA shall have contractual agreements (code of conduct) with employees and con tractors that reflect the organization's policies for information security

6.2 Terms and Conditions of Service

MCDAs shall ensure that the employment contracts state the personnel's and organization's responsibility towards information security.

MCDAs shall ensure that employees and contractors sign confidentiality or non-disclosure agreement prior to access provisioning.

DRAFT

6.2.1 MCDAs shall ensure that employees and contractors are provided with guidelines to state information security legal responsibilities and rights.
6.2.2 There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

6.3 Termination or change of responsibilities

MCDA shall define, enforce and communicate information security responsibilities and duties that remain valid after termination or change of employment.

6.3.1 MCDAs shall define a process for communicating changes in responsibilities or Termination of employment to all relevant parties or Termination of employment to all relevant parties.
6.3.2 All access rights issued shall be disabled or reassigned in accordance to the access control policy

6.4 Information Security Awareness, PublicEducation and Training

MCDA shall develop an information security awareness program to educate and train personnel and stakeholders on information security policy, sector specific policies and procedures.

6.4.1 MCDA shall develop and implement an information security awareness and training program in line with the organization's information security policies, topic specific and relevant procedures.
6.4.2 MCDAs shall assess effectiveness of the awareness program to test knowledge retention.
6.4.3 MCDA shall build capacity for technical teams whose roles require specific skill sets and expertise.

6.5 Disciplinary Process

MCDAs shall define a disciplinary process to handle information security policy violation by employees and third party.

7. SYSTEMS AND APPLICATIONS SECURITY

7.1 Systems acquisition and development

MCDAs shall:

DRAFT

7.1.1 Identify, specify and approve Information Security Requirements when developing or acquiring applications
7.1.2 Monitor and review activities related to system development to ensure compliance to Information security requirements.
7.1.3 Include security requirements in the specification and design phases
7.1.4 Ensure secure coding practices appropriate to the programming language and development environment are being used.
7.1.5 Carry out system, acceptance and security testing such as regression testing, acceptance testing and penetration testing.
7.1.6 Apply secure coding principles to ensure software is written securely reducing potential in formation security vulnerability.
7.1.7 Maintain secure repositories for source code and configurations to prevent access to source code, development tools and software libraries.
7.1.8 Verify that the version of all software acquired from outside the organization is still supported by the developer or appropriately hardened based on developer security recommendations.
7.1.9 Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities to reduce dependency on contractors.
7.1.10 Apply mechanisms to verify use of secure coding practices and adherence to internally developed software.
7.1.11 Ensure developers have capability to prevent, identify and fix software vulnerabilities
7.1.12 Escrow agreements are entered into for safeguarding of source code in the event the system is not fully owned by the MCDA
7.1.13 For both in house and off shelf systems require that quality assurance is guaranteed in meeting the requirements of the system.
7.1.14 Ensure user acceptance testing is performed before acceptance of the system

7.2 Separation of development, testing and operational environments

MCDAs shall:

7.2.1 Changes to information systems are subject to change management procedures to preserve information security
7.2.2 Maintain a change management policy, secure development and implementation. Adhere to licensing requirements and ensure cost effective license solutions to avoid licensing risks.

7.3 Cloud security

MCDA's shall ensure:

DRAFT

7.3.1 Effective governance, risk and compliance are catered for by ensuring the following measures are taken into consideration;

7.3.2 Risk assessment of the cloud solution has been undertaken and the controls to the risks have been implemented

7.3.3 Continued availability of the information systems and data by considering business continuity planning that seeks to prevent interruption of mission-critical services, and to reestablish full functionality.

7.3.4 Integrity of the information stored within the system and while on transit

7.3.5 Confidentiality of sensitive data while stored and in transit

7.3.6 Conformity to applicable laws and regulations

7.3.7 If possible include a right of audit in the contract

7.3.8 Request proof of independent security reviews and certification reports that meet the MCDA compliance requirement

7.3.9 The use of private cloud deployment model only, no multi-tenancy, for additional security

7.3.10 The MCDA in safeguarding its interest shall also ensure that the following policies are effected:

7.3.10.1 **Privacy policy** - A privacy policy document informs readers how a technology or other product or service will use an MCDA's personal information. The term privacy policy is often used because many IT systems gather and use personal information from users in many different ways. It is important to ensure that a privacy policy is in place to protect or cover the MCDA against this risk of exposure.

7.3.10.2 **Confidentiality policy** - The purpose of a Confidentiality Policy is to lay down the principals that must be observed by all that have access to information on the cloud service mostly confidential information.

7.3.10.3 **Data Soveriegnity laws** - Data sovereignty is the idea that data is subject to the laws and governance structures within the nation it is collected or stored.

7.3.10.4 **Data integrity (data modification) policy** - Data integrity is the maintenance and assurance of data accuracy and consistency over its entire life-cycle

7.3.10.5 **Authentication and access policy** - Authentication is the process by which a system or application confirms that a person or device really is who or what it is claiming to be and through which access to the requested resource is authorized.

7.3.10.6 **Exit strategy policy** - An exit strategy is a planned approach to terminating a situation in a way that will maximize benefit and/or minimize damage or risk.

8. COMMUNICATION SECURITY

8.1 Network Security

Network and network devices should be secured, managed and controlled in order protect information in systems and applications from compromise

The MCDA shall;

8.1.1 Maintain an up-to-date documentation including network diagrams and configurations of network devices.

8.1.2 Establish controls to protect confidentiality & Integrity of data transmitted over systems and applications transmitted through public networks, third party networks or wireless networks.

8.1.3 Log, monitor and detect any activities that may compromise the network security

8.1.4 Implement network security measures to ensure availability of network services

8.1.5 Segregate networks in security boundaries and control traffic based on business needs

8.1.6 Detect, restrict, and authenticate connection of equipment and devices on the network

8.1.7 Manage and restrict access to external websites through web filtering to prevent exposure to malicious content.

8.1.8 Establish responsibilities and procedures for management of network equipment and devices.

8.2 Information Transfer

MCDAS shall:

8.2.1 Establish policies, procedures and agreements for internal and external information transfers
8.2.2 Establish controls to protect information on transit from interception, unauthorized access & modification
8.2.3 Establish controls to ensure traceability and nonrepudiation including maintaining a chain of custody for information while in transit
8.2.4 Classify and label information in transit.
8.2.5 Develop retention and disposal guidelines for all business records including messages
8.2.6 Ensure reliability and availability of transfer services.
8.2.7 Protect against transmission of malware during electronic communication.
8.2.8 Protect against sending documents and messages to the wrong address
8.2.9 Implement stronger levels of authentication while transferring information
8.2.10 Establish rules, procedures and agreements on transfer of physical media e.g., physical documents, removable media, network attached storage devices from loss and unauthorized information disclosure.
8.2.11 Institute measures to ensure confidential verbal information is secured and not overheard by unauthorized persons.

8.3 Electronic messaging

This is the creation, storage, exchange, and management of text, images, voice, e-mail, paging, and Electronic Data Interchange over a communications network

MCDA shall develop and implement policies taking into consideration:
8.3.1 Protecting messages from unauthorized access, modification or denial of service commensurate with the classification scheme adopted by the organization.
8.3.2 Ensuring correct addressing and transportation of the messages;
8.3.3 Reliability and availability of the service;
8.3.4 Requirements for electronic signatures;
8.3.5 Obtaining approval prior to using external public services such as instant messaging, social networking or file sharing;
8.3.6 Implementation of cryptographic technologies to protect user authentication and email data.
8.3.7 The mail clients are deployed, configured, and used properly to meet the security requirements of the organization.
8.3.8 Use of sandboxing to analyze and block inbound email attachments with malicious behavior
8.3.9 Domain based Message Authentication Reporting and Conformance (DMARC) policy, the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards.
8.3.10 Compliance with any relevant legal requirements

8.4 Agreements on information transfer

MCDA shall be subject to terms of agreements to address the secure transfer of business information between the organization and external parties.

The information security content of the agreement shall reflect the sensitivity of the business information involved.The Information transfer agreements should incorporate the following:

DRAFT

8.4.1 Management responsibilities for controlling and notifying transmission, dispatch and receipt;
8.4.2 Procedures to ensure traceability and non-repudiation;
8.4.3 Minimum technical standards for packaging and transmission;
8.4.4 Courier identification standards;
8.4.5 Responsibilities and liabilities in the event of information security incidents, such as loss of data;
8.4.6 Use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected
8.4.7 Technical standards for recording and reading information and software;
8.4.8 Any special controls that are required to protect sensitive items, such as cryptography
8.4.9 Maintaining a chain of custody for information while in transit;
8.4.10 Acceptable levels of access control.

9. RISK MANAGEMENT

9.1 Information Asset Management

MCDAs shall:

DRAFT

9.1.1 Implement and maintain an inventory of assets associated with information and information processing facilities

9.1.2 For each of the identified assets, ownership of the asset shall be assigned and the classification shall be identified

9.1.3 The owner shall ensure the assets are appropriately classified and protected,

9.1.4 Ensure labellingofclassified information. Physical labels and metadata shall be used

9.1.5 Assign the owner the responsibility of periodically reviewing access restrictions and classifications to important assets, taking into account applicable access control policies;

9.1.6 Assign the owner the responsibility of proper securing information when the asset is retired or destroyed.

9.1.7 Establish rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, created, documented and implemented.

9.1.8 Conduct an Information security awareness training for employees and external party users using or having access to the organization's assets containing information and with access to information processing facilities and resources

9.1.9 **Ensure** all employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement unless there exists a pre-arrangement for transfer of ownership.

9.1.10 Ensure the termination process includes the return of all previously issued physical and electronic assets owned by or entrusted to the organization

9.1.11 Establish procedures to ensure that where an employee or external party user purchases the organization's equipment or uses their own personal devices, that all relevant information is transferred to the organization and securely erased from the equipment

9.1.12 Establish procedures to ensure that where an employee or external party user has knowledge that is important to ongoing operations, that information shall be documented and transferred to the organization.

9.1.13 Control unauthorized copying of relevant information (e.g., intellectual property) by terminated employees and contractors, while serving the notice period of termination

9.1.14 Develop and implement a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities

9.1.15 Establish a clear desk and clear screen policy that will take into account the information classifications, legal and contractual requirements and the corresponding risks and cultural aspects of the organization. The following guidelines shall be implemented

9.1.15.1 Lock way sensitive or critical business informationwhen not required, especially when the office is vacated.

9.1.15.2 Log off computers and terminals and setup user authentication mechanisms when unattended

9.1.15.3 Prevent the use of unauthorized photocopiers and other reproduction technology

9.1.16 Ensure the physical asset is maintained in accordance with the supplier's recommended service intervals and only authorized maintenance personnel shall carry out repairs and service equipment;

9.1.17 Maintain records of all suspected or actual faults, and of all preventive and corrective maintenance;

9.1.18 Establish appropriate controls when the asset is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, information shall be cleared from the asset or the maintenance personnel shall be cleared;

9.1.19 Ensure compliance with insurance policies during maintenance

9.1.20 Inspect the asset before putting the asset back into operation after its maintenance to verify that it has not been tampered with and does not malfunction.

9.1.21 Develop procedures for the management of removable media in accordance with the classification scheme adopted by the organization.

9.1.22 Document procedures for the secure disposal of media and assets to minimize the risk of confidential information leakage to unauthorized persons.

9.1.23 All users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

9.2 Information Classification and Sharing

The MCDA shall ensure that;

9.2.1 Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification and aligned to the access control policy
9.2.2 Each level shall be given a name that makes sense in the context of the classification scheme's application.
9.2.3 The scheme shall be consistent across the whole organization so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection.
9.2.4 Classification shall be included in the organization's processes, and be consistent and coherent across the organization. Results of classification shall indicate value of assets depending on their sensitivity and criticality to the organization. Results of classification shall be updated in accordance with changes of their value, sensitivity and criticality through their life-cycle.
9.2.5 Information confidentiality classification scheme shall be based on four levels as follows:
9.2.6 Disclosure causes no harm
9.2.7 Disclosure causes minor embarrassment or minor operational inconvenience
9.2.8 Disclosure has a significant short-term impact on operations or tactical objectives
9.2.9 Disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.
9.2.10 MCDA shall ensure labelling of classified information using physical labels and metadata
9.2.11 MCDA shall ensure access restrictions supporting the protection requirements for each level of classification;
9.2.12 MCDA shall ensure maintenance of a formal record of the authorized recipients of assets;
9.2.13 MCDA shall ensure protection of temporary or permanent copies of information to a level consistent with the protection of the original information;
9.2.14 MCDA shall ensure storage of IT assets in accordance with manufacturers' specifications;
9.2.15 MCDA shall ensure clear marking of all copies of media for the attention of the authorized recipient.
9.2.16 MCDA shall document and implement the following guidelines to protect media containing information being transported:
9.2.17 Reliable transport or couriers shall be used;
9.2.18 A list of authorized couriers shall be agreed with management;
9.2.19 Procedures to verify the identification of couriers shall be developed;
9.2.20 Packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;
9.2.21 Logs shall be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

9.3 Business Continuity Management

MCDAs shall establish processes to ensure the prevention and recovery from potential threats to the organization to ensure that personnel and assets are protected and are able to recoverquickly in the event of a disruption/disaster.

9.3.1 Information Backup

MCDAs shall:

9.3.1.1 Define a backup policy to define the organization's requirements for backup of information, software and systems.

9.3.1.2 Design a backup plan, taking intoconsideration the following:

a) Accurate and complete records of the backup copies and documented restoration procedures.
b) The extent (e.g., full or differential backup) and frequency of backups
c) Criticality of the information to the continued operation of the organization;

9.3.1.3 Store backups in a remote location, at a sufficient distance to escape any physical damage from a disaster at the main site;

9.3.1.4 Establish the appropriate physical and environmental control measures to protect backup information consistent with the standards applied at the primarysite;

9.3.1.5 Regularly test backup media to ensure that they can be relied upon for emergency use when necessary;

9.3.1.6 Test the ability to restore backed-up data onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss;

9.3.1.7 Utilize encryption on backups where confidentiality is of great importance.

9.3.1.8 Monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups.

9.3.1.9 Establish backup arrangements ofinformationsystems, applications and data of critical systems that are necessary to recover the complete system in the event of a disaster.

9.3.1.10 Determine the retention period for essential business information, taking into account any requirement for archive copies to be permanently retained.

9.3.2 Business Continuity and Disaster Recovery Plan

MCDA shall develop, implement and maintain business continuity and disaster recovery plan.Information security requirements shall be determined when planning for business continuity and disaster recovery. MCDAs shall:

9.3.2.1 Establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation

9.3.2.2 Establish adequate management structure to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;

9.3.2.3 Appoint Incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated;

9.3.2.4 Develop approved plans, response and recovery procedures, detailing how the organization will manage a disruptive event based on management-approved information security continuity objectives

9.3.2.5 Establish and maintainsupporting systems and tools;

9.3.2.6 Develop processes, procedures and implementation changes to maintain existing information securitycontrols during an adverse situation;

9.3.2.7 Establish Compensating controls for information security controls that cannot be maintained during an adverse situation.

9.3.2.8 Establish appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements

9.3.2.9 Verify their information security management continuity by exercising and testing the functionality of information security continuity processes, procedures and controls to ensure consistency;

9.3.2.10 Identify business requirements for the availability of information systems. Where applicable, redundant information systems shall be tested to ensure the failover from one component to another component works as intended.

9.3.3 Availability

DRAFT

Critical MCDA systems shall be designed to be resilient to single failures of infrastructure and application components and as such shall run on robust reliable hardware and software supported by alternative or duplicate facilities.

9.4 Threat and Vulnerability Management

MCDAs shall identify, assess, classify, remediate, and mitigate security weaknesses to understand fully theroot cause of potential flaws in policy, process and, standards.

The MCDAs shall:

9.4.1 Develop and maintain an effective management process for technical vulnerabilities

9.4.2 Establish the roles and responsibilities associated with vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;

9.4.3 Identify Information resources that will be used to detect relevant technical vulnerabilities and to maintain awareness about them based on the asset inventory list.

9.4.4 Define timelines to react to notifications of potentially relevant technical vulnerabilities;

9.4.5 Identify associated risks and actions to be taken once a potential vulnerability is identified, such action could involve patching of vulnerable systems or applying compensating controls;

9.4.6 Test and evaluate patches before they are installed on a production system to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls shall be considered, such as:

9.4.6.1 Stopping services or capabilities related to the vulnerability where permissible

9.4.6.2 Adapting or adding access controls, e.g., firewalls, at network borders

9.4.6.3 Increased monitoring to detect actual attacks;

9.4.6.4 Raising awareness of the vulnerability;

9.4.7 Regularly monitor the vulnerability management process to ensure its effectiveness and efficiency;

9.4.8 Ensure alignment with the incident management policy to confirm an effective vulnerability management process in order to communicate vulnerabilities to the incident response function and informtechnical procedures to be carried out should an incident occur;

9.4.9 Define procedures to address the situation where vulnerability has been identified but there is no suitable countermeasure

9.4.10 Establish a formal policy prohibiting the use of unauthorized software and implement controls that prevent or detect the use of unauthorized software suspected malicious websites.

9.4.11 Establish a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, and reducing vulnerabilities that could be exploited by malware, e.g., through technical vulnerability management.

9.4.12 Regularly review the software and data content of systems supporting critical business to detect the presence of any unapproved files or unauthorized amendments which shall be formally investigated.

9.4.13 Carry out installation and regular updates of anti-malware software

9.4.14 Establish procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks shall be defined

9.4.15 Define and enforce strict policy on which types of software users may install and identify and document what types of software installations are permitted and what types of installations are prohibited.

10. OPERATIONAL SECURITY

MCDA shall ensure correct and secure operations of information processing facilities.

10.1 User End-point Device Security

DRAFT

10.1.1 General

MCDAs shall put measures to protect information stored, processed and accessed using endpoint devices and develop policies on secure configuration and handling end-point devices.

The policies should cover: -

- 10.1.1.1 Type of information and classification
- 10.1.1.2 Registration of the devices
- 10.1.1.3 Requirements for physical protection and restrictions of software installation
- 10.1.1.4 Access control and encryption
- 10.1.1.5 Protection against malware
- 10.1.1.6 Data loss\leakage prevention mechanisms in case of device loss or damage
- 10.1.1.7 End user data backup
- 10.1.1.8 Ensure awareness of security and procedures towards protection of end point devices

10.1.2 Bring Your Own Device

MCDAs shall:

- 10.1.2.1 Ensure network authentication, authorization and accounting of devices logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies havebeen enforced in the same manner as enterprise devices. E.g., valid anti-malware, genuine licensed and supported OS, non-approved software is not installed.
- 10.1.2.2 Ensure that users to acknowledge the understanding of their duties in upholding security by signing of acceptance use agreements and waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. This policy needs to take account of privacy legislation.
- 10.1.2.3 Establish procedures for reporting suspected breaches on personal devices.
- 10.1.2.4 Segregate networks being accessed by personal devices
- 10.1.2.5 Enforce a deactivation control on inactivity for a specified period of time, that requires a user to re-establish trust/connection.
- 10.1.2.6 Monitor activities performed by personal devices.

10.1.3 Remote Working

MCDAs shall implement measures to protect information accessed, processed and stored when personnel work remotely.

MCDAs shall develop a Remote Working policy that should cover: -

DRAFT

10.1.3.1 Secure mechanisms for deploying and initializing systems remotely, authentication and enablement of access privileges where remote access to the organization's network is allowed.

10.1.3.2 Security of devices used for remote working

10.1.3.3 Use secured network connections during remote working

10.1.3.4 Physical security at remote working sites to prevent unauthorized access to information or resources.

10.1.3.5 Use of remote access such as virtual desktop access that prevents processing and storage of information of privately owned devices.

10.1.3.6 Communications security requirements, taking into account the need for remote access to the organization's systems, the sensitivity of the information to be accessed and passed over the communication link and the sensitivity of the systems and applications;

10.1.3.7 The teleworker's PC configuration shall be protected, updated and monitored. Theusers understand their role in protecting corporate resources – e.g., appropriate useof resources, user should not modify security configuration, use of anti-virus software

10.1.3.8 Storage of corporate data on local drives and use of encryption tools

10.1.3.9 That a code of practice is signed by teleworkers for accountability if the requirements ofthe policy are contravened.

10.1.3.10 User support and preventive maintenance for remote worker and preventive maintenance respectively.

10.2 Collection of Evidence

MCDAs shall ensure effective evidence collection to sanction a consistent and effective management of evidence related to information security incidentsfor the purposes of disciplinary and legal actions.

MCDAsshall: -

10.2.1 Establish and implement procedures for the identification, collection, acquisition and preservation of evidence specific to the different storage media, and status of device.

10.2.2 Engage only qualified persons in the identifying analyzing and presenting digital evidence

10.2.3 Ensure that chain of custody is maintained

10.2.4 Ensure that the tools used in the digital forensics are accredited as sound forensics tools.

10.2.5 Ensure to collect evidences in alignment with applicable legal and regulatory requirements.

10.3 Protection Against Malware

The MCDA shall;

DRAFT

10.3.1 Implement rules and controls that prevent/control the use of unauthorized software.
10.3.2 Utilize anti-malware software to continuously scan data received through networks and electronic storage for malware.
10.3.3 Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
10.3.4 Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.
10.3.5 conducting regular automated validation of the software and data content of systems, especially for systems supporting critical business processes; investigating the presence of any unapproved
10.3.6 files or unauthorized amendments
10.3.7 Provide awareness training to all users on how to identify and potentially mitigate the receipt, sending or installation of malware infected emails, files or programs
10.3.8 Take care toprotect against the introduction of malware during maintenance and emergency procedures, which can bypass normal controls against malware
10.3.9 Implement a process to authorize temporarily or permanently disable some or all measures against malware, including exception approval authorities, documented justification and reviewdate
10.3.10 Determine the placement and configuration of malware detection and repair tools based on risk assessment outcomes

10.4 APIs and Interoperability

When implementing APIs and designing interoperability of systems the MCDA shall ensure
10.4.1 Validation of agreed standards for message formats to avoid transmission errors.
10.4.2 Encryption standards are agreed between the parties for API transactions.
10.4.3 Service account credentials must always be secured through encryption/hashing.
10.4.4 Usernames, passwords, session tokens, and API keys should not appear in the URL.
10.4.5 Validation of all request parameters to defend against injection attacks
10.4.6 Relevant error messaging without giving out too much information on the backend technologies.
10.4.7 Proper authentication and authorization to determine messages are from authorized parties only.
10.4.8 Establish controls to guard against manipulation of data in active transactions and attempts to alter transactions should issue alerts and be recorded.
10.4.9 Electronic signatures are used to safeguard against non-repudiation of transactions.
10.4.10 Message authentication codes exist to ensure messages are not altered during transmission.

10.5 Virtualization

In the deployment of virtualization technology MCDA shall take into consideration the following:

10.5.1 Isolation of the guest host from the host operating system e.g., file sharing should be disabled.
10.5.2 Both the host and virtual environments are hardened to only allow the intended use.
10.5.3 Hypervisors are patched as vendor fixes are released.
10.5.4 Access and visibility between the guests hosted within the host operating systems should be restricted
10.5.5 Security monitoring of the hypervisors and auditing to generate reports that flag suspicious configurations and communication between the guests.
10.5.6 Routinely inspect event and task logs

11. ACCESS CONTROL

MCDAs shall establish Control mechanisms based on business owner requirements and assessed/accepted risks for controlling logical access to all information assets to prevent unauthorized access.

DRAFT

11.1 Access control policy

MCDAs shallestablish, document and review an access control policy based on business and information security requirements.The policy shall take account of the following:

11.1.1 Information dissemination and authorization considering least privilege and the need-to-know principle and information security levels and classification of information

11.1.2 Consistency between the access rights and information classification policies of systems and networks;

11.1.3 Relevant legislation and any contractual obligations regarding limitation of access to data or services

11.1.4 Management of access rights in a distributed and networked environment which recognizes all types of connections available;

11.1.5 Segregation of access control roles, e.g., access request, access authorization, access administration;

11.1.6 Requirements for formal authorization of access requests

11.1.7 Requirements for periodic review of access rights

11.1.8 Requirements for disabling and removal of access rights

11.1.9 Archiving of records of all significant events concerning the use and management of user identities and secret authentication information;

11.1.10 Restrictions to privileged access

11.1.11 Physical Access supported by appropriate physical controls

11.1.12 Logging of user access events

11.1.13 Requirements to Access to networks and network services

11.1.13.1 Management controls and procedures to protect access to network connections and network services;

11.1.13.2 The means used to access networks and network services (e.g., use of VPN or wireless network);

DRAFT

11.2 Access control to program source code

MCDA shall: -

11.2.1 manage Read and write access to source code, development tools and software libraries Where possible, program source libraries shall not be held in operational systems;

11.2.2 Establish procedures to centrally manage the program source code and the program source libraries

11.2.3 Access to source code shall be granted based on business need and managed to address risks of alteration/misuse.

11.2.4 The updating of program source libraries and associated items and the issuing of program sources to programmers shall only be performed after appropriate authorization has been received and through change control procedures

11.2.5 Program listings shall be held in a secure environment;

11.2.6 An audit log should be maintained of all accesses to program source libraries;

11.2.7 Maintenance of source code and program source libraries shall be subject to strict change control procedures

11.3 Identity management

MCDAs shall establish procedures to follow when granting users system access to the resources they need at the as and when needed, this includes access to applications, permissions, and security requirements.

11.3.1 User registration and de-registration

MCDAs shall:

11.3.1.1 develop a formal user registration and de-registration process to enable assignment of access rights.The process for managing user IDs should include:

11.3.1.2 Using unique user IDs to enable users to be linked to and held responsible for their actions; the use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented;

11.3.1.3 Immediately disabling or removing user IDs of users who have left the organization

11.3.1.4 Periodically identifying and removing or disabling redundant user IDs;

11.3.1.5 Identities assigned to non-human entities are subject to appropriately segregated approval and independent ongoing oversight

11.3.2 User access provisioning

MCDAs shall provision, modify and review access rights in line with the Access Control Policy.

11.3.3 Administrative Privileges

The MCDA shall:

DRAFT

11.3.3.1 Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

11.3.3.2 Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

11.3.3.3 Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not daily user activities.

11.3.3.4 Where multi-factor authentication is not supported, accounts will use passwords that are unique to that system.

11.3.3.5 Use multi-factor authentication and encrypted channels for all administrative account access.

11.3.3.6 Limit access to scripting tools to only administrative or development users with the need to access those capabilities.

11.3.3.7 Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

11.3.3.8 Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

11.4 Privileged access rights

MCDAs shall:

11.4.1 Ensure the allocation of privileged access rights is controlled through a formal authorization process in accordance with the relevant access control policy.

11.4.2 Conform to the password policy with regards to privileged accounts

11.4.3 Identify the privileged access rights associated with each system or process, e.g., operating system, database management system and each application and the users to whom they need to be allocated should be identified;

11.4.4 Allocate Privileged access rights shall be allocated to users on a need-to-use basis and on an event-by event basis in line with the access control policy i.e., based on the minimum requirement for their functional roles;

11.4.5 Assign privileged access rights to a user ID different from those used for regular business activities. Regular business activities shall not be performed from privileged ID;

11.4.6 Regularly review access rights and competences of users with privileged access to verify if they are in line with their duties;

11.4.7 Establish and maintain specific procedures to avoid the unauthorized use of generic administration user IDs, according to systems' configuration capabilities;

11.4.8 Maintain the confidentiality of secret authentication when shared for generic administration user IDs, (e.g., changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

11.4.9 Logall privileged access for audit purposes.

11.5 Management of Authentication Information

DRAFT

MCDA shall;

11.5.1 Document procedures on allocation and management of secret authentication information. It should include the following:

11.5.2 Require users to sign a statement to keep personal secret authentication information confidential and to keep group (i.e., shared) secret authentication information solely within the members of the group; this signed statement may be included in the terms and conditions of employment

11.5.3 Ensure users maintain their own secret authentication When users are required to maintain their own secret authentication information, they shall be provided initially with secure temporary secret authentication information`, which they are forced to change on first use;

11.5.4 Procedures shall be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information;

11.5.5 Secret authentication information should be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages should be avoided;

11.5.6 Temporary secret authentication information should be unique to an individual and shall not be guessable;

11.5.7 Users shall acknowledge receipt of secret authentication information;

11.5.8 Default vendor secret authentication information shall be altered following installation of systems or software.

11.5.9 Ensure unique passwords for secret authentication information. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens (e.g., smart cards) that produce authentication codes.

11.5.10 User acknowledgement

11.5.11 Change of default authentication information

11.5.12 Secure management of authentication of events records.

11.5.13 Ensure that users are aware of their responsibility on confidentiality of passwords, and immediate change of authentication information in case of compromise.

11.5.14 Develop a password policy and implement a password management system to establish password guidelines and enforce them.

11.6 Review of user access rights

11.6.1 MCDA shall review logical and physical access rights at regularintervals. Authorizations for privileged access rights should be reviewed at more frequent intervals;

11.6.2 Changes to privileged accounts should be logged for periodic review.

11.7 Removal or adjustment of access rights

MCDAs shall revoke/adjustaccess rights of all employees and external party users to information andinformation processing facilities shall be removed upon termination of their employment, contract or agreement.

DRAFT

11.8 Information access restriction

The MCDA shall;

11.8.1 Ensure that access to information and other associated assets is restricted in accordance with access control policy.
11.8.2 Implement restrictions to access based on individual business application requirements and in accordance with the defined access control policy and consider the following in order to support access restriction requirements:
11.8.3 Providing menus to control access to application system functions;
11.8.4 Controlling which data can be accessed by a particular user;
11.8.5 Controlling the access rights of users, e.g., read, write, delete and execute;
11.8.6 Controlling the access rights of other applications;
11.8.7 Limiting the information contained in outputs, applications or systems.

11.9 Child Online Protection

MCDAs will ensure that they enforce child online safety policy on internet use bysetting up measures that protect children online.

MCDAs shall:

11.9.1 Protect access by minors from inappropriate content on the Internet.
11.9.2 Ensure the Safety and security of minors when using electronic mail, chat rooms andother forms of direct electronic communications under their responsibility.
11.9.3 Control unauthorized access and other unlawful activities by minors online
11.9.4 Control unauthorized disclosure, use, and dissemination of personal informationregarding minors; and
11.9.5 Provide measures restricting minors' access to materials harmful to them.

11.10 Data Masking

MCDAs shall:

11.10.1 Implement data masking in accordance with the Access control policy, business requirements and applicable legislation to limit exposure of PII.
11.10.2 Employ techniques such as data masking, pseudo-anonymization and anonymization

11.11 Secure log-on procedures

MCDAs shall

DRAFT

11.11.1 Design a procedure for logging into a system to minimize the opportunity for unauthorized access. The log-on procedure shall disclose the minimum information about the system or application, in order to avoid providing an unauthorized user with any unnecessary assistance.

11.11.2 Not display system or application identifiers until the log-on process has been successfully completed;
11.11.3 Display a general notice warning that the computer should only be accessed by authorized users;
11.11.4 Not provide help messages during the log-on procedure that would aid an unauthorized user;
11.11.5 Validate the log-on information only on completion of all input data. If an error condition arises, the system shall not indicate which part of the data is correct or incorrect;
11.11.6 Protect against brute force log-on attempts;
11.11.7 Log unsuccessful and successful attempts;
11.11.8 Raise a security event if a potential attempted or successful breach of log-on controls is detected;
11.11.9 Display the following information on completion of a successful log-on:
11.11.10 Date and time of the previous successful log-on;
11.11.11 Details of any unsuccessful log-on attempts since the last successful log-on;
11.11.12 Not display a password being entered;
11.11.13 Not transmit passwords in clear text over a network;
11.11.14
11.11.15
11.11.16 Terminate inactive sessions after a defined period of inactivity, especially in high-risk locations such as public or external areas outside the organization's security management or on mobile devices;
11.11.17 Restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

11.12 Use of privileged utility programs

MCDAs shall:

11.12.1 Use identification, authentication and authorization procedures;
11.12.2 Ensure Segregation of utility programs from applications software;
11.12.3 Limit the use of utility programs to the minimum practical number of trusted, authorized users
11.12.4 Ensure authorization for ad hoc use of utility programs;
11.12.5 Limit the availability of utility programs, e.g., for the duration of an authorized change;
11.12.6 Log of all use of utility programs;
11.12.7 Removal or disabling of all unnecessary utility programs;

11.13 Change Management

MCDA shalldevelop change management policies and procedures to preserve information security when executing changes in information processing facilities. The policy shall cover:

DRAFT

11.13.1 The identification and recording of significant changes;
11.13.2 Planning, testing and assessing potential impacts of changes
11.13.3 Verification that information security requirements have been met;
11.13.4 Implementation of changes including deployment plans.
11.13.5 Communication of change details to all relevant persons;
11.13.6 Fall-back procedures, including procedures and responsibilities for aborting and recovering from
11.13.7 Unsuccessful changes and unforeseen events;
11.13.8 Update operating documentation, user procedures and continuity plan to reflect the change
11.13.9 An audit log containing all relevant information shall be retained.
11.13.10 MCDA shall Test information is selected to ensure the reliability of test results and confidentiality of the relevant operational information.

11.14 Incident Management

11.14.1 Management of information security incidents and improvements

MCDA shall ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

11.14.2 Responsibilities and procedures

MCDAs shall establish management responsibilities and develop the following procedures to ensure a quick, effective and orderly response to information security incidents.

11.14.2.1 Procedures for incident response planning and preparation;
11.14.2.2 Procedures for monitoring, detecting, analyzing and reporting of information security events and incidents;
11.14.2.3 Procedures for logging incident management activities;
11.14.2.4 Procedures for handling of forensic evidence;
11.14.2.5 Procedures for assessment of and decision on information security events and assessment of information security weaknesses;
11.14.2.6 Procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organizations;

11.14.3 Procedures established shall ensure that:

11.14.3.1 competent personnel handle the issues related to information security incidents within theorganization;
11.14.3.2 a point of contact for security incidents' detection and reporting is implemented;
11.14.3.3 appropriate contacts with relevant entities, external interest groups or forums that handle the issuesrelated to information security incidents are maintained;

11.14.4 Reporting procedures

MCDAs shall:

DRAFT

11.14.4.1 Ensure all employees and contractors shall be made aware of their responsibility to report information security events as quickly as possible.

11.14.4.2 Establish an internal process for identifying and reporting security incidents.

11.14.4.3 Create awareness to employees on its internal incident reporting process.

11.14.4.4 Establish a suitable feedback process to ensure that those persons reporting information security events are notified of results after the issue has been dealt with and closed.

11.14.5 Assessment of information security events

11.14.5.1 Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents

11.14.5.2 The point of contact shall assess each information security event using the agreed information security event and incident classification scale and decide whether the event shall be classified as an information security incident.

11.14.5.3 Classification and prioritization of incidents can help to identify the impact and extent of an incident.

11.14.5.4 In cases where the organization has an information security incident response team (ISIRT), the assessment and decision can be forwarded to the ISIRT for confirmation or reassessment.

11.14.5.5 Results of the assessment and decision shall be recorded in detail for the purpose of future reference and verification.

11.14.6 Response to information security incidents

MCDA shall document procedures for response to information security incidents which shall include the following:

11.14.6.1 Collecting evidence as soon as possible after the occurrence;

11.14.6.2 Conducting information security forensics analysis

11.14.6.3 Escalate as required;

11.14.6.4 Ensuring that all involved response activities are properly logged for later analysis;

11.14.6.5 Communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;

11.14.6.6 Dealing with information security weakness(es) found to cause or contribute to the incident;

11.14.6.7 Once the incident has been successfully dealt with, formally closing and recording it.

11.14.6.8 Post-incident analysis should take place, as necessary, to identify the source of the incident.

11.14.7 Learning from information security incidents

11.14.7.1 Knowledge gained from analyzing and resolving information security incidents shall be documented and used to reduce the likelihood or impact of future incidents.

11.14.7.2 There shall be mechanisms in place to enable the types, volumes and costs of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

11.14.8 Collection of digital evidence

DRAFT

11.14.8.1 The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

11.14.8.2 Where available, certification or other relevant means of qualification of personnel and tools shall be sought, so as to strengthen the value of the preserved evidence.

11.14.8.3 The procedures shall take account of:

a) chain of custody;
b) safety of evidence;
c) safety of personnel;
d) roles and responsibilities of personnel involved;
e) competency of personnel;
f) documentation;
g) incident briefing

11.14.9 Threat Intelligence

MCDAs shall:

11.14.9.1 Collect and analyze information security threats to provide an understanding of the organizations' threat landscape.

11.14.9.2 Share threat findings with relevant Authorities and special groups

11.14.9.3 Collect threat information of all types to produce contextual and actionable analysis.

11.14.9.4 Establish processes to utilize information gathered from threat analysis and sources into the organization's information security risk management process.

11.14.10 Event logging

MCDAs shall produce, store, protect and analyze information security event logs exceptions and faults for systems to ensure integrity of log information, to prevent against unauthorized access and support investigation.

11.14.10.1 Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures shall be taken

11.14.10.2 System administrators shall not have permission to erase or de-activate logs of their own activities

11.14.11 Protection of log information

MCDAs shall protect Logging facilities and log information against tampering and unauthorized access.

11.14.12 Administrator and operator logs

MCDAs shall log and regularly review system administrator and system operator activities.

11.14.13 Clock synchronization

MCDAs shall ensure:

11.14.13.1 External and internal requirements for time representation, synchronization and accuracy are documented.

11.14.13.2 A standard reference time for use within the organization shall be defined.The organization's approach to obtaining a reference time from external source(s) and how to synchronize internal clocks reliably is documented and implemented.

DRAFT

11.15 Physical and environmental security

MCDAs shallensure:

11.15.1 Security perimeters or areas that contain either sensitive or critical information or information processing facilities are defined.

11.15.2 The date and time of entry and departure of visitors shall be recorded, and all visitors shall be supervised.

11.15.3 Access to areas where confidential information is processed or stored shall be restricted to authorized individuals.

11.15.4 All employees, contractors and external parties shall be required to wear some form of visible identification and shall immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.

11.15.5 External party support service personnel shall be granted restricted access to secure areas or information processing facilities only when required; this access shall be authorized and monitored.

11.15.6 Access rights to secure areas shall be regularly reviewed and updated, and revoked when necessary

11.15.7 Establish measures to protect against external and environmental threats such as earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

11.15.8 Buildings shall be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;

11.15.9 Directories and internal telephone books identifying locations of information processing facilities shall not be readily accessible to anyone unauthorized.

11.15.10 Access to a delivery and loading area from outside of the building shall be restricted to identified and authorized personnel;

11.15.11 The delivery and loading area shall be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building; -

11.15.12 The external doors of a delivery and loading area shall be secured when the internal doors are opened;

11.15.13 Incoming material shall be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area;

11.15.14 The following cabling security controls shall be implemented

11.15.14.1 Power and telecommunications lines into information processing facilities shall be underground, where possible, or subject to adequate alternative protection;

11.15.14.2 Power cables shall be segregated from communications cables to prevent interference;

11.15.14.3 For sensitive or critical systems further controls to consider include:

a) Installation of armored conduit and locked rooms or boxes at inspection and termination points;
b) Use of electromagnetic shielding to protect the cables;
c) Initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;
d) Controlled access to patch panels and cable rooms.

DRAFT

11.15.15 Establish procedures for secure removal of assets from information processing facilities.

11.15.16 The use of any mission critical information storing and processing equipment outside the organization's premises shall be authorized by management. This applies to equipment owned by the organization and that equipment owned privately and used on behalf of the organization.

11.15.17

11.15.18 Packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;

11.15.19 Logs shall be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

12. CRYPTOGRAPHY

MCDAs shall apply cryptography to secure information with the objective is to protect confidentiality, Authenticity or Integrity of Information.

12.1Cryptographic controls

MCDAs shall develop and implement a policy on the use of encryption for protection of information. The policy shall address the following:

12.1.1 Use of cryptographic controls

12.1.2 Principles under which business information should be protected

12.1.3 Type, strength and quality of the encryption algorithm required

12.1.4 The use of encryption on information transported by mobile or removable media devices or across communication lines

12.1.5 Methods to deal with the protection of cryptographic keys and the recovery of encrypted information.

12.1.6 Roles and responsibilities

12.1.7 Standards to be adopted

12.1.8 The impact of using encrypted information on controls

The MCDA shall consult relevant authorities to get specialist advice in selectingappropriate cryptographic controls.

12.2 Key Management

MCDAs shall:

12.2.1 Develop and implement a policy on the use, protection and lifetime of cryptographic keys. The policy shall be based on agreed set of standards, procedures and secure methods for generating and managing keys.

12.2.2 Define the Activation and deactivation dates for keys to reduce the likelihood of improper use.

12.2.3 Consider the authenticity of public keys to securely manage secret and private keys.

12.2.4 Develop the contents of service level agreements or contracts with external suppliers of cryptographic services to cover issues of liability, reliability of services and response times for the provision of services

12.2.5 Establish procedures to be considered for handling legal requests for access to cryptographic keys.

12.3 Digital Signatures

MCDAs shall:

DRAFT

12.3.1 Utilize use digital signature certificates duly issued by a licensed certifying authority.
12.3.2 Define the roles and responsibility of various users for the usage of Digital Signature and their revocation
12.3.3 **I**mmediately contact the respective Certifying Authority to initiate revocation **when** a Digital Signature Certificate is compromised.

12.4 E-Commerce

MCDAs shall:
12.4.1 Take measures to protect Personal Identifiable Information of their clients.
12.4.2 Encrypt transmission of confidential information sent through open and public networks.
12.4.3 Protect systems against malware through regular scanning and updating of the anti-malware solutions.
12.4.4 Develop and maintain secure systems and applications through secure software development lifecycle and vulnerability management
12.4.5 Restrict access to sensitive customer information to a "need to know" basis.
12.4.6 Uniquely identify and authenticate access to system components and users to ensure accountability of access to critical data systems.
12.4.7 Tracking and monitoring all access to confidential information through logging mechanisms
12.4.8 Test security systems and processes regularly.
12.4.9 Take into consideration mechanisms and procedures that taken together constitute a security architecture for e-commerce e.g., internet firewalls, Public Key Infrastructure (PKI), Payment Card Industry Data Security Standard (PCI DSS) compliance, password and authentication management.

DRAFT

13. SUPPLIER RELATIONSHIPS

13.1 Supplier Relationships

13.1.1 Information security in supplier relationships

MCDAs shall:

13.1.1.1 Establish policies, procedures and processes to manage information security risks related to supplier products and services.

13.1.1.2 Maintain an inventory of suppliers Identifying and documenting the types of suppliersand components supplied that can impact information security.

13.1.1.3 Establish a standardized process to manage the supplier relationship lifecycle defining the types of information accessed, transferred and compliance to MCDA security requirements.

13.1.1.4 Define information assets that suppliers can access, monitor, control and use.

13.1.1.5 Establish processes and procedures for monitoring adherence to established information security requirementsfor each type of supplier and type of access, including third party review and product validation;

13.1.1.6 Handle incidents, resilience, recovery and contingencyarrangementsassociated with supplier access including responsibilities of both the organization and suppliers;

13.1.1.7 Conduct awareness training for the organization's personnel interacting with suppliers regarding appropriate rules of engagement and based on the type of supplier and the level of access to the organization information.

13.1.2 Addressing security within supplier agreements

13.1.2.1 Supplier agreements shall be established and documented rules of engagement and obligations between the organization and the Supplier.

13.1.2.2 Terms specified in ANNEX to supply agreements shall be considered for inclusion in the contract. Description of the information to be provided or accessed and methods of providing or accessing the information;

13.1.2.3 Classification of information according to the organization's classification scheme.

13.1.2.4 Legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;

13.1.2.5 Obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;

13.1.2.6 Rules of acceptable use of information, including unacceptable use if necessary;

13.1.2.7 explicit list of supplier personnel authorized to access or receive the organization's information.

13.1.2.8 Information security policies relevant to the specific contract;

13.1.2.9 Incident management requirements and procedures (especially notification and collaboration during incident remediation);

13.1.2.10 Training and awareness requirements for specific procedures and information security requirements, e.g., for incident response, authorization procedures;

13.1.2.11 Relevant regulations for sub-contracting, including the controls that need to be implemented;

13.1.2.12 Relevant agreement partners, including a contact person for information security issues;

13.1.2.13 Screening requirements, for supplier's personnel including responsibilities for conducting the screening and notification procedures.

13.1.2.14 Right to audit the supplier processes and controls related to the agreement;

13.1.2.15 Defect resolution and conflict resolution processes Supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;

13.1.2.16 Supplier's obligations to comply with the organization's security requirements.

DRAFT

13.1.3 Managing information security in ICT supply chain

MCDAs shall:

13.1.3.1 Define information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;

13.1.3.2 For information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;

13.1.3.3 For information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;

13.1.3.4 Implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

13.1.3.5 Implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;

13.1.3.6 Obtaining assurance that critical components and their origin can be traced throughout the supply chain;

13.1.3.7 Obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;

13.1.3.8 Defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

13.1.3.9 Implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks

13.1.3.10 This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

13.2 Supplier service delivery management

MCDAs shall regularly monitor, review and audit supplier service delivery and shall involve:

13.2.1 Monitoring service performance levels to verify adherence to the agreements;

13.2.2 Reviewing service reports produced by the supplier and arrange regular progress meetings as required by the agreements;

13.2.3 Conducting audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;

13.2.4 Providing information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

13.2.5 Reviewing supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

13.2.6 Resolving and manage any identified problems;

13.2.7 Review information security aspects of the supplier's relationships with its own suppliers;

13.2.8 Ensuring that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster

DRAFT

14. COMPLIANCE

14.1 Identification of applicable legislation and contractual requirements

MCDAs shall identify applicable legal, regulatory and contractual requirement related to information security and document theorganizations' commitment to meet the requirements.

MCDA shall institute mechanisms to review and monitor changes to, regulatory or contractual and ensure compliance.

14.2 Intellectual property rights

MCDAs shall:

14.2.1 Establish a policy to govern protection of intellectual rights in accordance to existing legal frameworks.
14.2.2 Publish procedures for acquiring software only through known and reputable sources, to ensure that copyright is not violated;
14.2.3 Maintain awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them;
14.2.4 Maintain appropriate asset registers and identify all assets with requirements to protect intellectual property rights;
14.2.5 Carry out reviews at regular intervals to ensure that only authorized software and licensed products are installed;

14.3 Protection of records

MCDAs shall protect records from falsification, loss, leakage and access as per legal, regulatory and business requirements.

MCDAs shall establish guidelines on secure management of records throughout the document life cycle.

14.4 Privacy and protection of personally information

MCDAs shall:

14.4.1 Develop and implement a data policy for privacy and protection of personally identifiable information as guided by applicable Legal and regulatory requirements. Compliance with security policies, rules and standards
14.4.2 Regularly review the compliance of information processing and procedures within area of responsibility with the appropriate security policies, standards and

INDEPENDENT REVIEW OF INFORMATION SECURITY

MCDAs shall periodically or when changes occur conduct independent reviews of information security to ensure information security assurance.

MCDAs to report the results of information security independent reviews to relevant Authorities.

DRAFT

15. APPENDIX I: Compliance Checklist for information Security

Sub-domain	Subject	CODE	Requirement	Compliance {Yes/No}	Comments
Information Security Governance and Management	Information security policy	1	An information security policy exists		
		2	All mandatory clauses in the standard can be located in the information security policy		
		3	There has been consultation across major business areas within the MCDA		
		4	Business requirements have been documented within the policy		
		5	A risk assessment has been documented and the results have informed the development of the policy		
		6	Legislative requirements relevant to the MCDA have been documented within the policy		
		7	Staff are aware of and trained in the use of the policy with refresher courses available		
		8	The policy can be easily accessed by all employees		
		9	Senior Executive signoff/endorsement can be located within the policy or brief		
		10	The date of the policy's last review is no more than 24 months old		
		11	The date for the policy's next review is documented within the policy, and appropriate review mechanisms in place		
	Information Security Plan	12	An information security plan exists		
		13	There has been consultation across major		

DRAFT

			business areas within the MCDA and business requirements have been documented within the plan		
		14	A risk assessment has been documented and the results have informed the development of the plan		
		15	A threat and risk assessment has been conducted and documented for all ICT assets that create, store, process or transmit security classified information. The date of the last assessment is no more than 12 months old		
	Governance	16	Senior executive management group agenda/minutes include information security matters		
		17	There's an information security steering committee		
		18	Information security roles and responsibilities documented and approved by senior executive management		
		19	Employees with information security roles and responsibilities have signed a document stating that they understand their roles and responsibilities		
	External Party Governance	20	Standard templates for service level agreement and operational level agreements include clauses dealing with information security requirements		
		21	Minutes of Information security steering committee meetings include outcomes of routine checks on inclusion of information security requirements in SLAs, and audits to ensure third party adherence to these		

DRAFT

			agreements		
	Information Security Risk Management	22	Risk management plan has been put in place that includes identification, qualification and prioritisation of risks against acceptance criteria and identifies appropriate controls to protect against risks.		
		23	Risk analysis against the agencies information Asset register has been completed		
Information Resource Management	Data Security	24	MCDA Records Management Program in Place. MCDA has an Information Management Policy outlining governance arrangements, roles and responsibilities of all staff for the management of information		
		25	Records Manager appointed with up-to-date statement of duties		
		26	Information asset register in place, Information Owners and Custodians are identified on the register. MCDA has security classified each asset.		
	Information Asset Register	27	Procedures for the protective control of information assets have been documented and approved by the Information security committee body		
		29	An ICT asset register exists, that documents the security classification of application and technology assets (in accordance with the policy and the manual or in the case of national security information relevant national arrangements) and the corresponding controls that are applied to that asset (actual controls may be documented elsewhere)		

DRAFT

		30	ICT asset register has been completed and is updated at least annually		
		31	ICT asset register identifies the ICT asset custodian for all assets		
	Information Security Classification	32	Procedures for the classification of information assets have been documented and approved by the Information security c0mmittee		
		33	MCDA has a complete information asset register, where all information assets are assigned a classification, or in the case of national security information, as per national arrangements		
		34	The information security classification policy and procedure document state that legislative obligations override the classification scheme. For example, the security classification of an information asset does not prevent it from being considered for release under the freedom of information		
Physical Environment Security	Building controls and security areas	35	Physical security protection controls (commensurate with the security classification of information levels) have been implemented for all offices, rooms, storage facilities and cabling infrastructure in line with the standards		
		36	Control policies (including clear desk/clear screen) has been implemented in information processing areas that deal with security classified information		
	Asset Management	37	MCDA equipment is located in secure areas. Records of routine checks confirm that these areas		

DRAFT

			are accessible only to authorised personnel		
		38	MCDA information security policies address the protection and monitoring of ICT assets that are offsite		
		39	Policies are implemented for the secure disposal or reuse of ICT assets which are commensurate with the information asset's security classification level		
		40	Processes are implemented for the secure disposal or reuse of ICT assets which are commensurate with the information asset's security classification level		
Information and Communications Technology	Operational procedures and responsibilities	41	Operational procedures ensuring information assets and ICT assets, including information systems and network tasks, are managed consistently in accordance with the required level of security, have been documented and approved		
	Third Party Service Delivery	42	Agreements clearly articulate the level of security required, are regularly monitored and endorsed by the relevant senior executives and governance body		
	Capacity planning and system acceptance	43	System acceptance include confirmation of the application of appropriate security controls and of the capacity requirements of the system		
		44	System capacity is regularly monitored to ensure risks of system overload or failure, which could lead to a security breach, are avoided		
	Malicious and Mobile Code Control	45	Adequate controls have been defined and implemented for the prevention, detection,		

DRAFT

			removal and reporting of attacks of malicious code on all ICT assets		
		46	Details of vulnerability/integrity scans have been documented including what core software has been scanned, when it has been scanned, when the next scan is due, and the scan results		
		47	Employee education about malicious code and associated processes have been conducted, for example through induction programs, training programs/plans and awareness campaigns (e.g., emails, posters, factsheets, intranet contents etc)		
	Backup procedures	48	Comprehensive systems maintenance processes and procedures (including operator and audit/fault logs), information backup procedures and archiving have been implemented		
	Network security	49	Network security policy and guidelines have been documented and approved. Network administrators are aware of and follow these documents		
		50	Firewall rule and associated network architecture testing processes are documented. MCDA records document tests, their results and any corrective action taken		
		51	Processes for reviewing and updating network security design, configuration, vulnerability and integrity are documented. MCDA		

DRAFT

			records demonstrate that periodic network security checks, reviews and updates are occurring		
		52	A policy on scanning has been documented and approved. Supporting processes to ensure adherence to the manual have also been developed		
		53	Processes relating to IT change management (including maintenance of network systems) and configuration management processes are established and updated as required		
	Information Technology Media Management	54	Media handling procedures have been documented and implemented		
		55	All the requirements of the manual have been documented within these procedures		
	Electronic Information Transfer	56	A Network policy has been implemented to ensure the security of data during transportation over communication networks		
		57	Methods for exchanging information within the MCDA, between agencies, through online services, and/or third parties are compliant with legislative requirements		
		58	Appropriate authorisation has been obtained and documented for the type and level of encryption used within the MCDA.		
		59	All information exchanges over public networks, including all online or publicly available transactions/systems must be authorised either directly or through clear policy		
		60	A policy to control email, has been approved by the		

DRAFT

			relevant senior executive/governance body and has been implemented within the MCDA		
	e-commerce	61	Details of penetration testing have been documented, including what critical online services have been tested, when the testing has occurred, when the next test is due and test results		
		62	Policies and controls have been developed to manage all aspects of on-line and internet activities including anonymity/privacy, data confidentiality, use of cookies, applications/plug-ins, types of language used, practices for downloading executables, web server security configuration, auditing, access controls and encryption		
		63	There is a policy for adoption of PKI digital signatures for e-commerce		
	Security Audit Logging	64	Details of operator and audit/fault logs have been documented including what events are logged, when and who will review and monitor logs, where and for how long the logs are stored, are logs adequately protected		
		65	All assets have a synchronized time source which is visible		
Identity and Access Management	Access Control Policy	66	Control mechanisms based on business owner requirements and assessed/accepted risks for controlling access to all information assets and ICT assets have been established		
		67	Access control rules are		

DRAFT

			consistent with business requirements		
		68	Access control rules are consistent with information classification		
		69	Access control rules are consistent with legislative obligations		
	Authentication	70	MCDA records indicate that all authentication requirements have been assessed against the standard. Business requirements for all online transactions and services include consistency with the standard. MCDA records indicate that online transactions and services have been assessed against the standard		
		71	MCDA records indicate that all authentication of users external to the MCDA have been assessed against the standard		
	User access	72	MCDA information systems cannot be accessed without specific authorisation. MCDA records that may indicate evidence of compliance include completed system access request forms for all users		
		73	MCDA records indicate that each user is issued a unique personal identification code and secure means of authentication		
	Network access	74	MCDA records indicate that system and network access and use is logged, monitored and reviewed. Events are recorded		
		75	MCDA records indicate that authorisation has been obtained and documented for new and		

DRAFT

			existing access to networks		
		76	All wireless communications have appropriate configured product security features and afford at least the equivalent level of security of wired communications		
		77	MCDA records indicate that a risk assessment has been performed for all ICT facilities and devices (including non-government equipment) prior to connection. Records all indicate that appropriate controls have been implemented based on this risk assessment		
	Operating system access	78	MCDA has documented and approved access controls for operating systems that cover user registration, authentication, user responsibilities. Access to operating systems is conducted in compliance with these controls		
	Mobile computing and tele-work access	79	MCDA records indicate that mobile technologies and tele-working facilities are not introduced unless a risk assessment has been performed		
		80	MCDA has documented and approved processes for mobile technologies and teleworking facilities		
Information Systems Acquisition Development and Maintenance	Security Systems Requirements	81	MCDA system security controls are commensurate with the highest level of security classification of the information stored and passing through the system		
		82	Business requirements for all systems include information security requirements		
		83	Records of audit results are documented for new		

DRAFT

			or significant changes to financial or critical business information systems		
		84	Documented system security controls address acquisition, development and maintenance stages		
		85	MCDA records document change control, acceptance and system testing, planning and migration control measures have been taken when upgrading or installing software		
		86	MCDA records document change control, acceptance and system testing, planning and migration control measures have been taken when upgrading or installing software		
		87	Access controls have been identified and implemented including access restrictions and segregation/isolation of systems into all infrastructures, business and user developed applications		
		88	Cryptographic controls are implemented		
		89	Access controls for system files are documented		
		90	Records of the processes for secure development have been documented		
		91	Audit logs for UNCLASSIFIED and security classified information log activity		
		92	Existence of an audit log for all technical vulnerability procedures		

DRAFT

			undertaken		
		93	Patch management program is implemented and documented including any tests that are carried out		
Personnel and Awareness	Pre-employment	94	Job descriptions include information security requirements		
		95	MCDA policies addressing information security issues within human resources have been approved by the senior executive management group/CEO		
		96	Procedures for addressing information security within human resource management have been document and approved		
		97	Induction program documentation includes information security		
		98	An information security training plan has been approved by the CEO (note that this may be part of the MCDA's general information security plan). Attendance records for information security training		
		99	Security awareness programs have been implemented to ensure that employees are aware of and acknowledge their security responsibilities. Example evidence of compliance might include emails, posters, fact sheets, intranet content etc that communicate information security responsibilities		
		100	Induction program documentation includes an overview of the MCDA's information security policies and processes and details of where employees can go to get		

DRAFT

			further information		
		101	The information security training plan includes targeted training in the MCDA's information security policies and processes		
		102	Training attendance records or documents signed by all employees that document that they have been shown and understand MCDA information security policies and processes including how to use MCDA ICT assets		
		103	Information security roles and responsibilities documented and approved by senior executive management		
		104	Roles and responsibilities have been physically assigned to employees (with appropriate records retained)		
		105	Employees with information security roles and responsibilities have signed a document stating that they understand their roles and responsibilities		
	Post-Employment	106	Procedures for the separation of employees within the MCDA have been approved		
		107	MCDA records demonstrate that all employee separations follow the approved procedure		
		108	Procedures for the movement of employees within the MCDA have been approved		
		109	MCDA records demonstrate that all employee movements within the MCDA follow the approved procedure		
Incident Management	Incident Management Controls	110	Copies of information security incident reports are present. Receipt of incident reports by		

DRAFT

			relevant management channels		
		111	Agency records indicate that information security incidents are reported to appropriate authorities (e.g., police) where applicable		
		112	Training attendance records or documents signed by all employees, contractors and third parties that document that they understand their responsibilities to report events/weaknesses and incidents		
	Incident procedures	113	Agency information security 30 procedures have been documented and covers the review of and response to incidents		
		114	Records of information security incident reports and corresponding investigations are present.		
		115	Disciplinary processes for deliberate violations or breaches of information security policy have been approved by the senior executive management group/CEO. Where these incidents have occurred, agency records demonstrate that these processes have been applied		
		116	Existence of a current agency information security incident and response register		
Business Continuity Management	Business continuity	117	Business continuity plans have been established to enable information and ICT assets to be restored or recovered in the event of a major security failure		
		118	Processes that enable the information environment to be restored or recovered in the event of a major information security failure have been		

DRAFT

			approved		
		119	Business continuity risk and impact assessment processes have been approved. Agency records indicate that these assessments are made, and inform the development of the agency's business continuity plan		
		120	Existence of a risk register that documents how known risks will be managed		
		121	Business continuity plan is regularly updated. Business continuity tests are conducted and any weaknesses identified as a result are addressed Records show that a business impact analysis has been undertaken, and the results have been used to reduce risks		
		122	Records show that all critical business processes and associated assets have been identified, prioritised and documented		
	ICT Disaster Recovery	123	An information and ICT asset disaster recovery register has been established to assess and classify systems to determine their criticality		
		124	An ICT disaster recovery plan has been established to enable information and ICT assets to be restored or recovered in the event of a disaster		
		125	Processes that enable the information environment to be restored or recovered in the event of a disaster have been approved		
		126	Disaster recovery risk and impact assessment processes have been		

DRAFT

			approved. Agency records indicate that these are made, and inform the development of the agency's disaster recovery plan		
		127	Existence of a risk register that documents how known risks will be managed		
		128	Disaster recovery plan is regularly updated. Disaster recovery tests are conducted and any weaknesses identified as a result are addressed		
		129	Clearly defined maximum acceptable downtimes are documented within ICT disaster recovery plans		
		130	Maximum acceptable downtimes for ICT services are documented in all service and operational level agreements with external parties		
		131	Copies of ICT disaster recovery plans are located in multiple locations including at least one offsite location		
Monitoring for Compliance	Legal requirements	132	Agency has identified and documented all its legal obligations relating to information security and its response to these		
		133	A list of legislation compliance has been developed and is cross referenced against all information security policies and processes on a regular basis (including when changes to legislation occur)		
		134	The results of compliance reviews against information security policies and processes have been reported to		

DRAFT

			appropriate agency management		
		135	All information security requirements (including contracts with third parties) have been reviewed for legislative compliance on a regular basis		
		136	Agency has identified and documented processes for assessing compliance against its information security related legal obligations. Agency records indicate that these processes are being conducted		
	Policy Requirements	137	All reporting obligations relating to information security have been complied with and managed appropriately		
	Audit Requirements	138	All reasonable steps have been taken to monitor, review and audit agency information security compliance		
		139	Employees with information security roles and responsibilities have signed a document stating that they are understand their roles and responsibilities		

DRAFT

16. Appendix II: Guidelines

Subject	Requirement
General	• All MCDA computing resources must be used in an acceptable manner consistent with the policy. • Use may include, but is not limited to, access of Internet/Intranet/Extranet resources via web, email, file transfer or other network-based services, instant messaging, or accessing non- networked resources, such as through dedicated consoles or management systems. • The MCDA shall come up with acceptable use of computing resources (assets)
Definition and Ownership of Computing Resources	• Computing resources are defined as all digital or analog computational devices owned by the MCDA. • The MCDA owns all computing resources provided. Permission for use of computing resources is granted to employees on an as-needed basis in accordance with this and all other application policies and agreements. • These devices may include, but are not limited to, computer equipment, software, operating systems, storage media, network infrastructure, and network or local
Guidelines for Acceptable Use	The information security discipline evaluates risks according to the concepts of confidentiality, integrity and availability. The evaluation of risks may also weigh applicable laws and regulations as well as MCDA policies, standards, guidelines and procedures. The following guidelines are provided to assist users in making proper decisions about whether certain uses of computing resources are acceptable.
	1.Confidentiality Maintaining the confidentiality of data and people is of the utmost importance. When using computing resources, ask yourself the question: "Am I intentionally violating the confidentiality of the business, corporate data or an individual?" If the answer to this question is "yes" then determine whether or not you are authorized to view the information or data in question. If you are authorized, then determine whether or not you have a need to view the information or data. If you are not authorized to view the data or information, then do not view it. If you believe that you have inappropriate access to data or information, immediately report this finding to the proper owner or management.
	2.Integrity Integrity is defined as the soundness of data or systems and the certainty that data is authentic and unaltered. • Modifying data or information without proper authorization is unacceptable use and a violation of data integrity. • Accessing systems without proper authorization or through unapproved methods is also unacceptable and a violation of system integrity. • Always access data or systems through approved methods. If you believe that data or systems are accessible through unapproved methods, it is your responsibility to report the error. Violations of integrity may include, but are not limited to, • Circumvention of simple controls on data files, access to systems through unapproved methods, • Unauthorized escalation of privileges on a system, • Modifying data without permission, or • Intentionally corrupting data. Violation of data or system integrity on systems external to the MCDA through the use of MCDA assets is also unacceptable use.

DRAFT

	3.Availability Intentionally denying access to data or systems without authorization, or outside the intended function of an application or system is unacceptable use. Some applications and systems contain locking features designed to control access to data or processes (e.g., version control software). This behavior is expected and acceptable. Use of MCDA computing resources to deny access to internal or external systems is unacceptable use. When accessing data or systems, ask yourself the question: "Am I denying authorized access to data or systems as a result of my actions?" If the answer to this question is "yes" then determine whether you are authorized to undertake this action, and then determine whether or not there is a business need for the action. Availability also applies to client-side applications, such as mail readers and web browsers. Intentionally causing an application to crash, lock or otherwise perform errantly is unacceptable use. By extension, knowingly allowing your system to become or remain infected with malicious code may be deemed a violation of this policy. All perceived violations must be reported to the appropriate contact or management immediately. Reporting suspected infections in a timely manner will often exonerate a user from direct responsibility, pending the outcome of an investigation.
	4.Legal compliance It is important to be aware of applicable laws and regulations when accessing or using data or systems that are internal or external to the MCDA. Areas of consideration should include, but are not limited to, copyright, trademark, patent, privacy, wiretap, confidentiality and communication laws and regulations. Use of computing resources to violate laws or regulations represents a violation of this policy, regardless of intent or jurisdiction. Software must be used in accordance with its licensing terms and MCDA policies. Access of systems must not be in contravention of The Computer Fraud and Abuse Act (18 USC 1030) or other applicable laws. Use of systems to send communication in violation of Human Resources (HR) policies and applicable laws will be considered a serious breach of this policy and will be addressed swiftly and strictly. Communication must be appropriate for a business environment and in line with the Professional Standards of Conduct (PSC). All users are expected to act in a professional and courteous manner at all times and in all forms of communication. Suspected violations of this tenet of the policy should be reported to the appropriate contact immediately. The appropriate contact may be a member of management, HR, PSC or Legal. It is recommended that management be approached first, unless the suspected violation directly involves management.
	5.Policy compliance All users of computing resources must be familiar with applicable policies, standards, guidelines and procedures. Training and awareness programs will be provided to inform the user of corporate policies and applicable laws in order to ensure the ability of users to comply with acceptable computing policies. If a user is in doubt of whether or not a given action is acceptable, it is that user's responsibility to seek clarification before proceeding.
Specific Prohibitions and Restrictions on Use	The following activities are generally prohibited or restricted. Certain individuals may be exempted from these rules in order to perform their required job responsibilities (e.g., Operations Security is authorized to actively monitor network traffic and respond in a disruptive manner to mitigate a detected threat). Employees are not authorized, under any circumstances, to actively engage in activities deemed illegal under applicable jurisdictions. The list provided below is not comprehensive, but should be used as a baseline for helping determine whether or not a proposed action is unacceptable. Omission of an action from this list does not imply that it is an acceptable use. Any violations of these specific prohibitions and restrictions will be treated severely and may reasonably result in immediate termination of employment.

DRAFT

	1.Illegal use Computing resources must be used within the confines of the law. Any use of computing resources to infringe intellectual property protections, such as copyrights, trademarks, patents or trade secrets, is prohibited. Infringing acts may include, but are not limited to, unauthorized copying of copyrighted materials, use of a trademark without authorization or exporting software, technical information, encryption or technology in violation of export control laws. Any action, intentional or unintentional, that serves to copy or transmit protected materials without proper authorization is an unacceptable use.
	2.Threats, harassment or harm to minors Computing resources must not be used to threaten, harass or harm others. Unauthorized uses of this type may include, but are not limited to: • communication that is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, tortuous, or containing explicit or graphic descriptions or accounts of sexual acts (including but not limited to sexual language of a violent or threatening nature directed at another individual or group of individuals); • communication that victimizes, harasses, degrades, or intimidates an individual or group of individuals on the basis of religion, gender, sexual orientation, race, ethnicity, age, or disability; • any form of harassment via email, telephone, paging or instant messaging, whether through language, frequency, or size of messages; • use of computing resources to harm, or attempt to harm, minors in any way.
	3.Fraud, forgery or impersonation Any use of computing resources to commit fraud, forgery or impersonation is strictly prohibited. All users must truthfully and accurately represent their identity at all times. Adding, removing or modifying identifying network header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers, including email header information, or other identifying information is prohibited. Postings to public places intended to mask your employment status and employer, may be allowed. Users may not utilize computing resource to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters." Unless part of normal job duties, making statements about warranty, expressly or implied, is also prohibited.
	4.SPAM / SPIM Creation, sending and forwarding of unsolicited advertising, junk or bulk email ("SPAM") or instant messages ("SPIM") are strictly prohibited, unless explicitly authorized as part of your normal job duties. Undertaking any activities that serve to facilitate unsolicited commercial email or unsolicited bulk email, whether or not that email is commercial in nature, are prohibited. Use of instant messaging facilities to accomplish the same is also prohibited.
	5.Unauthorized access or circumvention of access controls Any access to systems or data that is not specifically authorized is prohibited. Any circumvention of access controls, whether for accessing systems with or without authorization, is also prohibited. Users may not circumvent authentication or security of any host, network or account.
	6.Collection of confidential data Use of computing resources to collect confidential data, such as about members, employees or intellectual property, is prohibited. Collection, or attempts to collect, personal information about third parties, without their knowledge or consent, is prohibited and may constitute a violation of MCDA privacy policies and agreements. The MCDA strictly

DRAFT

	limits its liability in cases where individuals act of their own accord and without proper authorization. Any attempts to harvest or collect confidential data without explicit and proper authorization is prohibited and will be subject to severe disciplinary actions, up to and including termination of employment.
	7.Disrupting network services or access to data Rendering systems, networks, applications or data inaccessible or unusable due to an unauthorized disruption or corruption, is prohibited. Such prohibited acts may include, but are not limited to, ping floods, packet spoofing, executing denial of service or distributed denial of service attacks, forging routing information, corrupting data upon which an application or system relies, or removing or disabling a service, such as a process or application, on a host or network. Port or security scanning without prior authorization by Operations Security is strictly prohibited. Using any automated tool, such as a program, script or command, to send any message with the intent to interfere with or disable terminal sessions is not acceptable.
	8.Making public statements under cover of MCDA identity Individuals making public statements under the cover of their organization identity, including through email, web postings, instant messaging or public presentations, must seek explicit authorization and approval from management. Communications department is the only department authorized to publish Press Releases and to communicate with members of the journalistic community ("the press"). Any public statement made in contravention of this policy and related policies is expressly prohibited and may result in severe disciplinary action, up to and including termination of employment. "Whistle blowing," or the disclosure of information about questionable internal practices, may be a legally protected form of disclosure. However, these disclosures must not occur in a public arena, but must be limited to specific conversations with law enforcement or regulators. Disclosure of protected information in public under the guise of “whistle blowing” will be subject to legal action against the individual by the MCDA.
	9.Disclosure of protected information Disclosing MCDA confidential information is prohibited. Disclosures may include, but are not limited to, unique account names, account passwords or lists of employees, contractors, consultants, vendors or products. All information must be treated as confidential and protected unless labeled otherwise, in accordance with the Confidentiality, Non-Competition and Proprietary Rights Agreement. Certain information may be disclosed, including email address, assigned desk phone number, fax number, mailing address or title.
	10.Monitoring or interception of network traffic Monitoring or intercepting any form of network traffic or data not intended for your own host is prohibited, unless authorized as part of your normal job duties. Monitoring or intercepting network traffic may violate the privacy or confidentiality of the data being transmitted.
	12.Introduction of network services or routing configurations The introduction of routing patterns or network services that are inconsistent with established patterns or services and/or that may disrupt or interfere with the intended patterns or services are expressly prohibited. Examples of unacceptable use include, but are not limited to, broadcasting routing information, providing Dynamic Host Control Protocol (DHCP) services in conflict with authorized services, or sending network messages designed to terminate network connections (such as TCP RST packets, or "sniping").
	13.Use of MCDA resources to conduct non-MCDA business MCDA resources may not be put to use for any business purpose outside of government business. These includes, but is not limited to, the use of MCDA computers to store, forward, copy or manage information for any other MCDA; the use of MCDA equipment to

DRAFT

	produce printed or electronic documents for any other MCDA or MCDA; or the use of any MCDA resources, including personnel time, for the furtherance of any other MCDA or MCDA. Specific exemptions to this policy may be granted by management for specific charitable, promotional, or in-kind business partnerships, but such exemptions must be specifically authorized and must comply with all relevant laws and regulations.
	14.Release of information regarding security incidents Authorization to release information regarding security incidents involving the MCDA is restricted solely to management and its assigned agents (e.g., legal counsel or public relations agents). In the event of a security incident involving the MCDA, individuals are not authorized to communicate news of such incidents to any outside party. It is solely the MCDA's responsibility to appropriately notify public MCDA of security incidents in compliance with state and federal regulations.
Policy Enforcement and Limitation of Liability to the MCDA	The MCDA will take all reasonable measures to ensure that compliance with all applicable laws occurs with respect to the acceptable use of computing resources. The MCDA will also undertake training and awareness programs to ensure that all employees, contractors, temporaries and vendors are informed of this, and other, policies. The MCDA is responsible for the disclosure of expected performance with respect to acceptable use of computing resources. Any failure of an individual to comply with this policy, despite the reasonable efforts of the MCDA to inform and educate, are the sole responsibility of the individual. Any violations that result from an internal or external investigation and that may include legal actions are strictly assigned to the individual.
	1.Reporting violations or seeking clarification All suspected violations of this policy must be reported to management or through the communication methods provided by the MCDA. Failure to report knowledge of a suspected policy violation will itself be considered a violation and will be subject to disciplinary review and action. It is the responsibility of all employees to help minimize risk to the MCDA as a whole.
	2.Automated methods for policy enforcement The MCDA will implement automated methods for monitoring MCDA assets for unacceptable use and abuse. These automated methods will assist the MCDA in taking reasonable measures to ensure that violations do not occur. Disabling or tampering with these automated methods is strictly prohibited and may result in disciplinary action. These tools are intended strictly to monitor MCDA assets for acceptable use of computing resources. These tools are not intended as a method for "spying" on employees or to violate any privacy protections afforded employees.
	3.Procedures for remediation of violations All potential violations will be considered through due process. Ownership for the violation will be determined and the need for disciplinary review and action will be addressed. If the MCDA finds that it is in violation of this policy, immediate actions will be taken to bring the MCDA into compliance. If the MCDA finds that the violation is the result of individual actions that were not properly authorized, the individual or individuals directly responsible will be referred for disciplinary review.
	4.Process for levying disciplinary action Once a determination is made that a violation has occurred as a result of the actions of an individual or individuals, management will refer the matter to Human Resources for consideration and action under the disciplinary plan. Disciplinary actions may include, but are not limited to, levying of fines, suspension or termination of employment. In all cases, the violating behavior must be immediately stopped. If a determination is made that the MCDA caused or authorized the violation, a decision will have to be made about whether or not the offending action should be halted or permitted.

DRAFT

	5.Periodic policy review This document will be periodically reviewed, no less than annually, and suggestions for changes will be reviewed and voted upon by a Policy Review Committee to be assigned by the Board of Directors. This committee will collect comments and suggestions for policy change between meetings, and will decide upon suggestions in a timely fashion. Legal must review all policy changes before they can be accepted and implemented. Changes to policy will be announced to the MCDA through appropriate channels, including but not limited to, MCDA wide electronic mail, announcement at MCDA meetings, and the distribution of updated MCDA policy documents.
Agreement to and Acceptance of this Policy	• By accepting employment with the MCDA and using computing resources owned by the MCDA, the user is accepting the terms of this policy and agreeing to abide by its provisions. • The following signature by the user signifies acceptance of this policy in its entirety and represents a commitment to make use of computing resources in an acceptable and responsible manner. • Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. The signature of a witness affirms that the user has been apprised of this policy and been given an opportunity to voice questions or concerns up front. • Sample employer agreement form I, the below signed, agree to the requirements and guidelines set forth in this, the "Acceptable Use of Computing Resources" policy, and promise to use computing resources, provided by the MCDA to perform my job duties, in an acceptable, appropriate and professional manner. Furthermore, I waive my right to privacy, except for those rights specifically guaranteed by the law, and accept that the MCDA may monitor and respond to my use of computing resources in accordance with this, and other, MCDA policies. Name: _____ Employee ID: _____ Signature: _____ Date: _____ I, the below signed, have witnessed the signing of this agreement. I have ensured that the above-signed has received a current copy of the "Acceptable Use of Computing Resources" policy and that I have answered or referred for answer any questions or concerns that the above-signed has expressed. Name: _____ Employee ID: _____ Signature: _____ Date: _____ Legal and HR should be consulted to ensure that this agreement is allowable under applicable laws. Also, it may be wise to add language stating that, should any part of the policy be deemed illegal, the rest of the policy will remain intact and valid.
Ethical, moral and legal implications of the "acceptable use of computing resources"	Policy must consider the ethical, moral and legal implications of its provisions and entirety. The primary focus of the policy is to outline expected patterns of behavior and professional conduct with respect to use of computing resources. Furthermore, provisions within the policy set expectations for monitoring and enforcement of the policy, as well as to document potential disciplinary actions.
	A. Ethical Implications: Fairness • An ethical analysis of a policy must consider the fairness of the rules of behavior codified in the policy. The concept of fairness, in this case, pertains to whether or not the MCDA is fairly allowing and limiting access to and use of computing resources. Specifically, there is an inherent contradiction in the requirement of employees to have access to computing resources and the desire of the business to limit use and abuse of these resources. • From the standpoint of fairness, the policy should provide a general guideline for acceptable use, while adding specific prohibitions and restrictions that are considered unacceptable use under most, if not all, circumstances.
	B. Moral Implications: Right vs. Wrong • MCDA are not allowed to promote illegal or illicit activity and are constrained to ensure,

DRAFT

	within reason, that their employees are compliant with the requirements. In limiting the ability and permission of employees to use computing resources, the business will exceed reasonable restrictions and should stipulate limits on use that are not only legal, but quite possibly protected or necessary. • Situations where an action falls into the gap between acceptable and unacceptable use, the right and reasonable approach is for the user to seek clarification before undertaking the action.
	C. Legal Implications: Indemnification Against Direct Liability • The creation and promotion of policies, standards, guidelines and procedures are used by MCDA to limit the liability they might otherwise incur in instances where bad things have happened. • In this specific case, one of the primary objectives of the policy is to clearly define legal behavior as acceptable and illegal behavior as unacceptable. • Coupled with an active training and awareness program, the policy serves to transfer some, if not most, of the responsibility for illegal behavior onto the individual. • The MCDA bears the responsibility of proving that due diligence has been performed with respect to monitoring and enforcement of the policy, implementation and maintenance of access controls, and implementation and maintenance of security countermeasures. • By reading and agreeing to the policy, the employee accepts responsibility for their actions and indemnifies the MCDA against being held directly responsible for the actions of an individual. • By defining the expectations for disciplinary action as a result of violating this policy, the MCDA protects itself against lawsuits from terminated employees in which this policy will have been used as the basis for the disciplinary action. • Automated and manual monitoring and response tactics must be developed and deployed.
	D. Legal Implications: Fairness and Due Process • This has to do with the fair and consistent application of rules to all employees without discrimination. • Rules must be applied to every employee in the MCDA, regardless of title, race, gender, etc. If the policy is not applied fairly and consistently, then the legal issue of discrimination may arise. • To recapitulate, this policy must be applied fairly and without discrimination. All resulting actions, whether for monitoring and enforcement or a resulting disciplinary action, must be undertaken in an objective manner that does not target the individual out of context, but instead considers the situation objectively and within the full context.
	E. Legal Implications: Adequate Training and Awareness • A comprehensive training and awareness program is fundamental to the success of policies like the acceptable use policy. Responsibility is placed on the MCDA to fully educate its users about the hazards of interconnected computing and how to make use of computing resources in an acceptable, responsible and safe manner.
	F. Legal Implications: Implied Contractual Obligations • Acceptable Use of Computing Resources" serves as an implied set of contractual obligations. • The MCDA should set forth its expectations for behavior and performance, commits to performing due diligence in providing training, awareness and countermeasures, and requires that the employee abide by the terms of the agreement. • The agreement is not only signed by the employee, but it is also signed by a witness who could attest under oath that the employee was provided with the terms of the agreement and given opportunities to resolve questions or seek clarification.

DRAFT

DRAFT