GOVERNMENT ICT STANDARDS

Information Security Standard

First Edition 2016

The ICT Authority is a State Corporation under the State Corporations Act 446
www.icta.go.ke

Contents

ICTA STANDARDS DESCRIPTION

S / No	Thematic Area	Standards	Brief Description
1	Infrastructure	ICTA-2.001:2016 Network Standard	Provides compliant requirements for design, installations and management of all categories of IT Networks to be deployed in government.
		ICTA-2.001:2016 Data Center Standard	Provides compliant requirements for design, installations and management of government data centers
		ICTA-2.001:2016 Cloud Computing Standard	Provides compliant requirements for design, installations and management of cloud computing infrastructures for government
		ICTA-2.001:2016 End-User Equipment Standard	Provides the minimum specifications for all computing devices being deployed in government
2	Systems & Applications	ICTA-6.001:2016 Systems & Applications Standard	Provides compliant requirements for design, installations and management of all government Software and applications Systems.
3	IT Security	ICTA-3.001:2016 Information Security Standard	Provides compliant requirements for design, installations and management of Information Technology Security in government.
4	Electronic records management	ICTA-4.001: 2016 Electronic records and Data Management Standard	Provides compliant requirements for management of government electronic records and data
5	IT Governance	ICTA. 5.001: 2016 IT Governance Standard	Provides compliant requirements for IT Governance in government. This includes compliance requirements for government IT service providers and Professional Staff.
6	ICT Human Capacity	ICTA.7.001:2016 ICT Human Capital and Work force Development Standard	Provides compliant requirements for development of Human Capital capacity for deployment and support for government ICT infrastructure and services.

REVISION OF ICT STANDARDS

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

DOCUMENT CONTROL

Document Name:	Information Security Standard
Prepared by:	ICTA Information Security Standard Technical Committee
Edition:	First Edition
Approved by:	Board of Directors
Date Approved:	11th August 2016
Effective Date :	1st January 2017
Next Review Date:	After 3 years

FOREWORD

The ICT Authority has express mandate to, among others, 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 specific mandate is to ensure coherence and unified approach to acquisition, deployment, management and operation of ICTs across the public service, including state agencies, in order to promote service integration, adaptability and cost savings through economies of scales in ICT investments.

In pursuit of achievement of this mandate, the Authority established a Standards Committee to identify the critical standards domain areas as well as oversee the standards development process. A total of Nine Standards falling under six different domain areas were identified by the committee to be relevant for government ICT Standards. The development of all the identified standards was done through a process which took into consideration international requirements, government requirements, stakeholder participation as well as industry/sector best practices. In order to conform to the format of other existing national standards, the committee adopted the Kenya Bureau of Standards (KEBS) format and procedure for standards development. In addition, through Memoranda of Understanding, KEBS has made invaluable contribution to the development of ICT Authority standards.

The ICTA Information Security Standard, which falls under the overall Government Enterprise Architecture (GEA), has therefore been prepared in accordance with KEBS standards development guidelines.

The Authority has the oversight role and responsibility for management and enforcement of this standard. The review and approval of the standard is done by the ICTA Board upon recommendation of Standard Review Board. The Authority shall be carrying out quarterly audits in all the Ministries, Counties, and Agencies (MCA) to determine their compliance to this Standard.

The Authority will issue a certificate of compliance to agency upon completion of the audit assessment. 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 will advise on action to take.

All government agencies are required to ensure full compliance to this standard for effective and efficient service delivery to the citizen. The compliance period is six months from effective date.

Kipronoh Ronoh P.
Director, Programmes and Standards

INTRODUCTION

Data and Information are assets that, like other important government assets, is essential to Government and it's operations and consequently needs 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, and 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 MCAs 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 MCA ICT resources do not adversely affect other Users or other Systems.

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 MCAs 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.

Application

This standard will be applicable to the following:

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

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.

- ISO/IEC 27002:2013- Information technology — Security techniques — Code of practice for information security controls

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

Definitions

- Asset -Anything that has value to the MCA
- Availability -The property of being accessible and usable upon demand by an authorized entity
- Confidentiality- The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- 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 MCA structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

- Integrity- The property of safeguarding the accuracy and completeness of assets
- Residual risk- The risk remaining after risk treatment
- 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 MCA with regard to risk
- Risk treatment- Process of selection and implementation of measures to modify risk
- Application Security- Application security is the use of software, hardware, and procedural methods to protect applications from external threats from development, deployment to maintenance.
- Data Security- Data security refers to protective measures that are applied to prevent unauthorized access to computers, databases and websites that causes data corruption.
- 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.

- Network Security- Network security refers to any activities designed to protect the usability, reliability, integrity, and safety of your network and data.
- A duress alarm- Is a method for secretly indicating that an action is taking place 'under duress'.
- 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).
- Tele- working- refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as "telecommuting", "flexible workplace", "remote work" and "virtual work" environments.

Abbreviations

GEA	Government Enterprise Architecture
ISMS	Information Security Management System
ISO	International Standards Organization
MCAs	Ministry, Counties, Departments and MCAs
IT	Information Technology
ICT	Information and Communication Technologies
IS	Information Security

Sub-domains

The following are the sub domains covered under Information security standardization:

1. Information Security Policies
2. Organizing Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications Security
7. Cryptography Controls
8. Operations Security
9. Access Control
10. Information Systems Acquisition, Development and Maintenance
11. Information Security Incident Management
12. Supplier Relationships
13. Business Continuity Management
14. Compliance

Requirements

Sub-Domain	Description	Requirement
8.1 Information Security Policy	MCAs shall develop and maintain security policies to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	Annex A.1
8.2 Organization of Information Security	MCAs shall establish a management framework to initiate and control the implementation and operation of information security within the organization.	Annex A.2
8.3 Asset Management	MCAs shall identify organizational assets and define appropriate protection responsibilities.	Annex A.3
8.4 Human Resource Security	MCAs shall ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	Annex A.4
8.5 Communications Security	MCAs shall ensure the protection of information in networks and its supporting information processing facilities	Annex A.5
8.6 Operations Security	MCAs shall ensure correct and secure operations of information processing facilities.	Annex A.6
8.7Physical and environmental security	MCAs shall prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Annex A.7
8.8 Cryptographic Controls	MCAs shall ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	Annex A.8
8.9 Access Control	MCAs shall limit access to information and information processing facilities	Annex A.9
8.10 Information Systems Acquisition, Development and Maintenance	MCAs shall ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.	Annex A.10
8.11 Supplier Relationships	MCAs shall ensure protection of the organization's assets that is accessible by suppliers	Annex A.11
8.12 Information Security Incident Management	MCAs shall ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	Annex A.12
8.13 Information Security Aspects of Business continuity	MCAs shall ensure information security continuity should be embedded in the organization's business continuity management systems.	Annex A.13
8.14 Compliance	MCAs shall avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	Annex A.14

ANNEX

Annex A.1: Information Security Policy

		Requirement
A.1-1 Policies for information security	A.1-1.1:Guidance	a. MCAs shall define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives. b. These policies shall be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme" (see A-4-1.4). c. The policies shall address regulations, legislation and contracts;
	A.1-1.2:Structure	The ICT policy shall contain:- • Definition of information security, objectives and principles to guide all activities relating to information security; • Assignment of general and specific responsibilities for information security management to • Defined roles; • Processes for handling deviations and exceptions.
	A.1-1.3:Topic specific policies	• Access control (see AnnexA.9); • Information classification (and handling) (see A-3-2); • Physical and environmental security (see Annex A.7); • End user oriented topics such as: 1) Acceptable use of assets (seeA-3-1.3); 2) Clear desk and clear screen (see A.7-2.9); 3) Information transfer (see A.5-2.3); 4) Mobile devices and tele-working (see A-2-2); 5) Restrictions on software installations and use (see A.6-6.2); • Backup (see A.6-3); • Information transfer (see A.5-2); • Protection from malware (see A.6-2); • Management of technical vulnerabilities (A.6-6.1); • Cryptographic controls (see Annex A.8); • Communications security (see Annex A.5); • Protection of personally identifiable information (see A.14-1.4); • Supplier relationships (see Annex A.11). • Other topic-specific policies to address certain target groups from the MCA.

A.1-2Review of the policies for information security	A.1-2.4:Guidance	a. The policies for information security shall be reviewed every 2 years or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness b. The review shall include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment. c. The review of policies for information security shall take the results of management reviews into account.
	A.1-2.5:Approval	Management approval for a revised policy shall be obtained.

Annex A.2 Organization of Information Security

		Requirement
A.2-1 Internal organization	A.2-1.1: Information security roles and responsibilities	a. MCAs shall have an information security steering committee b. Senior executive management group agenda/minutes shall include information security matters c. MCAs shall appoint an officer/ officers in charge of information security d. To be able to fulfill responsibilities in the information security area the appointed individuals shall be certified in the area and be given opportunities to keep up to date with developments in information security sector e. Information security roles and responsibilities shall be documented and approved by senior executive management f. Employees with information security roles and responsibilities shall sign a document stating that they understand their roles and responsibilities
	A.2-1.2: Segregation of duties	a. MCA shall ensure that no single person can access, modify or use assets without authorization or detection. The initiation of an event shall be separated from its authorization. The possibility of collusion shall be considered in designing the controls. b. Whenever it is difficult to segregate, other controls such asmonitoring of activities, audit trails and management supervision shall be considered.
	A.2-1.3: Contact with Authorities	a. MCAs shall have contacts with ICT Authority Information security team for reporting in case of attacks from the internet for action to be taken b. MCAs shall have contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers.
	A.2-1.4: Contact with special interest groups	a. MCAs ICT security personnel shall maintain membership with specialist security forums and professional associations
	A.2-1.5: Information security in project management	a. Information security objectives shall be included in all projects objectives; b. An information security risk assessment shall be conducted at an early stage of the project to identify necessary controls; c. Information security shall be part of all phases of the applied project methodology.

A.2-2:Mobile devices and tele-working	A.2-2.1: Mobile device policy	a. MCAs shall develop a mobile device policy to ensure that business information is not compromised b. The mobile device policy shall consider: - registration of mobile devices; - requirements for physical protection; - restriction of software installation; - requirements for mobile device software versions and for applying patches; - restriction of connection to information services - access controls; - cryptographic techniques; - malware protection; - remote disabling, erasure or lockout; - backups; - usage of web services and web apps. - separation of private and business use of the devices, including using software to support such separation and protect business data on a private device; - providing access to business information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), 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. c. Protection shall be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques (see Annex A.8) and enforcing use of secret authentication information. d. Devices carrying important, sensitive or critical business information shall not be left unattended and, where possible, shall be physically locked away, or special locks shall be used to secure the devices. e. Each MCA shall have a specific procedure taking into account legal, insurance and other security requirements of the organization for cases of theft or loss of mobile devices. f. Training shall be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented.

	A.2-2.2: Tele-working	a. MCAs allowing tele-working shall define a policy with following content: - The provision of suitable equipment and storage furniture for the tele- working activities, where the use of privately owned equipment that is not under the control of the organization is not allowed; - A definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the tele- worker is authorized to access; - The provision of suitable communication equipment, including methods for securing remote access; - Physical security; - Rules and guidance on family and visitor access to equipment and information; - The provision of hardware and software support and maintenance; - The provision of insurance; - The procedures for backup and business continuity; - Audit and security monitoring; - Revocation of authority and access rights, and the return of equipment when the tele- working activities are terminated.

Annex A.3 Asset management

		Requirement
A.3-1:Responsibility for assets	A.3-1.1:Inventory of assets	a. MCAs shall implement and maintain an inventory of assets associated with information and information processing facilities b. The asset inventory shall be accurate, up to date, and consistent and aligned with other inventories. c. For each of the identified assets, ownership of the asset shall be assigned (see A-3-1.2) and the classification shall be identified (see A-3-1).
	A.3-1.2:Ownership of assets	a. MCAs shall assign each information asset to an owner b. The owner shall - Ensure that assets are inventoried; - Ensure that assets are appropriately classified and protected; - Define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies; - Ensure proper handling when the asset is deleted or destroyed.
	A.3-1.3:Acceptable use of assets	a. MCAs shall create rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented b. Guidance on acceptable policy structure is as shown on Appendix II c. Employees and external party users using or having access to the organization's assets shall be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources. d. They shall be responsible for their use of any information processing resources and of any such use carried out under their responsibility. e. Use of messaging and collaboration, social media, BYOD shall conform to the systems and applications standard
	A.3-1.4:Return of assets	a. All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement. b. The termination process shall be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization. c. In cases where an employee or external party user purchases the organization's equipment or uses their own personal equipment, procedures shall be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment (see A.7-2.7). d. In cases 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. e. During the notice period of termination, the organization shall control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

A.3-2:Information classification	A.3-2.1:Classification of information	a. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. b. The scheme shall also be aligned to the access control policy (see A.9-1.1). c. Each level shall be given a name that makes sense in the context of the classification scheme's application. d. 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. e. 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, e.g. in terms of confidentiality, integrity and availability. f. Results of classification shall be updated in accordance with changes of their value, sensitivity and criticality through their life-cycle. g. Information confidentiality classification scheme shall be based on four levels as follows: - Disclosure causes no harm; - Disclosure causes minor embarrassment or minor operational inconvenience; - Disclosure has a significant short term impact on operations or tactical objectives; - Disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.
	A.3-2.2:Labelling of information	a. MCAs shall ensure labelling of classified information. Physical labels and metadata shall be used.
	A.3-2.3:Handling of assets	- MCAs shall ensure access restrictions supporting the protection requirements for each level of classification; - MCAs shall ensure maintenance of a formal record of the authorized recipients of assets; - MCAs shall ensure protection of temporary or permanent copies of information to a level consistent with the protection of the original information; - MCAs shall ensure storage of IT assets in accordance with manufacturers' specifications; - MCAs shall ensure clear marking of all copies of media for the attention of the authorized recipient.

A.3-3:Media handling	A.3-3.1:Management of removable media	a. MCAs shall develop procedures for the management of removable media in accordance with the classification scheme adopted by the organization. b. The procedures shall include the following: - If no longer required, the contents of any re-usable media that are to be removed from the organization shall be made unrecoverable; - Where necessary and practical, authorization shall be required for media removed from the organization and a record of such removals should be kept in order to maintain an audit trail; - All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications; - If data confidentiality or integrity are important considerations, cryptographic techniques should be used to protect data on removable media; - To mitigate the risk of media degrading while stored data are still needed, the data shall be transferred to fresh media before becoming unreadable; - Multiple copies of valuable data shall be stored on separate media to further reduce the risk of coincidental data damage or loss; - Registration of removable media shall be considered to limit the opportunity for data loss; - Removable media drives shall only be enabled if there is a business reason for doing so; - Where there is a need to use removable media the transfer of information to such media shall be monitored. - Procedures and authorization levels shall be documented.
	A.3-3.2:Disposal of media	a. MCA shall document formal procedures for the secure disposal of media to minimize the risk of confidential information leakage to unauthorized persons. b. The procedures for secure disposal of media containing confidential information shall be proportional to the sensitivity of that information. The following items shall be included in the procedures: - Media containing confidential information shall be stored and disposed of securely, e.g. by incineration or shredding, or erasure of data for use by another application within the organization; - procedures shall be in place to identify the items that might require secure disposal; - It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items; - Many organizations offer collection and disposal services for media; care should be taken in selecting a suitable external party with adequate controls and experience; - Disposal of sensitive items shall be logged in order to maintain an audit trail. - When accumulating media for disposal, consideration shall be given to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.
	A.3-3.3:physical media transfer	MCAs shall document and implement the following guidelines to protect media containing information being transported: - Reliable transport or couriers shall be used; - A list of authorized couriers shall be agreed with management; - Procedures to verify the identification of couriers shall be developed; - 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; - 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.

Annex A.4: Human Resource Security

		Requirement
A.4-1Prior to employment	A.4-1.1:Screening	a. Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. b. Verification shall take into account all relevant privacy, protection of personally identifiable information and employment based legislation, and shall, where permitted, include the following: - Availability of satisfactory character references, e.g. one business and one personal; - A verification (for completeness and accuracy) of the applicant's curriculum vitae; - Confirmation of claimed academic and professional qualifications; - Independent identity verification (passport or similar document); - More detailed verification, such as credit review or review of criminal records. c. When an individual is hired for a specific information security role, organizations shall make sure the candidate: - Has the necessary competence to perform the security role; - Can be trusted to take on the role, especially if the role is critical for the organization. d. Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and, in particular, if these are handling confidential information, e.g. financial information or highly confidential information, the organization shall also consider further, more detailed verifications. e. Procedures shall define criteria and limitations for verification reviews, e.g. who is eligible to screen people and how, when and why verification reviews are carried out. f. Screening process shall also be ensured for contractors. In these cases, the agreement between the MCA and the contractor shall specify responsibilities for conducting the screening and the notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern. g. Information on all candidates being considered for positions within the MCA shall be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates shall be informed beforehand about the screening activities.
	A.4-1.2:Terms and conditions of employment	a. MCAs shall have contractual agreements (code of conduct) with their employees and contractors that reflect the organization's policies for information security b. The contractual agreements with employees and contractors shall state the following: - That all employees and contractors who are given access to confidential information shall sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities (see A.5-2.6); - The employee's or contractor's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation (see A.14-1.2and A.14-1.4); - Responsibilities for the classification of information and management of MCA assets associated with information, information processing facilities and information services handled by the employee or contractor (see Annex A.3); - Responsibilities of the employee or contractor for the handling of information received from other MC As or external parties; actions to be taken if the employee or contractor disregards the MCA's security requirements (see A-4-1.5). c. Information security roles and responsibilities shall be communicated to job candidates during the pre-employment process. d. The MCA shall ensure that employees and contractors agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the MCA's assets associated with information systems and services. e. Where appropriate, responsibilities contained within the terms and conditions of employment shall continue for a defined period after the end of the employment (see A-4-2).
	A.4-1.3:During employment	MCA shall ensure all employees and contractors : • Are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems; • Are provided with guidelines to state information security expectations of their role within the organization; • Are motivated to fulfill the information security policies of the organization; • Achieve a level of awareness on information security relevant to their roles and responsibilities within the organization (see A-4-1.4); • Conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working; • Continue to have the appropriate skills and qualifications and are educated on a regular basis; • Are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").

	A.4-1.4:Information security awareness, education and training	a. MCAs shall conduct an information security awareness programme in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. b. The awareness programme shall include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters. c. The awareness programme shall be planned taking into consideration the employees' roles in the organization, and, where relevant, the organization's expectation of the awareness of contractors. d. The activities in the awareness programme shall be scheduled over time, preferably regularly, so that the activities are repeated and cover new employees and contractors. e. The awareness programme shall also be updated regularly so it stays in line with organizational policies and procedures, and shall be built on lessons learnt from information security incidents. f. Awareness training shall be performed as required by the organization's information security awareness programme. g. Awareness training can use different delivery media including classroom-based, distance learning, web-based, self-paced and others. h. Information security education and training shall also cover general aspects such as: - Stating management's commitment to information security throughout the organization; - The need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements; - Personal accountability for one's own actions and inactions, and general responsibilities towards - Securing or protecting information belonging to the organization and external parties; - Basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks); - Contact points and resources for additional information and advice on information security matters, including further information security education and training materials. i. Information security education and training shall take place annually. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active. j. The MCA shall develop the education and training programme in order to conduct the education and training effectively. The programme should be in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. The programme shall consider different forms of education and training, e.g. lectures or self-studies. k. An assessment of the employees' understanding shall be conducted at the end of an awareness, education and training course to test knowledge transfer.
	A.4-1.5:Disciplinary process	a. MCAs shall have a disciplinary process take action againstemployees who have committed an information security breach. b. The disciplinary process shall not be commenced without prior verification that an information security breach has occurred (see A.12-1.7). a. Deliberate breaches may require immediate actions.
A.4-2:Termination and change of employment	A.4-2.1:Termination or change of employment responsibilities	a. MCAs shall ensure that the communication of termination responsibilities include on-going information security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement (see A.5-2.6) and the terms and conditions of employment (see A-4-1.2) continuing for a defined period after the end of the employee's or contractor's employment. b. Responsibilities and duties still valid after termination of employment shall be contained in the employee's or contractor's terms and conditions of employment (see A-4-1.2). c. Changes of responsibility or employment shall be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment. d. MCAs shall inform employees, customers or contractors of changes to personnel and operating arrangements.

Annex A.5 Communications security

		Requirement
A.5-1:Network security management	A.5-1.1:Network controls	a. MCAs shall develop and document controls to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items shall be implemented: - Responsibilities and procedures for the management of networking equipment shall be established; - Operational responsibility for networks should be separated from computer operations where appropriate (see A.12-1.2); - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (see Annex A.8and A.5-2); special controls may also be required to maintain the availability of the network services and computers connected; - Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security; - Management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure; - Systems on the network should be authenticated; - Systems connection to the network should be restricted.
	A.5-1.2:Security of network services	a. MCAs shall develop service level agreements for network services b. The SLA shall define security requirements and the right to audit
	A.5-1.3:Segregation in networks	a. MCAs shall divide large networks into separate network domains based on trust either physically into different networks or by using different logical networks (e.g. virtual private networking). b. The perimeter of each domain shall be well defined. Access between network domains shall be allowed, but shall be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, shall be based on an assessment of the security requirements of each domain. The assessment shall be in accordance with the access control policy (see A.9-1.1), access requirements, value and classification of information processed and shall also take account of the relative cost and performance impact of incorporating suitable gateway technology. c. Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls policy (see A.5-1.1) before granting access to internal systems. d. The authentication, encryption and user level network access control technologies of modern, standards based wireless networks may be sufficient for direct connection to the organization's internal network when properly implemented.

A.5-2:Information transfer	A.5-2.3:Information transfer policies and procedures	a. MCAs shall develop formal transfer policies, procedures and controls to protect the transfer of information through the use of all types of communication facilities. b. The procedures and controls to be followed when using communication facilities for information transfer shall consider the following items: - Procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction; - Procedures for the detection of and protection against malware that may be transmitted through - the use of electronic communications (see A.6-2.1); - Procedures for protecting communicated sensitive electronic information that is in the form of - an attachment; - Policy or guidelines outlining acceptable use of communication facilities (see A.14-1.3); - Personnel, external party and any other user's responsibilities not to compromise the organization, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.; - Use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information (see Annex A.8); - Retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations; - Controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses; - Advising personnel to take appropriate precautions not to reveal confidential information; - Not leaving messages containing confidential information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing; - advising personnel about the problems of using facsimile machines or services, namely: i. Unauthorized access to built-in message stores to retrieve messages; ii. Deliberate or accidental programming of machines to send messages to specific numbers; iii. 3) Sending documents and messages to the wrong number either by misdialing or using the wrongstored number. - In addition, personnel shall be reminded that they shall not have confidential conversations in public places or over insecure communication channels, open offices and meeting places. - Information transfer services shall comply with any relevant legal requirements (see A.14-1).

	A.5-2.4:Agreements on information transfer	a. MCAs shall have agreements to address the secure transfer of business information between the organization and external parties. a. The information security content of the agreement shall reflect the sensitivity of the business information involved. b. The Information transfer agreements should incorporate the following: - Management responsibilities for controlling and notifying transmission, dispatch and receipt; - Procedures to ensure traceability and non-repudiation; - Minimum technical standards for packaging and transmission; - Escrow agreements; - Courier identification standards; - Responsibilities and liabilities in the event of information security incidents, such as loss of data; - 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 (see A-3-2); - Technical standards for recording and reading information and software; - Any special controls that are required to protect sensitive items, such as cryptography (see Annex A.8); - Maintaining a chain of custody for information while in transit; - Acceptable levels of access control.
	A.5-2.5:Electronic messaging	a. MCAs shall develop and implement the following policies: - Protecting messages from unauthorized access, modification or denial of service commensurate - with the classification scheme adopted by the organization; - Ensuring correct addressing and transportation of the message; - Reliability and availability of the service; - Legal considerations, for example requirements for electronic signatures; - Obtaining approval prior to using external public services such as instant messaging, social - networking or file sharing; - Stronger levels of authentication controlling access from publicly accessible networks.
	A.5-2.6:Confidentiality or non-disclosure agreements	a. MCAs shall identify, regularly review and document requirements for confidentiality or non-disclosure b. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered: - A definition of the information to be protected (e.g. confidential information); - Expected duration of an agreement, including cases where confidentiality might need to be - maintained indefinitely; - Required actions when an agreement is terminated; - d) responsibilities and actions of signatories to avoid unauthorized information disclosure; - Ownership of information, trade secrets and intellectual property, and how this relates to the - protection of confidential information; - The permitted use of confidential information and rights of the signatory to use information; - The right to audit and monitor activities that involve confidential information; - Process for notification and reporting of unauthorized disclosure or confidential information leakage; - Terms for information to be returned or destroyed at agreement cessation; - Expected actions to be taken in case of a breach of the agreement. c. There shall be forms of confidentiality and non-disclosure agreements in different circumstances.

Annex A.6: Operations Security

		Requirement
A.6-1:Operational procedures and responsibilities	A.6-1.1:Documented operating procedures	a. MCAs shall document operating procedures and make them available to all users who need them. b. The operating procedures shall specify the operational instructions, including: - The installation and configuration of systems; - Processing and handling of information both automated and manual; - Backup (see A.6-3); - Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times; - Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (see A.9-4.4); - Support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties; - Special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs (see A-3-3and A.7-2.7); - System restart and recovery procedures for use in the event of system failure; - The management of audit-trail and system log information (see A.6-4); monitoring procedures. c. Operating procedures and the documented procedures for system activities shall be treated as formal documents and changes authorized by management. d. Where technically feasible, information systems shall be managed consistently, using the same procedures, tools and utilities.
	A.6-1.2:Change management	MCAs shall ensure the following: - Identification and recording of significant changes; - Planning and testing of changes; - Assessment of the potential impacts, including information security impacts, of such changes; - Formal approval procedure for proposed changes; - Verification that information security requirements have been met; - Communication of change details to all relevant persons; - Fall-back procedures, including procedures and responsibilities for aborting and recovering from - Unsuccessful changes and unforeseen events; - Provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident (see A.12-1). - An audit log containing all relevant information shall be retained.
	A.6-1.3:Capacity management	MCAs shall ensure: - Deletion of obsolete data (disk space); - Decommissioning of applications, systems, databases or environments; - Optimizing batch processes and schedules; - Optimizing application logic or database queries; - Denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming). - A documented capacity management plan shall be considered for mission critical systems.
	A.6-1.4:Separation of development, testing and operational environments	The following items shall be documented and implemented: - Rules for the transfer of software from development to operational status shall be defined and documented; - Development and operational software shall run on different systems or computer processors and - in different domains or directories; - Changes to operational systems and applications shall be tested in a testing or staging environment prior to being applied to operational systems; - Other than in exceptional circumstances, testing shall not be done on operational systems; - Compilers, editors and other development tools or system utilities shall not be accessible from operational systems when not required; - Users shall use different user profiles for operational and testing systems, and menus should - display appropriate identification messages to reduce the risk of error; - Sensitive data shall not be copied into the testing system environment unless equivalent controls are provided for the testing system (see A.10-3).

A.6-2:Protection from malware	A.6-2.1:Controls against malware	a. Detection, prevention and recovery controls to protect against malware shall be implemented by MCAs, combined with appropriate user awareness. b. The following shall be implemented: - Establishing a formal policy prohibiting the use of unauthorized software (see A.6-6.2 and 14.2.); - Implementing controls that prevent or detect the use of unauthorized software (e.g. application white listing); - Implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting); - Establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures shall be taken; - Reducing vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management (see A.6-6); - Conducting regular reviews of the software and data content of systems supporting critical business - Processes; the presence of any unapproved files or unauthorized amendments should be formally - investigated; - Installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include: i. Scan any files received over networks or via any form of storage medium, for malware before use; ii. Scan electronic mail attachments and downloads for malware before use; this scan should be iii. carried out at different places, e.g. at electronic mail servers, desk top computers and when iv. entering the network of the organization; v. Scan web pages for malware; - Defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks; - Preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements (see A.6-3); - Implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware; - Implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers shall ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them; - Isolating environments where catastrophic impacts may result.

A.6-3:Backup	A.6-3.1:Information backup	a. MCAs shall define a backup policy to define the organization's requirements for backup of information, software and systems. b. When designing a backup plan, the following items shall be taken into consideration: - Accurate and complete records of the backup copies and documented restoration procedures shall be produced; - The extent (e.g. full or differential backup) and frequency of backups shall reflect the business - Requirements of the organization, the security requirements of the information involved and the - Criticality of the information to the continued operation of the organization; - The backups shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site; - Backup information shall be given an appropriate level of physical and environmental protection (see Annex A.7) consistent with the standards applied at the main site; - Backup media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary; this shall be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data shall be performed 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; - In situations where confidentiality is of importance, backups shall be protected by means of encryption. - Operational procedures shall monitor the execution of backups and address failures of scheduledbackups to ensure completeness of backups according to the backup policy. - Backup arrangements for individual systems and services shall be regularly tested to ensure thatthey meet the requirements of business continuity plans. In the case of critical systems and services,backup arrangements should cover all systems information, applications and data necessary to recoverthe complete system in the event of a disaster. - The retention period for essential business information shall be determined, taking into account anyrequirement for archive copies to be permanently retained.

A.6-4:Logging and monitoring	A.6-4.1:Event logging	a. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed by MCAs. b. Event logs shall include: - user IDs; - System activities; - Dates, times and details of key events, e.g. log-on and log-off; - Device identity or location if possible and system identifier; - Records of successful and rejected system access attempts; - Records of successful and rejected data and other resource access attempts; - Changes to system configuration; - Use of privileges; - Use of system utilities and applications; - Files accessed and the kind of access; - Network addresses and protocols; - Alarms raised by the access control system; - Activation and de-activation of protection systems, such as anti-virus systems and intrusion - Detection systems; - Records of transactions executed by users in applications. c. Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures shall be taken (see A.14-1.4). d. System administrators shall not have permission to erase or de-activate logs of their own activities (see A.6-4.3).
	A.6-4.2:Protection of log information	a. Logging facilities and log information shall be protected against tampering and unauthorized access b. Controls shall aim to protect against unauthorized changes to log information and operational problems with the logging facility including: - Alterations to the message types that are recorded; - Log files being edited or deleted; - Storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.
	A.6-4.3:Administrator and operator logs	a. System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
	A.6-4.5:Clock synchronization	a. External and internal requirements for time representation, synchronization and accuracy shall be documented. b. A standard reference time for use within the organization shall be defined. c. The organization's approach to obtaining a reference time from external source(s) and how to synchronize internal clocks reliably shall be documented and implemented.

A.6-5:Control of operational software	A.6-5.1:Installation of software on operational systems	a. MCAs shall document procedures to control changes of software on operational systems b. The procedures shall include: - The updating of the operational software, applications and program libraries shall only be performed by trained administrators upon appropriate management authorization (see A.9-4.5); - Operational systems shall only hold approved executable code and not development code or compilers; - Applications and operating system software shall only be implemented after extensive and successful testing; the tests shall cover usability, security, effects on other systems and user friendliness and shall be carried out on separate systems (see A.6-1.4); it shall be ensured that all - Corresponding program source libraries have been updated; - A configuration control system shall be used to keep control of all implemented software as well - as the system documentation; - A rollback strategy shall be in place before changes are implemented; - An audit log shall be maintained of all updates to operational program libraries; - Previous versions of application software shall be retained as a contingency measure; - Old versions of software shall be archived, together with all required information and parameters, - Procedures, configuration details and supporting software for as long as the data are retained in archive. c. Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization shall consider the risks of relying on unsupported software. d. Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release, e.g. the introduction of new information security functionality or the number and severity of information security problems affecting this version. e. Software patches shall be applied when they can help to remove or reduce information security weaknesses (see A.6-6). f. Physical or logical access shall only be given to suppliers for support purposes when necessary and with management approval. The supplier's activities shall be monitored. g. Computer software may rely on externally supplied software and modules, which shall be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

A.6-6:Technical vulnerability management	A.6-6.1:Management of technical vulnerabilities	a. MCAs shall develop and maintain an effective management process for technical vulnerabilities b. The process shall contain: - The organization shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required; - Information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them shall be identified for software and other technology (based on the asset inventory list, see A.14-1.1); these information resources shall be updated based on changes in the inventory or when other new or useful resources are found; - Timeline shall be defined to react to notifications of potentially relevant technical vulnerabilities; - Once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls; - Depending on how urgently a technical vulnerability needs to be addressed, the action taken shall be carried out according to the controls related to change management (see A.6-1.2) or by following information security incident response procedures (see A.12-1.5); - If a patch is available from a legitimate source, the risks associated with installing the patch shall be assessed (the risks posed by the vulnerability shall be compared with the risk of installing the patch); - Patches shall be tested and evaluated before they are installed 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: i. turning off services or capabilities related to the vulnerability; ii. adapting or adding access controls, e.g. firewalls, at network borders (see A.5-1); iii. increased monitoring to detect actual attacks; iv. raising awareness of the vulnerability; c. An audit log should be kept for all procedures undertaken; d. The technical vulnerability management process shall be regularly monitored and evaluated in order to ensure its effectiveness and efficiency; e. Systems at high risk should be addressed first; f. An effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur; g. Define a procedure to address the situation where vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate
	A.6-6.2:Restrictions on software installation	a. The organization shall define and enforce strict policy on which types of software users may install. b. The policy of least privilege shall be applied. If granted certain privileges, users may have the ability to install software. The organization shall identify and document what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges shall be granted having regard to the roles of the users concerned.
	A.6-6.3:Information systems audit considerations	MCAs shall document and observe the following: - Audit requirements for access to systems and data shall be agreed with appropriate management; - The scope of technical audit tests shall be agreed and controlled; - Audit tests shall be limited to read-only access to software and data; - Access other than read-only shall only be allowed for isolated copies of system files, which shall be erased when the audit is completed, or given appropriate protection if there is an obligation to - keep such files under audit documentation requirements; - Requirements for special or additional processing shall be identified and agreed; - Audit tests that could affect system availability shall be run outside business hours; - All access shall be monitored and logged to produce a reference trail.

Annex A.7: Physical and Environmental Security

		Requirement
A.7-1:Secure areas	A.7-1.1:Physical security perimeter	a. MCAs shall define security perimeters to protect areas that contain either sensitive or critical information or information processing facilities. b. The following guidelines shall be documented and implemented where appropriate for physical security perimeters: - Security perimeters shall be defined, and the siting and strength of each of the perimeters shall depend on the security requirements of the assets within the perimeter and the results of - a risk assessment; - Perimeters of a building or site containing information processing facilities shall be physically sound (i.e. there shall be no gaps in the perimeter or areas where a break-in could easily occur); - The exterior roof, walls and flooring of the site shall be of solid construction and all external doors shall be suitably protected against unauthorized access with control mechanisms, (e.g. bars, - alarms, locks); doors and windows shall be locked when unattended and external protection shall be considered for windows, particularly at ground level; - A manned reception area or other means to control physical access to the site or building shall be in place; access to sites and buildings shall be restricted to authorized personnel only; - Physical barriers shall, where applicable, be built to prevent unauthorized physical access and environmental contamination; - All fire doors on a security perimeter shall be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner; - Suitable intruder detection systems shall be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied - areas shall be alarmed at all times; cover shall also be provided for other areas, e.g. computer room or communications rooms; - Information processing facilities managed by the organization should be physically separated from those managed by external parties.
	A.7-1.2:Physical entry controls	a. MCAs shall ensure:- - The date and time of entry and departure of visitors shall be recorded, and all visitors shall be supervised unless their access has been previously approved; they shall only be granted access for specific, authorized purposes and shall be issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors shall be authenticated by an appropriate means; - Access to areas where confidential information is processed or stored shall be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a - two-factor authentication mechanism such as an access card and secret PIN; - A physical log book or electronic audit trail of all access shall be securely maintained and monitored; - 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; - External party support service personnel shall be granted restricted access to secure areas or confidential information processing facilities only when required; this access shall be authorized and monitored; - Access rights to secure areas shall be regularly reviewed and updated, and revoked when necessary
	A.7-1.3:Securing offices, rooms and facilities	MCAs shall ensure:- - Key facilities are sited to avoid access by the public; - Where applicable, 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; - Facilities shall be configured to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding shall also be considered as appropriate; - Directories and internal telephone books identifying locations of confidential information processing facilities shall not be readily accessible to anyone unauthorized.
	A.7-1.4:Protecting against external and environmental threats	- Specialist advice shall be obtained from ICT Authority on how to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.
	A.7-1.5:Working in secure areas	MCAs shall consider the following: - Personnel shall only be aware of the existence of, or activities within, a secure area on a need to-know basis; - Unsupervised working in secure areas shall be avoided both for safety reasons and to prevent opportunities for malicious activities; - Vacant secure areas shall be physically locked and periodically reviewed; - Photographic, video, audio or other recording equipment, such as cameras in mobile devices, shall not be allowed, unless authorized. - The arrangements for working in secure areas include controls for the employees and external party users working in the secure area and they cover all activities taking place in the secure area.

	A.7-1.6:Delivery and loading areas	MCAs shall ensure the following: - Access to a delivery and loading area from outside of the building shall be restricted to identified and authorized personnel; - 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; - The external doors of a delivery and loading area shall be secured when the internal doors are opened; - Incoming material shall be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area; - Incoming material shall be registered in accordance with asset management procedures (see Annex A.3) on entry to the site; - Incoming and outgoing shipments shall be physically segregated, where possible; - Incoming material shall be inspected for evidence of tampering en route. If such tampering is discovered it shall be immediately reported to security personnel.

A.7-2:Equipment	A.7-2.1:Equipment siting and protection	a. MCAs shall ensure the following: - Equipment shall be sited to minimize unnecessary access into work areas; - Information processing facilities handling sensitive data shall be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use; - Storage facilities shall be secured to avoid unauthorized access; - Items requiring special protection shall be safeguarded to reduce the general level of protection required; - Controls should be adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism; - Guidelines for eating, drinking and smoking in proximity to information processing facilities shall be established; - Environmental conditions, such as temperature and humidity, shall be monitored for conditions which could adversely affect the operation of information processing facilities; - Lightning protection shall be applied to all buildings and lightning protection filters shall be fitted to all incoming power and communications lines; - The use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments; - Equipment processing confidential information shall be protected to minimize the risk of information leakage due to electromagnetic emanation.
	A.7-2.2:Supporting utilities	a. Supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) shall: - Conform to equipment manufacturer's specifications and local legal requirements; - Be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities; - Be inspected and tested regularly to ensure their proper functioning; - If necessary, be alarmed to detect malfunctions; - If necessary, have multiple feeds with diverse physical routing. - Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms. - Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider.
	A.7-2.3:Cabling security	The following guidelines for cabling security shall be implemented: - Power and telecommunications lines into information processing facilities shall be underground, where possible, or subject to adequate alternative protection; - Power cables shall be segregated from communications cables to prevent interference; - 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.
	A.7-2.4:Equipment maintenance	The following guidelines for equipment maintenance shall be implemented: - Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications; - Only authorized maintenance personnel shall carry out repairs and service equipment; - Records shall be kept of all suspected or actual faults, and of all preventive and corrective maintenance; - Appropriate controls shall be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, confidential information shall be cleared from the equipment or the maintenance personnel shall be sufficiently cleared; - All maintenance requirements imposed by insurance policies shall be complied with; - Before putting equipment back into operation after its maintenance, it shall be inspected to ensure that the equipment has not been tampered with and does not malfunction.
	A.7-2.5:Removal of assets	The following guidelines shall be implemented: - Employees and external party users who have authority to permit off-site removal of assets shall be identified; - Time limits for asset removal shall be set and returns verified for compliance; - Where necessary and appropriate, assets shall be recorded as being removed off-site and recorded when returned; - The identity, role and affiliation of anyone who handles or uses assets shall be documented and this documentation returned with the equipment, information or software.
	A.7-2.6:Security of equipment and assets off-premises	a. The use of any 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. b. The following guidelines shall be implemented for the protection of off-site equipment: - Equipment and media taken off premises shall not be left unattended in public places; - Manufacturers' instructions for protecting equipment shall be observed at all times, e.g. protection against exposure to strong electromagnetic fields; - Controls for off-premises locations, such as home-working, tele-working and temporary sites shall be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office - When off-premises equipment is transferred among different individuals or external parties, a log shall be maintained that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment.

	A.7-2.7:Secure disposal or re-use of equipment	- Equipment shall be verified to ensure whether or not storage media is contained prior to disposal or re-use. - Storage media containing confidential or copyrighted information shall be physically destroyed or the information shall be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function
	A.7-2.8:Unattended user equipment	a. 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. Users shall be advised to: - Terminate active sessions when finished, unless they can be secured by an appropriate locking - mechanism, e.g. a password protected screen saver; - Log-off from applications or network services when no longer needed; - Secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use
	A.7-2.9:Clear desk and clear screen policy	a. MCAs shall develop and implement a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities b. The clear desk and clear screen policy shall take into account the information classifications (see A-3-2), legal and contractual requirements (see A.14-1) and the corresponding risks and cultural aspects of the organization. The following guidelines shall be implemented: - Sensitive or critical business information, e.g. on paper or on electronic storage media, shall be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. - Computers and terminals shall be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and shall be protected by key locks, passwords or other controls when not in use; - Unauthorized use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) shall be prevented; - Media containing sensitive or classified information shall be removed from printers immediately.

Annex A.8: Cryptography

		Requirement
A.8-1:Cryptographic controls	A.8-1.1:Policy on the use of cryptographic controls	a. MCA shall develop and implement a policy on the use of cryptographic controls for protection of information b. The policy shall address the following - The management approach towards the use of cryptographic controls across the organization, - including the general principles under which business information should be protected; - Based on a risk assessment, the required level of protection should be identified taking into account - The type, strength and quality of the encryption algorithm required; - The use of encryption for protection of information transported by mobile or removable media devices or across communication lines; - The approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys; - Roles and responsibilities, e.g. who is responsible for: - The implementation of the policy; - The key management, including key generation (see A.8-1.2); - The standards to be adopted for effective implementation throughout the organization (which solution is used for which business processes); - The impact of using encrypted information on controls that rely upon content inspection (e.g. malware detection). c. MCA shall consult ICT Authority to get specialist advice in selecting appropriate cryptographic controls to meet the information security policy objectives.
	A.8-1.2:Key management	a. MCA shall develop and implement a policy on the use, protection and lifetime of cryptographic keys. b. The key management policy shall be based on the following: - Shall be based on an agreed set of standards, procedures and secure methods for: - Generating keys for different cryptographic systems and different applications; - Issuing and obtaining public key certificates; - Distributing keys to intended entities, including how keys should be activated when received; - Storing keys, including how authorized users obtain access to keys; - Changing or updating keys including rules on when keys should be changed and how this will be done; - Dealing with compromised keys; - Revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived); - Recovering keys that are lost or corrupted; - Backing up or archiving keys; - Destroying keys; - Logging and auditing of key management related activities. c. In order to reduce the likelihood of improper use, activation and deactivation dates for keys shall be defined so that the keys can only be used for the period of time defined in the associated key management policy. d. In addition to securely managing secret and private keys, the authenticity of public keys shall also be considered. This authentication process can be done using public key certificates, which are shall be issued by ICT authority, e. The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with ICT authority, shall cover issues of liability, reliability of services and response times for the provision of services (see A.11-2). f. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case.

Annex A.9: Access control

		Requirement
A.9-1:Business requirements of access control	A.9-1.1:Access control policy	a. MCAs shall establish, document and review an access control policy based on business and information security requirements. b. The policy shall take account of the following: - Security requirements of business applications; - Policies for information dissemination and authorization, e.g. the need-to-know principle and information security levels and classification of information (see A-3-2); - Consistency between the access rights and information classification policies of systems and networks; - Relevant legislation and any contractual obligations regarding limitation of access to data or services (see A.14-1); - Management of access rights in a distributed and networked environment which recognizes all types of connections available; - Segregation of access control roles, e.g. access request, access authorization, access administration; - Requirements for formal authorization of access requests (see A.9-2.1and A.9-2.2); - Requirements for periodic review of access rights (see A.9-2.5); - Removal of access rights (see A.9-2.5); - Archiving of records of all significant events concerning the use and management of user identities and secret authentication information; - Roles with privileged access (see A.9-2.3). c. Role based access control is an approach used successfully by many organizations to link access rights with business roles. d. The policy shall be based on need to know and need to use basis
	A.9-1.2:Access to networks and network services	a. MCAs shall develop a policy concerning the use of networks and network services. This policy shall cover: - The networks and network services which are allowed to be accessed; - Authorization procedures for determining who is allowed to access which networks and networked services; - Management controls and procedures to protect access to network connections and network services; - The means used to access networks and network services (e.g. use of VPN or wireless network); - User authentication requirements for accessing various network services; - Monitoring of the use of network services. - The policy on the use of network services should be consistent with the organization's Access Control. Policy. (SeeA.9-1.1).

A.9-2:User access management	A.9-2.1:User registration and de-registration	a. MCAs shall develop a formal user registration and de-registration process to enable assignment of access rights b. The process for managing user IDs should include: - 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; - Immediately disabling or removing user IDs of users who have left the organization (see A.9-2.5); - Periodically identifying and removing or disabling redundant user IDs; - Ensuring that redundant user IDs are not issued to other users.
	A.9-2.2:User access provisioning	a. MCAs shall develop and implement a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services. b. The provisioning process for assigning or revoking access rights granted to user IDs shall include: - Obtaining authorization from the owner of the information system or service for the use of the information system or service (see control A-3-1.2); - Separate approval for access rights from management may also be appropriate; - Verifying that the level of access granted is appropriate to the access policies (see A.9-1) and is consistent with other requirements such as segregation of duties; - Ensuring that access rights are not activated (e.g. by service providers) before authorization procedures are completed; - Maintaining a central record of access rights granted to a user ID to access information systems and services; - Adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organization; - Periodically reviewing access rights with owners of the information systems or services (see A.9-2.5).
	A.9-2.3:Management of privileged access rights	a . MCA shall ensure the allocation of privileged access rights is controlled through a formal authorization process in accordance with the relevant access control policy (see control A.9-1.1). The following steps shall be considered: - 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; - 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 (see A.9-1.1), i.e. based on the minimum requirement - for their functional roles; - An authorization process and a record of all privileges allocated should be maintained. Privileged access rights shall not be granted until the authorization process is complete; - Requirements for expiry of privileged access rights shall be defined; - Privileged access rights shall be assigned to a user ID different from those used for regular business activities. Regular business activities shall not be performed from privileged ID; - The competences of users with privileged access rights shall be reviewed regularly in order to verify if they are in line with their duties; - Specific procedures should be established and maintained in order to avoid the unauthorized use of generic administration user IDs, according to systems' configuration capabilities; - For generic administration user IDs, the confidentiality of secret authentication information shall be maintained when shared (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).
	A.9-2.4:Management of secret authentication information of users	a. MCAs shall document a formal management process for the allocation of secret authentication information. It shall include the following : - Users shall be required 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 (see A-4-1.2); - 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; - Procedures shall be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information; - Temporary 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; - Temporary secret authentication information should be unique to an individual and shall not be guessable; - Users shall acknowledge receipt of secret authentication information; - Default vendor secret authentication information shall be altered following installation of systems or software. - MCAs shall also use 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.
	A.9-2.5:Review of user access rights	MCAs shall review users' access rights at regular intervals The review of access rights shall consider the following: - Users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment (see Annex A.4); - User access rights shall be reviewed and re-allocated when moving from one role to another within the same organization; - Authorizations for privileged access rights should be reviewed at more frequent intervals; - Privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained; - Changes to privileged accounts should be logged for periodic review.
	A.9-2.5:Removal or adjustment of access rights	a. The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9-3:User responsibilities	A.9-3.1:Use of secret authentication information	All users shall be advised to: - Keep secret authentication information confidential, ensuring that it is not divulged to any other - parties, including people of authority; - Avoid keeping a record (e.g. on paper, software file or hand-held device) of secret authentication information, unless this can be stored securely and the method of storing has been approved (e.g. - password vault); - Change secret authentication information whenever there is any indication of its possible compromise; - When passwords are used as secret authentication information, select quality passwords with sufficient minimum length which are: i. Easy to remember; ii. Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.; iii. Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries); iv. Free of consecutive identical, all-numeric or all-alphabetic characters; v. If temporary, changed at the first log-on; vi. Not share individual user's secret authentication information; - Ensure proper protection of passwords when passwords are used as secret authentication - information in automated log-on procedures and are stored; - Not use the same secret authentication information for business and non-business purposes.

A.9-.4:System and application access control	A.9-4.1:Information access restriction	a. MCAs shall implement restrictions to access based on individual business application requirements and in accordance with the defined access control policy. b. MCAs shall consider the following in order to support access restriction requirements: - Providing menus to control access to application system functions; - Controlling which data can be accessed by a particular user; - Controlling the access rights of users, e.g. read, write, delete and execute; - Controlling the access rights of other applications; - Limiting the information contained in outputs; - Providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.
	A.9-4.2:Secure log-on procedures	a. MCAs shall design a procedure for logging into a system to minimize the opportunity for unauthorized access. The log-on procedure shall disclose the minimum of information about the system or application, in order to avoid providing an unauthorized user with any unnecessary assistance. b. A good log-on procedure shall - Not display system or application identifiers until the log-on process has been successfully completed; - Display a general notice warning that the computer should only be accessed by authorized users; - Not provide help messages during the log-on procedure that would aid an unauthorized user; - 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; - Protect against brute force log-on attempts; - Log unsuccessful and successful attempts; - Raise a security event if a potential attempted or successful breach of log-on controls is detected; - Display the following information on completion of a successful log-on: i. Date and time of the previous successful log-on; ii. Details of any unsuccessful log-on attempts since the last successful log-on; - Not display a password being entered; - Not transmit passwords in clear text over a network;: - 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; - Restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.
	A.9-4.3:Password management system	a. MCAs shall establish a password management system b. The password management system shall: -Enforce the use of individual user IDs and passwords to maintain accountability; -Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors; -Enforce a choice of quality passwords; -Force users to change their passwords at the first log-on; -Enforce regular password changes and as needed; -Maintain a record of previously used passwords and prevent re-use; -Not display passwords on the screen when being entered; -Store password files separately from application system data; -Store and transmit passwords in protected form.
	A.9-4.4:Use of privileged utility programs	a. In case MCA is using utility program, the following guidelines shall be considered and documented: - Use of identification, authentication and authorization procedures for utility programs; - Segregation of utility programs from applications software; - Limitation of the use of utility programs to the minimum practical number of trusted, authorized - users (see A.9-2.3); - Authorization for ad hoc use of utility programs; - Limitation of the availability of utility programs, e.g. for the duration of an authorized change; - Logging of all use of utility programs; - Defining and documenting of authorization levels for utility programs; - Removal or disabling of all unnecessary utility programs; - Not making utility programs available to users who have access to applications on systems where segregation of duties is required.
	A.9-4.5:Access control to program source code	a. MCAs shall document the following guidelines to control access to such program source libraries in order to reduce the potential for corruption of computer programs: - Where possible, program source libraries shall not be held in operational systems; - The program source code and the program source libraries shall be managed according to established procedures; - Support personnel should not have unrestricted access to program source libraries; - 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; - Program listings shall be held in a secure environment; - An audit log should be maintained of all accesses to program source libraries; - Maintenance and copying of program source libraries shall be subject to strict change control procedures (see A.10-2.2).
		If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) should be considered.

Annex A.10: Systems acquisition, development and maintenance

		Requirement
A.10-1:Security requirements of information systems	A.10-1.1:Information security requirements analysis and specification	a. When implementing information system projects, information systems related requirements shall be included b. Information security requirements shall include: - The level of confidence required towards the claimed identity of users, in order to derive user - authentication requirements; - Access provisioning and authorization processes, for business users as well as for privileged or - technical users; - Informing users and operators of their duties and responsibilities; - The required protection needs of the assets involved, in particular regarding availability, confidentiality, integrity; - Requirements derived from business processes, such as transaction logging and monitoring, non-repudiation - requirements; - Requirements mandated by other security controls, e.g. interfaces to logging and monitoring or data leakage detection systems. - Criteria for accepting products shall be defined e.g. in terms of their functionality, which will give assurance that the identified security requirements are met. Products shall be evaluated against these criteria before acquisition. Additional functionality shall be reviewed to ensure it does not introduce unacceptable additional risks. c. If products are acquired, a formal testing and acquisition process shall be followed. Contracts with the supplier shall address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls shall be reconsidered prior to purchasing the product.
	A.10-1.2:Securing application services on public networks	a. MCAs shall develop and implement policies to secure application services on public networks. b. The policies shall include: - The level of confidence each party requires in each other's claimed identity, e.g. through authentication; - Authorization processes associated with who may approve contents of, issue or sign key transactional documents; - Ensuring that communicating partners are fully informed of their authorizations for provision or use of the service; - Determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes; - The level of trust required in the integrity of key documents; - The protection requirements of any confidential information; - The confidentiality and integrity of any order transactions, payment information, delivery address - details and confirmation of receipts; - The degree of verification appropriate to verify payment information supplied by a customer; - Selecting the most appropriate settlement form of payment to guard against fraud; - The level of protection required to maintain the confidentiality and integrity of order information; - Avoidance of loss or duplication of transaction information; - Liability associated with any fraudulent transactions; - Insurance requirements. c. Application service arrangements between partners shall be supported by a documented agreement which commits both parties to the agreed terms of services, including details of authorization. d. Resilience requirements against attacks shall be considered, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service.
	14.1.3:Protecting application services transactions	MCAs shall develop policies for application service transactions that shall include the following: a) The use of electronic signatures by each of the parties involved in the transaction; b) All aspects of the transaction, i.e. ensuring that: - user's secret authentication information of all parties are valid and verified; - the transaction remains confidential; - privacy associated with all parties involved is retained; c) Communications path between all involved parties is encrypted; d) Protocols used to communicate between all involved parties are secured; e) Ensuring that the storage of the transaction details is located outside of any publicly accessible environment, e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on a storage medium directly accessible from the Internet; f) Where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

A.10-2:Security in development and support processes	A.10-2.1:Secure development policy	a. MCAs shall develop policies for secure software development a. If development is outsourced, the organization should obtain assurance that the external party complies i). With these rules for secure development (see A.10-2.7). ii). The policy shall contain the following: - Security of the development environment; - Guidance on the security in the software development lifecycle: - Security in the software development methodology; - Secure coding guidelines for each programming language used; - Security requirements in the design phase; - Security checkpoints within the project milestones; - Secure repositories; - Security in the version control; - Required application security knowledge; - Developers' capability of avoiding, finding and fixing vulnerabilities.
	A.10-2.2:System change control procedures	1. Formal change control procedures shall be documented by MCAs and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts. 2. The change control procedures shall include but not be limited to: - Maintaining a record of agreed authorization levels; - Ensuring changes are submitted by authorized users; - Reviewing controls and integrity procedures to ensure that they will not be compromised by the changes; - Identifying all software, information, database entities and hardware that require amendment; - Identifying and checking security critical code to minimize the likelihood of known security weaknesses; - Obtaining formal approval for detailed proposals before work commences; - Ensuring authorized users accept changes prior to implementation; - Ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of; - Maintaining a version control for all software updates; - Maintaining an audit trail of all change requests; - Ensuring that operating documentation (see A.6-1.1) and user procedures are changed as necessary to remain appropriate; - Ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.
	A.10-2.3:Technical review of applications after operating platform changes	MCAs shall document and implement procedures to ensure that when operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security. This process shall cover: - Review of application control and integrity procedures to ensure that they have not been compromised - by the operating platform changes; - Ensuring that notification of operating platform changes is provided in time to allow appropriate - tests and reviews to take place before implementation; - Ensuring that appropriate changes are made to the business continuity plans (see Annex A.13).
	A.10-2.4:Restrictions on changes to software packages	a. MCAs shall document policies for discouraging modifications to software packages and limiting to necessary changes in a controlled manner. b. The policy shall contain the following:- Where a software package needs to be modified the following points shall be considered: - The risk of built-in controls and integrity processes being compromised; - Whether the consent of the vendor should be obtained; - The possibility of obtaining the required changes from the vendor as standard program updates; - The impact if the organization becomes responsible for the future maintenance of the software as a result of changes; - Compatibility with other software in use.

	A.10-2.5:Secure system engineering principles	a. MCA shall establish, document, maintain and review principles for engineering secure systems information system implementation efforts b Security shall be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility.
	A.10-2.6:Secure development environment	MCAs shall develop and implement policies for secure development environment. The policies shall address: - Sensitivity of data to be processed, stored and transmitted by the system; - Applicable external and internal requirements, e.g. from regulations or policies; - Security controls already implemented by the organization that support system development; - Trustworthiness of personnel working in the environment (see A-4-1.1); - The degree of outsourcing associated with system development; - The need for segregation between different development environments; - Control of access to the development environment; - Monitoring of change to the environment and code stored therein; - Backups are stored at secure offsite locations; - Control over movement of data from and to the environment.
	A.10-2.7:Outsourced development	MCAs shall develop and implement policies for outsourced development. The policy shall address: - Licensing arrangements, code ownership and intellectual property rights related to the outsourced - content (see A.14-1.2); - Contractual requirements for secure design, coding and testing practices (see A.10-2.1); - Provision of the approved threat model to the external developer; - Acceptance testing for the quality and accuracy of the deliverables; - Provision of evidence that security thresholds were used to establish minimum acceptable levels of - security and privacy quality; - Provision of evidence that sufficient testing has been applied to guard against the absence of both - intentional and unintentional malicious content upon delivery; - Provision of evidence that sufficient testing has been applied to guard against the presence of known - vulnerabilities; - Escrow arrangements, e.g. if source code is no longer available; - Contractual right to audit development processes and controls; - Effective documentation of the build environment used to create deliverables; - The organization remains responsible for compliance with applicable laws and control efficiency verification.
	A.10-2.8:System security testing	a. MCAs shall document requirements to ensure new and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests shall initially be performed by the development team. Independent acceptance testing shall then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected (see A.10-1.1and 14.1.9). The extent of testing shall be in proportion to the importance and nature of the system.
	A.10-2.9:System acceptance testing	a. Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions. b. System acceptance testing shall include testing of information security requirements (see A.10-1.1andA.10-1.2) and adherence to secure system development practices (see A.10-2.1). The testing should also be conducted on received components and integrated systems. Organizations can leverage automated tools, such as code analysis tools or vulnerability scanners, and should verify the remediation of security related defects. c. Testing shall be performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the organization's environment and that the tests are reliable.
A.10-3:Test data	A.10-3.1:Protection of test data	a. MCA policies shall prohibit the use of operational data containing personally identifiable information or any other confidential information for testing purposes. b. If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content shall be protected by removal or modification. c. The following guidelines shall be guide the policy to protect operational data, when used for testing purposes: - The access control procedures, which apply to operational application systems, shall also apply to test application systems; - There should be separate authorization each time operational information is copied to a test environment; - Operational information should be erased from a test environment immediately after the testing is complete; - The copying and use of operational information shall be logged to provide an audit trail.

Annex A.11: Supplier Relationships

		Requirement
A.11-1:Information security in supplier relationships	A.11-1.1:Information security policy for supplier relationships	a. MCAs shall agree with suppliers and document policies for supplier's access to the organization's assets b. These controls shall address processes and procedures to be implemented by the MCA, as well as those processes and procedures that the MCA shall require the supplier to implement, including: - Identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the MCA will allow to access its information; - A standardized process and lifecycle for managing supplier relationships; defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access; - Minimum information security requirements for each type of information and type of access to - Serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile; - Processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation; - Accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party; - Types of obligations applicable to suppliers to protect the organization's information; - Handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers; - Resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party; - Awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes and procedures; - Awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behavior based on the type of supplier and the level of - Supplier access to the organization's systems and information; Conditions under which information security requirements and controls will be documented in an agreement signed by both parties; - Managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.
	A.11-1.2:Addressing security within supplier agreements	a. Supplier agreements shall be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements. b. The following terms shall be considered for inclusion in the agreements in order to satisfy the identified information security requirements: - Description of the information to be provided or accessed and methods of providing or accessing the information; - Classification of information according to the organization's classification scheme (see A-3-2); if necessary also mapping between the organization's own classification scheme and the classification scheme of the supplier; - 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; - Obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing; - Rules of acceptable use of information, including unacceptable use if necessary; - Either explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel; - Information security policies relevant to the specific contract; - Incident management requirements and procedures (especially notification and collaboration during incident remediation); - Training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures; - Relevant regulations for sub-contracting, including the controls that need to be implemented; - Relevant agreement partners, including a contact person for information security issues; - Screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern; - Right to audit the supplier processes and controls related to the agreement; - 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; - Supplier's obligations to comply with the organization's security requirements.

	A.11-1.3:Information and communication technology supply chain	a. Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. b. The following topics shall be considered for inclusion in supplier agreements concerning supply chain security: - Defining 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; - 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; - For information and communication technology products, requiring that suppliers propagateappropriate security practices throughout the supply chain if these products include components purchased from other suppliers; - Implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements; - 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; - Obtaining assurance that critical components and their origin can be traced throughout the supply chain; - Obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features; - Defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers; - Implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks - 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.
A.11-2:Supplier service delivery management	A.11-2.1:	MCAs shall regularly monitor, review and audit supplier service delivery: This shall involve: - Monitoring service performance levels to verify adherence to the agreements; - Reviewing service reports produced by the supplier and arrange regular progress meetings as required - by the agreements; - Conducting audits of suppliers, in conjunction with review of independent auditor's reports, if available, - and follow-up on issues identified; - Providing information about information security incidents and review this information as required - by the agreements and any supporting guidelines and procedures; - Reviewing supplier audit trails and records of information security events, operational problems, - failures, tracing of faults and disruptions related to the service delivered; - Resolving and manage any identified problems; - Review information security aspects of the supplier's relationships with its own suppliers; - 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 (see Annex 13).

Annex A.12: Information security incident management

		Requirement
A.12-1:Management of information security incidents and improvements	A.12-1.1:Responsibilities and procedures	a. MCAs shall establish management responsibilities and procedures to ensure a quick, effective and orderly response to information security incidents. b. Management responsibilities shall be established to ensure that the following procedures are developed and communicated adequately within the organization: 1. Procedures for incident response planning and preparation; 2. Procedures for monitoring, detecting, analyzing and reporting of information security events and incidents; 3. Procedures for logging incident management activities; 4. Procedures for handling of forensic evidence; 5. Procedures for assessment of and decision on information security events and assessment of information security weaknesses; 6. Procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organizations; c. Procedures established shall ensure that: 1. competent personnel handle the issues related to information security incidents within the 2. organization; 3. a point of contact for security incidents' detection and reporting is implemented; 4. appropriate contacts with authorities, external interest groups or forums that handle the issues 5. related to information security incidents are maintained; d. Reporting procedures shall include: 1. Preparing information security event reporting forms to support the reporting action and to help 2. the person reporting to remember all necessary actions in case of an information security event; 3. The procedure to be undertaken in case of an information security event, e.g. noting all details 4. immediately, such as type of non-compliance or breach, occurring malfunction, messages on the 5. screen and immediately reporting to the point of contact and taking only coordinated actions; 6. Reference to an established formal disciplinary process for dealing with employees who commit 7. security breaches; 8. Suitable feedback processes to ensure that those persons reporting information security events are notified of results after the issue has been dealt with and closed.
	A.12-1.2:Reporting information security events	a. All employees and contractors shall be made aware of their responsibility to report information security events as quickly as possible. b. They shall also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported. c. Situations to be considered for information security event reporting include: - ineffective security control; - breach of information integrity, confidentiality or availability expectations; - human errors; - non-compliances with policies or guidelines; - breaches of physical security arrangements; - uncontrolled system changes; - Malfunctions of software or hardware; access violations.
	A.12-1.3:Reporting information security weaknesses	a. All employees and contractors shall report to note and report any observed or suspected information security weaknesses in systems or services matters to the point of contact as quickly as possible in order to prevent information security incidents. The reporting mechanism shall be as easy, accessible and available as possible.
	A.12-1.4:Assessment of and decision on information security events	a. Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents b. 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. c. Classification and prioritization of incidents can help to identify the impact and extent of an incident. d. 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. e. Results of the assessment and decision shall be recorded in detail for the purpose of future reference and verification.
	A.12-1.5:Response to information security incidents	a. MCAs shall document procedures for response to information security incidents b. The response shall include the following: - Collecting evidence as soon as possible after the occurrence; - Conducting information security forensics analysis, as required (see A.12-1.7); - Escalation, as required; - Ensuring that all involved response activities are properly logged for later analysis; - 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; - Dealing with information security weaknessles) found to cause or contribute to the incident; - Once the incident has been successfully dealt with, formally closing and recording it. c. Post-incident analysis should take place, as necessary, to identify the source of the incident.
	A.12-1.6:Learning from information security incidents	a. Knowledge gained from analyzing and resolving information security incidents shall be documented and used to reduce the likelihood or impact of future incidents. b. 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.
	A.12-1.7:Collection of evidence	a. The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. b. 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. a. The procedures shall take account of: o chain of custody; o safety of evidence; o safety of personnel; o roles and responsibilities of personnel involved; o competency of personnel; o documentation; o briefing.

Annex A.13: Information security aspects of business continuity

		Requirement
A.13-1:Information security continuity	A.13-1.1:Planning information security continuity	a. MCAs shall determine whether the continuity of information security is captured within the business continuity management process or within the disaster recovery management process. b. Information security requirements shall be determined when planning for business continuity and disaster recovery. c. In the absence of formal business continuity and disaster recovery planning, information security management shall assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. d. Alternatively, an MCA could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.
	A.13-1.2:Implementing information security continuity	a. The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation b. An MCA shall ensure that: - an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence; - incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated; - documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives (see A.13-1.1). c. According to the information security continuity requirements, the MCA shall establish, document, implement and maintain: - Information security controls within business continuity or disaster recovery processes, procedures - and supporting systems and tools; - Processes, procedures and implementation changes to maintain existing information security - controls during an adverse situation; - Compensating controls for information security controls that cannot be maintained during an adverse situation.
	A.13-1.3:Verify, review and evaluate information security continuity	- MCAs shall verify their information security management continuity by: - Exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives; - Exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives; - Reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/ disaster recovery management processes and solutions change.

A.13-2:Redundancies	A.13-3.1:Availability of information processing facilities	a. MCAs shall identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures shall be considered. b. Where applicable, redundant information systems shall be tested to ensure the failover from one component to another component works as intended.

Annex A.14: Compliance

		Requirement
A.14-1:Compliance with legal and contractual requirements	A.14-1.1:Identification of applicable legislation and contractual requirements	a. All relevant legislative statutory, regulatory, contractual requirements and the MCA's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization b. The specific controls and individual responsibilities to meet these requirements shall also be defined and documented. c. Managers shall identify all legislation applicable to their MCA in order to meet the requirements for their type of business.
	A.14-1.2:Intellectual property rights	The following guidelines shall be considered to protect any material that may be considered intellectual property: - Publishing an intellectual property rights compliance policy which defines the legal use of software - and information products; - Acquiring software only through known and reputable sources, to ensure that copyright is not violated; - Maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them; - Maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights; - Maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.; - Implementing controls to ensure that any maximum number of users permitted within the license is not exceeded; - Carrying out reviews that only authorized software and licensed products are installed; - Providing a policy for maintaining appropriate license conditions; - Providing a policy for disposing of or transferring software to others; - Complying with terms and conditions for software and information obtained from public networks; - Not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law; - Not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.
	A.14-1.3:Protection of records	To meet these record safeguarding objectives, the following steps should be taken within an organization: - Guidelines shall be issued on the retention, storage, handling and disposal of records and information; - A retention schedule shall be drawn up identifying records and the period of time for which they shall be retained; - An inventory of sources of key information shall be maintained.
	A.14-1.4:Privacy and protection of personally identifiable information	a. An MCA's data policy for privacy and protection of personally identifiable information shall be developed and implemented. This policy shall be communicated to all persons involved in the processing of personally identifiable information.
	A.14-1.5:Regulation of cryptographic controls	Legal advice shall be sought to ensure compliance with relevant legislation and regulations when using cryptography
	A.14-1.6:Information security reviews	- Management shall initiate the independent review - Such a review shall be carried out by individuals independent of the area under review - The results of the independent review shall be recorded and reported to the management who initiated the review. These records shall be maintained. - If the independent review identifies that the organization's approach and implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies (see A.1-1), management shall consider corrective actions.
	A.14-1.7:Compliance with security policies and standards	a. Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. b. Managers shall identify how to review that information security requirements defined in policies, standards and other applicable regulations are met. Automatic measurement and reporting tools shall be considered for efficient regular review. c. If any non-compliance is found as a result of the review, managers shall: - identify the causes of the non-compliance; - evaluate the need for actions to achieve compliance; - implement appropriate corrective action; - review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.
	A.14-1.8:Technical compliance review	a. Technical compliance shall be reviewed preferably with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer could be performed. b. If penetration tests or vulnerability assessments are used, caution shall be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable. c. Any technical compliance review shall only be carried out by competent, authorized persons or under the supervision of such persons.

APPENDIX

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 MCA		
		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 MCA 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 business areas within the MCA 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 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	MCA Records Management Program in Place. MCA 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. MCA 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)		
		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	MCA 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	MCA equipment is located in secure areas. Records of routine checks confirm that these areas are accessible only to authorised personnel		
		38	MCA 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, 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 (eg. 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. MCA 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. MCA 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 MCA, 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 MCA.		
		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 relevant senior executive/ governance body and has been implemented within the MCA		
	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 consistent with business requirements		
		68	Access control rules are consistent with information classification		
		69	Access control rules are consistent with legislative obligations		
	Authentication	70	MCA 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. MCA records indicate that online transactions and services have been assessed against the standard		
		71	MCA records indicate that all authentication of users external to the MCA have been assessed against the standard		
	User access	72	MCA information systems cannot be accessed without specific authorisation. MCA records that may indicate evidence of compliance include completed system access request forms for all users		
		73	MCA records indicate that each user is issued a unique personal identification code and secure means of authentication		
	Network access	74	MCA records indicate that system and network access and use is logged, monitored and reviewed. Events are recorded		
		75	MCA records indicate that authorisation has been obtained and documented for new and 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	MCA 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	MCA 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	MCA records indicate that mobile technologies and tele-working facilities are not introduced unless a risk assessment has been performed		
		80	MCA has documented and approved processes for mobile technologies and teleworking facilities		

Information Systems Acquisition Development and Maintenance	Security Systems Requirements	81	MCA 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 or significant changes to financial or critical business information systems		
		84	Documented system security controls address acquisition, development and maintenance stages		
		85	MCA records document change control, acceptance and system testing, planning and migration control measures have been taken when upgrading or installing software		
		86	MCA 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 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	MCA 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 MCA'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 MCA's information security policies and processes and details of where employees can go to get further information		
		101	The information security training plan includes targeted training in the MCA'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 MCA information security policies and processes including how to use MCA 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 MCA have been approved		
		107	MCA records demonstrate that all employee separations follow the approved procedure		
		108	Procedures for the movement of employees within the MCA have been approved		
		109	MCA records demonstrate that all employee movements within the MCA follow the approved procedure		
Incident Management	Incident Management Controls	110	Copies of information security incident reports are present. Receipt of incident reports by 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 incident management 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 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 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 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		

Appendix II: Acceptable Use of Computing Resources (Assets) Sample policy

Subject	Requirement
General	• All MCA 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 MCAs 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 MCA. • The MCA 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 accounts, such as for access to network- or host-based resources.

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 MCA 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 MCA through the use of MCA assets is also unacceptable use.
	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 MCA 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 MCA. 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 MCA 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.
	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 MCA privacy policies and agreements. The MCA strictly 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 MCA 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 MCA.
	9.Disclosure of protected information Disclosing MCA 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 MCA resources to conduct non-MCA business MCA 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 MCA computers to store, forward, copy or manage information for any other MCA; the use of MCA equipment to produce printed or electronic documents for any other MCA or MCA; or the use of any MCA resources, including personnel time, for the furtherance of any other MCA or MCA. 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 MCA 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 MCA, individuals are not authorized to communicate news of such incidents to any outside party. It is solely the MCA's responsibility to appropriately notify public MCAs of security incidents in compliance with state and federal regulations.

Policy Enforcement and Limitation of Liability to the MCA	The MCA will take all reasonable measures to ensure that compliance with all applicable laws occurs with respect to the acceptable use of computing resources. The MCA will also undertake training and awareness programs to ensure that all employees, contractors, temporaries and vendors are informed of this, and other, policies. The MCA 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 MCA 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 MCA. 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 MCA as a whole.
	2.Automated methods for policy enforcement The MCA will implement automated methods for monitoring MCA assets for unacceptable use and abuse. These automated methods will assist the MCA 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 MCA 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 MCA finds that it is in violation of this policy, immediate actions will be taken to bring the MCA into compliance. If the MCA 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 MCA caused or authorized the violation, a decision will have to be made about whether or not the offending action should be halted or permitted.
	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 MCA through appropriate channels, including but not limited to, MCA wide electronic mail, announcement at MCA meetings, and the distribution of updated MCA policy documents.
Agreement to and Acceptance of this Policy	• By accepting employment with the MCA and using computing resources owned by the MCA, 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 MCA 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 MCA may monitor and respond to my use of computing resources in accordance with this, and other, MCA 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.
	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 MCA 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.
	Moral Implications: Right vs. Wrong • MCAs are not allowed to promote illegal or illicit activity and are constrained to ensure, 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.

	Legal Implications: Indemnification Against Direct Liability • The creation and promotion of policies, standards, guidelines and procedures are used by MCAs 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 MCA 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 MCA 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 MCA 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.
	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 MCA, 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.
	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 MCA 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.
	Legal Implications: Implied Contractual Obligations • Acceptable Use of Computing Resources" serves as an implied set of contractual obligations. • The MCA 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.

Appendix III: Related Documents

Code Number:	Title
ICTA. 1.001: 2016	Government Enterprise Architecture
ICTA. 2.001: 2016	Infrastructure Standard (Networks, Cloud, End user Computing Devices, Data Centre)
ICTA. 3.001: 2016	Information Security Standard
ICTA. 4.001: 2016	Electronic Records and Data Management Standard
ICTA. 5.001: 2016	IT Governance Standard
ICTA. 6.001: 2016	Systems and Application Standard
ICTA. 7.001: 2016	ICT Human Capital and Work force Development Standard

ICT Authority
Telposta Towers, 12th Floor, Kenyatta Ave
P.O. Box 27150 - 00100 Nairobi, Kenya
t: + 254-020-2211960/62
Email: info@ict.go.ke or communications@ict.go.ke or standards@ict.go.ke
Visit: www.icta.go.ke
Become a fan: www.facebook.com/ICTAuthorityKE
Follow us on twitter: @ICTAuthorityKE


ICT
Authority