BANK OF TANZANIA

Summary of Changes

on

Information Security Guidelines Document

1. Introduction

The Bank has formulated the Information Security Policy to govern IT security in the Bank. To facilitate implementation of the Information Security Policy, 2014 the Management prepared an Information Security Guidelines of 2015.

The Information Security Policy, 2014 was reviewed and approved in October 2021 to incorporate practices recommended by recently enacted laws and changes that occurred in the Bank.

The review of the Information Security Guidelines, 2015 has been necessitated by the changes on the Information Security Policy, compliance with laws and guidance provided by Government Authorities and adoption of new information technologies.

Therefore, this document presents amendments made on the Information Security guidelines of 2015.

2. Objectives

To outline changes made on the Information Security guidelines document following a review held in March 2022.

3. Detail of Amendments

Details of amendments performed are presented in table 1.

Table 1: Amendments Details

S/N	Section	Section No.	Amendments
1	Cover Page	-	• Added a year of review of the guidelines.
2	Document Control	-	• Updated a list of authors • Changed approving mandate from Management Committee to ICT Steering Committee. *This is to align with current Bank IT Governance structure defined in the IT Governance Framework* • Added an item on reviewers • Changed dates for authoring, approval, and distribution to current dates • Updated amendment history to reflect current reviews
3	Abbreviation	-	• Removed MRC (Management Risk Committee), CIRT (Computer Incident Response Team) and SSL (Secure Socket Layer) as the terms are not used in recent guidelines

4	Glossary of terms	-	• Omitted the term asset as in the context of these guidelines the focus is on "information asset" the term which is defined in the document • Added the term "Antimalware" the term which refers to various malicious software including virus, worms, trojan horse, adware and ransomware • Updated the meaning of the term "Certificate Authority (CA)" by omitting the word "third party". This is to provide wider meaning that include CA maintained by the Bank • Added the term "data center" a term that provide a broad meaning of areas where information processing facilities are deployed • Added the term "Endpoints Devices" and its meaning. The term was introduced to protect end -user devices such as desktop, laptops and ipads. • Added the term "firewall" to provide more clarity to audience. The term was used but its meaning was not provided. • Added the meaning of the term "Information System" which was used in the document without being defined • Updated the meaning of the term "Intranet" to provide more clarity • Added the term" Multi-factor Authentication" and its meaning to provide clarity to audiences • Added the term "Non-Disclosure Agreement" introduced in the revised guidelines • Removed the term "Normal change" as the term is not used in the revised guidelines • Removed the term "standard change" as the term is not used in the revised guidelines

			• Updated the meaning of "Peer-to-peer" to provide more clarity • Removed the term "SSL" as the term is not used in this document. The successor of SSL is TLS which is defined • Replaced the term "Social Network" with "Social Media" to provide wider context of platforms used to share information. The meaning of the term was also updated • Added the term "Virtual Meeting" a new term introduced in the revised guidelines • Added the meaning of the term "Wireless Local Area Networks (WLAN)". The term was used but its meaning was not provided
5	Introduction	1.	On the second sentence, the following changes were made: • The phrase "Recognizing" was replaced by the phrase "In recognizing the" • Replaced 2014 with 2021 the year of approval of the Information Security Policy • "Information asset" replaced by them to avoid repetition of the phrase On 3rd sentence, omitted the "information security" to avoid repetition
6	Objective	2.	• Nil
7	Scope	3.	• Nil
8	Access Control	4.	• The 1st sentence was replaced by "Access to information and information systems need to be controlled on the basis of business and security requirements." *This is to provide a more focussed objective of the section*
9	Business Requirements for Access Control	4.1	• On item (ii), the phrase "on the basis of" was replaced by the phrase " based on" to provide more clarity
10	User Access Management	4.2	• Nil
11	User registration	4.2.1	• Nil

12	User De-activation and Activation	4.2.2	• Item (i) was amended to remove the requirement of the user to request for inactivation when on leave exceeding 14 days. Deactivation will be made to staff on unpaid leave, suspension, full-time training or secondment. *This is to align with current Bank practices and to improve employee productivity.* • Added a new item to guide on retirees to access information related with their active accounts maintained at the Bank. The item reads "Retirees shall only be provided with access to the retirees portal that shall offer limited services regarding their accounts maintained with the Bank" • Item (ii) was amended by omitting the requirement of being deactivated once on leave exceeding 14 days. The deactivation will be made upon receipt of notification from the Head Human Resource and Administration or from the Head Management Information System functions. *This is to align with current Bank practices and to improve employee productivity.* • On item (iii) the staff payment system is added in the list of systems excepted from activation. *This is because employees on unpaid leave, suspension, full-time training or secondment will still need access to the staff portal*
13	Maintenance and Review of User Access Rights	4.2.3	• Nil
14	Handling of Administrator and System Accounts	4.2.4	• Omitted the word "function" to maintain consistency • On item (ii), the word "Authentication" was added at the beginning of the sentence to provide more clarity
15	Network access	4.3	• Nil
16	Intranet Access Control	4.3.1	• On item (i) the phrase "so as to" was replaced by "to" to be concise.
17	Extranet Access Control	4.3.2	• Added a new item (iv) to require business partners intending to establish site-to-site network connectivity with the Bank network to provide independent assurance report to indicate that adequate security controls have been implemented. *This is to protect the Bank network resources against attacks that may emanate from Business partners.* The added item reads "Where there is a need to establish a site-to-site connectivity with a business partner, the Bank shall require the business partner to provide an independent assurance report indicating adequacy of security

			controls of the application intending to interact with Bank application prior to establishment of such connectivity."
18	Wireless Access Control	4.3.3	• Existing item (i) was split into two items to provide clarity. One item to focus on controls for access WLAN whereas the second item is to focus on service provided with WLAN • Item (i) was amended to indicate that WLAN shall be accessible by pre-registered devices only. *This is to enhance security of WLAN service* • Existing item (iv) was amended by removing the phrase "so that those devices are not operating with default settings" as *the phrase was narrowing the scope of securing WLAN. The item was also updated to set broad security requirements.* The item now reads "Network Administrator shall ensure that Bank network devices delivering wireless network services are securely configured"
19	Remote Access Control	4.3.4	• On item (ii), omitted the phrase "from the Internet is authenticated and". *This aimed at introducing a more concise requirement on authentication which is provided for in a new item (iv)* • Added item (iv) to require strong authentication for any remote access to Bank internal network. The item reads "Network Administrators shall ensure that any remote access to internal networks uses strong authentication mechanism."
20	Internet Access Control	4.3.5	• In item (ii), the phrase "entering" was replaced by "entering or leaving". *This to require filtering for both incoming and outgoing network traffic to enhance security.*
21	Operating System Access Control	4.4	• Nil
22	Database Access Control	4.5	• On item (ii), the phrase "day to day" was replaced by "day-to-day" to be concise • On item (vi), the phrase "taking into account" was replaced by "considering" to be concise
23	Application Access Control	4.6	• On Item (iii), the phrase "adequate authentication mechanisms" was replaced by "strong authentication mechanisms" *to maintain consistency* • Item (v), added the word "form" after the word "text" *for clarity* • Item (v), removed the word "sensitive" between the words "transfer" and "data". *This is to align with existing practices.* • Item (viii) was rephrased to read "No change on application shall be applied into a production

			unless tested and authorized". *This is provide clarity*
24	Physical Access to Information Systems	4.7	• Section heading was renamed to read "Physical Access to Data Center and Computer Rooms" to provide more clarity • Existing sentence "Information systems such as servers and network devices shall be protected against physical related attacks" was removed as it was too generic • Added five items as presented below: (i) access to areas where information systems are deployed shall be restricted to authorized individual. (ii) Entries to areas where information systems are stored shall be controlled by use of a combination of strong authentication mechanisms such as access control card, PIN, or biometric controls. (iii) Audit trails for individuals gaining physical access to information systems areas shall be securely maintained. (iv) Visitors and Third parties shall be supervised and be granted access for specific and authorized purposes (v) Access rights to secure areas shall be regularly reviewed, updated, and revoked when necessary • Three more items were added by relocating them from section 13 as the items are more relevant under this section. Added items are: (vi) Head Network and Office Automation shall authorize granting of access to data centers or computer room premises (vii) Head Internal Security or Branch Security Officer shall ensure monitoring of access to information System premises (viii) Head Internal Security shall put in place controls for restricting visitors and third party from accessing data center or computer room premises
25	Protection of Endpoint Devices	4.8	• A new section which was added to provide guidance on protection of endpoint devices • Added items under this section are: (i) Endpoint devices shall not be connected on Bank internal network without authorization. (ii) Employees are responsible to protect Bank information stored on endpoint devices (iii) Employees shall timely report to the Bank through helpdesk in the event of stolen or

			lost endpoint device that contains Bank information (iv) Endpoint devices shall be installed with antimalware protection that shall regularly be updated (v) Employees or third party are responsible to timely apply security patches on endpoint devices used to process or access the Bank internal network resources (vi) Endpoint devices used by third party to access the Internet only especially using guest WLAN shall not be subjected to authorization.
26	Protection of Information Assets	5.	• In the opening paragraph, the sentence "The Bank needs to properly protect such asset" was replaced by "thus, underscores the importance of protecting such assets. " *to provide logical flow between the two sentences*
27	Ownership and Inventory of Information Assets	5.1	• In item (ii), replaced the word "responsible" with "respective" to use a more appropriate term
28	Handling and Disposal of Storage Media	5.2	• Nil
29	Information Classification	5.3	• In item (i), the phrase "sensitivity" was replaced by the phrase "value, legal requirements, sensitivity, and criticality to the Bank". *To provide broader attributes to be considered during information classification* • Added new item (ii) that reads "Information shall be provided with adequate level of protection considering its confidentiality, integrity and availability". *To ensure that information is protected according to their classification* • Rephrased existing sentence to read "Head of Business Units shall review classification of information assets whenever need arises". This is to providing clarity.
30	Exchange of Information	5.4	• Added an item to require use of secure channels when exchanging information. *This is to ensure information are not disclosed to an unintended recipients.*
31	Acceptable Use of Email, Intranet and Internet	6.	• Title amended to include IT conference facilities and social media. Thus the new section heading is "Acceptable Use of Email, Intranet, Internet, IT conference facilities and Social media" • In the opening paragraph, the phrase " so as to" was replaced by "to" *to be concise*
32	E-Mail Usage	6.1	• Nil

33	E-mail Addresses	6.1.1	Item (ii) on use of auto-reply email feature was modified t*o align with global practices. Retained and modified item reads:* • "Employees may use auto-reply email feature when absent from the office to facilitate business continuity. However, employees shall be cautious with contents included in the auto-reply email to minimize possibility of security compromise."
34	Email Communication	6.1.2	• On item (vii) removed the word "junk" *to cover more broad email related attacks* • In item (viii) replaced the word "detailed" with "A detailed" *for clarity*
35	E-mail Security	6.1.3	• On item (iv), added the word "web" between the words unattended and email. The requirement only applies to email service accessible through the web.
36	Managing E-mail Records	6.1.4	• Nil
37	Internet usage	6.2	• Nil
38	Personal use of the Internet	6.2.1	• Nil
39	Compliance to license and copyright requirements	6.2.2	• On item (i) replaced the phrase intellectual properties laws" with "laws including but not limited to Intellectual Property laws". This is to require staff to observe requirement of various laws
40	Protection of Bank's internal network	6.2.3	• Item (i) updated to be more restrictive on use of portable storage media in line with *current Bank practices and to mitigate risks associated with use of such devices* • Item (ii) updated to be in line with updated item (i) by replacing the word "user" with "Authorized users" and the phrase "prior to using them" replaced with "when used" • In item (iv), the phrase "against external attacks" was replaced by "against attacks" to reflect the facts that *contents may lead to both internal or external attacks*
41	Social Media	6.2.4	• Added item (ii) that reads "Private use of social media by employees shall be in line with the Bank Communication Strategy". This is to alert Bank employees on secure private use of social media and consequences that may arise.
42	Preserving Internet bandwidth	6.2.5	• Item (i) updated to indicate that employees are allowed to use Internet Telecommunication facilities only for Bank related operations. *This is to keep abreast with current practices at the Bank and to increase employee productivity.*

43	Monitoring internet usage	6.2.6	• Nil
44	Intranet Access	6.3	• Nil
45	Use of Intranet	6.3.1	• Nil
46	Publishing on the Internal and public website	6.4	• On item (i), removed the phrase "Bank Intranet and". *This item is to focus on providing guidance on publishing on the Bank Internet website only* • Added item (ii) to provide guidance for publishing contents on Bank intranet. *To align with existing Bank practices where Business Units are involved in updating the intranet.*
47	Use of Information Technology Conference Facilities	6.5	• Added a new subsection to provide guidance on secure use of Information Technology Conference Facilities which was recently adopted at the Bank • Added items under this section are: (i) Organization of virtual meetings shall be carefully arranged to involve only eligible participants. (ii) Employees are required to observe sensitivity of information and environment being shared through IT conference facilities (iii) Security features built-in IT conference facilities shall be utilized to ensure safe participation in virtual meetings
48	Password Management	7.	• Under the opening paragraph, the phrase "has to" was replaced by "must". Also the phrase "so as to" replaced by "to". *This is to be concise.* •
49	Password Features	7.1	• Changed the section heading from "password features" to "password requirements" • On item (ii), time to reuse the password from 120 to 180 days. Also added the phrase "or after six cycles of password change". This is to provide flexibility on enforcing the requirement. • Added item (iii) that reads "Password shall not be similar to a user id or contain employee common details". *This is to emphasize more on secure password requirements*
50	Changing Passwords	7.2	• Nil
51	System password requirements	7.3	• Item (vii) amended by inserting the word "creation" between the words support and unique *to provide clarity*. Also replaced the

			word "group" and "generic". This is to use a commonly used term
52	Protection of Administrative Passwords	7.4	• Item (ii) was amended to read "Use of administrative accounts to perform non administrative operations is prohibited." *To discourage use of system account while performing non-administrative tasks as it may read to unnecessary risk exposure to the Bank* • Added a new item that reads "Direct access of system using system administrative accounts is prohibited." *To enhance accountability of activity performed by Administrators.* • Existing items (iii), (iv) and (v) were removed as were not practically implementable. • On existing item (vi), inserted the word "administrative" between the words "system" and "account" for clarity. The item was also amended to remove conflict with removed items (iii), (iv) and (v).
53	Handling Third Parties	8.	• On last sentence of the opening paragraph removed the phrase "so as" for clarity
54	Information Security in Third Party Agreements	8.1	• Added item to enforce non-disclosure agreement or form for Government employees involved in Bank operations on demand basis. The added item reads "Where a Third Party is an employee of the Government of Tanzania, such an employee shall be required to adhere to Bank Information Security policy including signing a Non-Disclosure Agreement or form"
55	Monitoring and Review of Third Party Services	8.2	• The phrase "Responsible Business Unit" was replaced by "Head of Management Information". *To align the responsibilities with existing mandates*
56	Managing Changes to Third Party Services	8.3	Replaced the word before with "without consultation with the Head of Management Information System and". *This is to guide Business Unit not to perform changes on IT related third party service without informing the Head Management Information Systems*
57	Monitoring of Information Security	9.	• In the opening paragraph, added the following sentences: "Various approaches are applied to assess effectiveness of information security controls and detection of security breaches. These include performing periodic technology vulnerability assessments and penetration testing, reviewing of logs and timely reporting of security breaches. "

			This is to broaden coverage of issues covered under the section.
58	Technology Vulnerability Management	9.1	• On item (ii), replaced the phrase "under item (ii)"with the phrase "as a result of vulnerability assessment". *This is for simplicity.* • Item (v), the phrase "maintained confidentially" replaced with "confidentially maintained"
59	Penetration Testing of Information Systems	9.2	• The section was added to provide guidance on penetration testing which is a requirement by the e-Government Act. • Added the following: (i) Head of Information Systems Services shall carry out penetration testing of information systems on a regular basis to identify weaknesses and propose appropriate measures. (ii) The Head of Information Management Systems shall authorize penetration testing to be carried out by government authorities or any other authorized entity to be approved on need basis. (iii) Responsible Heads of Business Units shall implement measures proposed as a result of penetration testing to address the identified vulnerabilities in line with change management procedures. (iv) Results of penetration testing on Bank Information Systems shall be confidentially maintained.
60	Collection and review of Information Systems logs	9.3	• Added a new requirement for configuring applications, database, system, and network audit logging. The added item reads "Application, Database, System and Network Administrators shall configure information systems to record audit logs that are relevant to the information security monitoring process." • Existing item (ii) was updated to specify frequency of log review to be on monthly basis.
61	Reporting Information Security Issues	9.4	• On item (i), inserted a word "regularly" between the word "shall" and prepare • Added item (ii) to set a requirement for the Head Management Information Systems to report security issues to the ICT Steering Committee. This is to align with existing IT governance structures.

			The added item reads "The Head Management Information System shall submit to ICT Steering Committee a consolidated report on information security issues and challenges for deliberation semi-annually."
62	Managing Information Technology Risks	10.	• New item introduced to address issues for managing IT risks in line with the Corporate Risk Management Framework and Guidelines. • The added section has three items as follows: (i) The Head Management Information Systems shall periodically perform risk assessment on IT systems and related infrastructure in line with the Corporate Risk Management Framework and Guidelines. (ii) Responsible heads of business units shall implement risk mitigation measures within the recommended implementation timelines. (iii) The Head Management Information systems shall maintain Information Technology risk register and status of implementation of mitigation measures that shall annually or on demand be communicated to the Head Risk Management
63	Outsourcing of Information Technology Services	11	• This was section 10 changed due to adding a new section before it
64	Outsourcing Requirements	11.1	• Replaced the word "during" with "for". This is to use an appropriate word • On item (ii), replaced the phrase "take into account" with "consider" • Removed items (ii)(a) and (ii)(b) as they are not directly related to information security • On item (iii), removed the phrase "specification such as business, legal and" as is not directly related to information security
65	Due Diligence	11.2	• Previous section 10.2. • Removed item (i) as it was not directly affecting information security • Item (ii) was amended to read "Where required to conduct due diligence of IT service provider, the Head Procurement Unit, shall consider adequacy of information security controls, business

			continuity and disaster recovery arrangements". *This to ensure security issues are considered during due diligence* • Item (iii) was removed. *This is because the requirement is not directly affecting information security*
66	Risk Management	11.3	• Previous section 10.3. • Title changed to read "Managing Risks of Outsourced IT Services". To focus on risks related to outsourced IT services. • On item (i), the phrase "for Head of Risk Management to decide" was replaced by the phrase "for deciding". This is to align with existing Structures as Decision for outsourcing is made by the EO.
67	Service Level Agreement (SLA)	11.4	• Previous section 10.4.
68	Review and Monitoring of Outsourced IT Services	11.5	• Previous section 10.5. • On item (i), the phrase "by Service Provider" was replaced by the phrase "for respective outsourced IT services". This is to align with existing practice as Internal Auditors usually perform audit of outsourced services. • Removed item (ii). The requirement is contrary to existing practices where the Bank is supposed to implement monitoring mechanisms. The item is also redundant as (iii) requires the Bank to monitor outsourced IT services • Item (iii) was rephrased to read "The Head Management Information System shall regularly review and monitor the outsourced IT services to ensure that Bank expectations are achieved as stipulated in the terms of engagement"
69	Information Systems Acquisition, Development and Maintenance	12.	• A new section introduced to provide guidance on embedding security during Information Systems Acquisition, Development and Maintenance • Added opening paragraph that reads "Security is an essential aspect that needs to be integrated during design and implementation of information systems supporting the business processes. This section outlines guidelines for managing security during information systems acquisition development and maintenance." • Added below subsections: 11.1 Security requirements and testing (i) Business requirements for new information systems, or enhancements to existing information systems shall include requirements for security controls. (ii) Security of new or enhanced systems shall be reviewed and tested prior to those systems

			being deployed into production environment. 11.2 Protection of system files and application source codes (i) Access to system files and application source code should be controlled to avoid their exposure which can result to security breaches. 11.3 Change Management (i) Head of Information Systems Services shall ensure that changes related to information system and processes are performed in line with existing change management procedures. (ii) Change management procedure shall consider risks, impacts and specification of required security controls.
70	Information Systems Change Management	Previous section 11.	• The entire section was removed. The domain of change Management is guided by the ITG framework and the Change Management Procedures documents. This is to maintain a single source of guidance on change management.
71	Protection of Environment with Information System	13.	• Section heading changed to read "protection of environment for data centers and computer Room". *To provide wider context of areas where information systems are deployed* • Open paragraph, 1st sentence was updated by inserting the phrase "deployment of" between "include" and "air". Also added the phrase "fire suppression systems". Replaced the phrase "humidity control" with "humidifier". The change is to provide clarity.
72	Protection of Environment for Computer Rooms	12.1	• *The subsection heading was removed as there is only one subsection under the main section.* • Item (i) was amended to read "Head Estate Management or Finance and Administration shall allocate space suitable for Data center or computer room operations that is protected against natural and artificial hazards." *To provide clarity.* • Item (ii), the word facilities was replaced by Estate and added a requirement for maintaining the areas for both data centers and computer rooms. To align the role to existing Bank structures. • Added item (iii) which assign DMIS a role of authorizing granting of physical access to data

			centers and computer rooms. To align the role to existing Bank structure. The item was relocated to item 4.7 • On item (iii), the word facilities was replaced by Estate. *To align the role to existing Bank structures* • On item (vi), the phrase "with information systems and network equipment" was removed. The phrase was narrowing types equipment available in the data center or computer room. The amended sentence now reads "Head Internal Security shall put in place controls for restricting visitors and third party from accessing data center or computer room premises" The sentence relocated to section 4.7 as it is more relevant under section 4.7 • Item (iv) was added to include a requirement to protect power and data network cables. The item reads "Power and data network cables shall be protected from interception, interference or damage"
73	Protection of Information Technology Equipment Environment	12.2	• The entire section was removed as its content were already covered under section 12.1
74	Information Security Incident Management	13.	• Section changed from 13 to 14. • In the opening paragraph, a new sentence was added to provide more clarity on information security incidents. The added sentence reads "Information security incidents or events may include loss of service equipment or facilities, attack executed via an email message or attachment, non-compliances with policies or guidelines, malfunctions of software or breaches of physical security arrangements."
75	Detection and Analysis of Information Security Incidents	13.1	• Section changed from 13.1 to 14.1 • Section heading was changed to "Detection and Reporting of Information Security Incidents". This is to focus on detection and reporting while aspects of analysis are provided for on another subsection. Also to provide clarity. • Added current item (i) to provide a requirement for IT Security Administrators to participate in detection of information security incident. The added item reads "IT Security Administrators shall use automated security tools such as firewall, antimalware and log monitoring to detect information security incidents" • Existing item (i) was amended to include a phrase "through helpdesk" to indicate that information security incidents will be reported through the helpdesk. This is to align with existing practices.

			• Existing items (ii) to (v) were relocated to a newly introduced subsection 13.2 titled Analysis and Containment of Information Security Incidents
76	Establishment of Computer Incident Response Team (CIRT)	13.2	• Section changed from 13.2 to 14.2 • Section heading changed to "Analysis and Containment of Information Security Incidents". • All existing items (i) to (v) were removed to align with existing practices for handling information security incidents • Current items (i), (iii), (iv) and (v) were relocated to this section from previous section 13.1 • Item (ii) was introduced to enable the Head of Management Information System to form a team to handle incidents on need basis rather than establishing a permanent team. This is to align with existing practices and Bank structure. • Item (iii) was amended to provide for a requirement to quarterly report to the ICT Steering Committee Information security incidents. This to align with recently approved IT Governance Framework
77	Contact with External Authorities	13.3	• Section changed from 13.3 to 14.3 • Added item (iv) on sharing with external entities knowledge related to information security incidents. This to foster collaboration among stakeholders in fighting against attacks to information systems. Added item reads "The Head Management Information Systems shall share appropriate knowledge regarding information security incidents with external institutions in line with existing arrangement"
78	Management of Public Key Infrastructure (PKI)	14	• Section changed from 14 to 15 • On the 2nd sentence of the opening paragraph, added the word "dissemination" to ensure security is also considered during dissemination of cryptographic related information
79	Management of Certificate Authority	14.1	• Section changed from 14.1 to 15.1
80	Protection of Keys	14.2	• Section changed from 14.2 to 15.2 • Removed items (v) and (vi). These items were redundant as they are covered under item 14.3
81	Key Backup, Recovery and Archiving	14.3	• Section changed from 14.3 to 15.3 • Section heading was amended to read "Backup , Recovery and Archiving of Cryptographic Keys"
82	Hardware Token Storage and Protection	14.4	• Section changed from 14.4 to 15.4
83	Protection of Servers or Applications Using Keys	14.5	• Section changed from 14.5 to 15.5 • On item (i) removed the phrase "Secure Socket Layer or" as the protocol is superseded by the Transport Layer Security (TLS).

			• Added a new item to require application administrators to monitor and timely renew certificates before expiry. Application Administrator shall monitor and timely renew digital certificates before expiry • Existing item (iv) was removed as it was redundant already covered by existing items (i) and (v). • On item (v), removed the phrase "SSL or"
84	Compliance and Enforcement	15.	• Section changed from 15 to 16
85	Issuance and Review	16.	• Section changed from 16 to 17 • Amended item (i) to indicate that the document will be approved by the "ICT Steering Committee" instead of the "Management Committee". *This is to align with existing Bank IT Governance Structure.* • Amended item (ii) to specify a review of three years instead of two years. *This is to align with the review period of the policy.* • Amended to indicate that the upon approval the guidelines will be signed by the Chairperson of the ICT Steering Committee instead of the Governor (Chairperson Management Committee). *This is to align with existing Bank IT Governance Structure.*