وزارة الاتصـــــــالات وتكنولوجيـــــــا المعلومـــــــات
Ministry of Communications and Information Technology
State of Qatar • دولـــة قطـــر

Consultation Document

This document is a draft intended for consultation purposes only. It is not the final version and is subject to change based on feedback received during the consultation period.

Minimum Required Internal IT Policies for Government Agencies Policy

Date: March 2025 | Version: 1.0.0 | Ref: P007

DISCLAIMER / LEGAL RIGHTS

The Ministry of Communications and Information Technology (MCIT) has designed and created this publication, entitled Minimum Required Internal IT Policies for Government Agencies Policy, with reference P007 (hereinafter referred to as the “Work”), as a resource primarily for all government agencies, and their senior management, IT management, risk management and IT, and IT security professionals in the State of Qatar.

The “Work” has been prepared in accordance with the laws of the State of Qatar and does not confer, and may not be used, to support any right on behalf of any person or entity against the State of Qatar or its agencies or officials. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Every effort has been made to ensure the “Work” is accurate, but no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the “Work”. Links to other websites are inserted for convenience only and do not constitute a warranty, guarantee or undertaking that these websites are still active and up to date, or an endorsement of any material at those sites, or any associated organization, product or service.

Any reproduction of this “Work”, either in part or full and irrespective of the means of reproduction, shall acknowledge MCIT as the source and owner of the “Work”. Any reproduction concerning the “Work” with intent of commercialization shall seek a written authorization from MCIT. MCIT shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent. The authorization from MCIT shall not be construed as an endorsement of the developed reproduction and such a developer, trademark owner or service provider shall in no way publicize, promote or misinterpret this in any form of media or personal / social discussions.

State of Qatar

Ministry of Communications and Information Technology - Digital Government Affairs Sector

Digital Government Policies and Standards Department

http://www.mcit.gov.qa

e-mail: policy@mcit.gov.qa

Legal Mandate

Article 17[1] of Amiri Decree No. 57 of 2021 sets the mandate and function for the Ministry of Communications and Information Technology (hereinafter referred to as "MCIT") to supervise, regulate, and develop the sector of Information and Communications Technology (hereinafter referred to as "ICT") in the State of Qatar in a manner consistent and aligned with, but not limited to the following:

- Supervising and developing the ICT sector in line with national development needs.
- Supervising the creation of an appropriate regulatory environment for fair competition.
- Supporting, developing, and stimulating the ICT sector and encouraging investment.
- Securing, developing, and raising the efficiency of information and technological infrastructure.
- Raising awareness on the importance of using ICT to advance society, build a knowledge-based digital economy, and improve the life of the individual.
- Implementing and supervising e-Government[2] and Smart Society programs.
- Strengthening government infrastructure and capabilities in the field of ICT.

Furthermore, this policy also draws legal support from the following text:

- Amiri Decision No. 47 of 2022 established the Digital Government Policies and Standards Department and its responsibilities, which include, but are not limited to, developing policies, guidelines, and technical frameworks for digital government affairs; proposing draft related legislative tools; setting standards and technical specifications related to digital government; measuring government agencies' compliance with policies, guidelines, and technical frameworks related to digital government affairs.

[1] Links to all external resources can be found in the Related Legislation and Documents section.

[2] Technical terms and their meaning can be found in the Glossary of Terms and Definitions section.

Strategic Alignment

Qatar National Vision 2030		Economic Development	Build world-class infrastructure with efficient and effective delivery mechanisms for public services and institutions.
Third Qatar National Development Strategy 2024-2030		Government Excellence	Build effective, efficient, and transparent governance.
Digital Agenda 2030	05 Nurtured Digital Technologies	Nurtured Digital Technologies	Refine ICT regulatory landscape.

Document Summary

Name	Minimum Required Internal IT Policies for Government Agencies Policy
Version	1.0.0
Document Reference	P007
Document Type	Policy
Summary	This policy defines a minimum set of internal IT policies that all government agencies must develop and adopt. It ultimately aims to create a similar level of IT policy maturity across agencies to provide a consistent approach to driving good practice and governance. Agencies shall, as deemed necessary, update and / or develop new internal IT policies to meet the minimum standards defined in the provisions and appendices of this policy.
Publishing Date	March 2025
Applicable To	All government agencies in the State of Qatar.
Adoption Period	24 months from policy publication date
Owner	Ministry of Communications and Information Technology (MCIT)

** For any feedback or inquiries please contact policy@mcit.gov.qa.*

Acronyms

BYOD	Bring Your Own Device
IT	Information Technology
MCIT	Ministry of Communications and Information Technology
NCSA	National Cyber Security Agency

Table of Contents

Table of Figures

1 Introduction

The implementation of robust IT policies is essential to fostering a well-functioning and secure IT environment that contributes to the success and maturity of government agencies. Internal IT policies provide a common approach to using best practices, meeting regulatory requirements, and running efficient IT operations in areas such as, but not limited to communication, resources, service levels, security, compliance, risk, and quality. Furthermore, clear internal IT policies can enhance employee productivity by providing transparent guidelines on acceptable technology use and preventing misuse or abuse of IT resources.

The maturity of the internal IT policy environment across different government agencies varies considerably, with some exceeding the basic requirements while others have yet to even identify their IT policy needs. The context, services, and needs of each government agency may vary, but there are common IT Policy areas which can be captured and used as a baseline that all government agencies should have in place.

This policy aims to create a level of consistency across government agencies by driving the creation and adoption of a minimum set of internal IT policies in alignment with the provisions included in this document.

1.1 Minimum Set of Internal IT Policies

After a comprehensive review of best practices, leading nations, and regional peers, the twelve internal IT policies shown in *Figure 1* were identified as being an essential part of a framework for efficient, secure, and compliant use of technology resources. They help protect the organization, its employees, and its stakeholders while promoting a culture of responsible technology use.

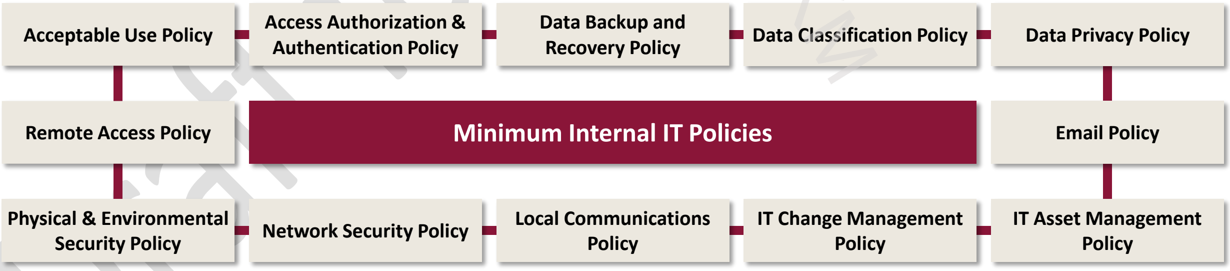
Acceptable Use Policy
Access Authorization & Authentication Policy
Data Backup and Recovery Policy
Data Classification Policy
Data Privacy Policy
Remote Access Policy
Minimum Internal IT Policies
Email Policy
Physical & Environmental Security Policy
Network Security Policy
Local Communications Policy
IT Change Management Policy
IT Asset Management Policy

Figure 1 - Minimum Set of Internal IT Policies

2 Policy Objectives

The key objectives of this policy are to:

2.1 Improve the maturity of the internal IT Policy environment and drive a common approach to the use of good practice within each government agency.

2.2 Define a baseline for a minimum set of internal IT policies required to be created or amended within each government agency.

2.3 Specify the minimum requirements for the scope, definition, and objectives of each internal IT policy.

2.4 Create a more consistent and aligned IT Policy environment across government agencies, to help facilitate government wide initiatives and support future digital transformation efforts.

3 Policy Scope and Application

3.1 Applicable to all government agencies that use IT, or deliver services involving IT systems or devices, internally or for communications over the internet, intranet, private networks, face-to-face or other means.

3.2 Applies to any process, system, computer, website, software, application, and IT device used internally, for any purpose, by and within any of the government agencies referred to in Provision 3.1.

3.3 Applies without prejudice to any stricter requirements by any other laws and policies already in force, including, without limitation, any data protection, physical and cyber security, digital and telecommunications laws and policies, and any stricter internal rules and procedures applied by any of the government agencies concerned, by complementing them as a set of minimum required rules.

4 Policy Provisions

This policy requires all government agencies to apply the following provisions:

4.1 Acceptable Use Policy

4.1.1 Each agency shall establish an Acceptable Use Policy for the appropriate use of computer equipment and other information systems in the course of an agency's daily operations, which defines what constitutes unsuitable internal use of information systems and highlight its potential risks to the agency's network systems, data and other information, assets, duties, functions, as well as to the State and third parties, and the serious legal repercussions associated with such risks.

4.1.2 Each agency's Acceptable Use Policy shall meet the minimum requirements set out in Appendix 1.1.

4.2 Access Authorization and Authentication Policy

4.2.1 Each agency shall establish an Access Authorization and Authentication Policy, with a minimum framework for granting and denying employees, agents and contractors' access to agency IT systems and apps that generate, process, manage, transmit, or retain sensitive data of any kind. In establishing its Access Authorization and Authentication Policy, each agency shall ensure that the Policy safeguards the agency's confidential data against breaches or compromises brought about by improper access and authentication management procedures and shall gather the data required for audit trails linked to compliance.

4.2.2 Each agency's Access Authorization and Authentication Policy shall meet the minimum requirements set out in Appendix 1.2.

4.3 Data Backup and Recovery Policy

4.3.1 Each agency shall establish a Data Backup and Recovery Policy describing minimum data backup processes that should be implemented by the agency to ensure information safety in the case of loss or damage of original data. This policy shall be aligned to the provisions of the National Information Assurance Standards and National Data Classification Policy for specific backup and recovery processes for each class of data (e.g., sensitive, restricted, etc.).

4.3.2 Each agency's Data Backup and Recovery Policy shall meet the minimum requirements set out in Appendix 1.3.

4.4 Data Classification Policy

4.4.1 Each agency shall establish a Data Classification Policy committed to following the data classification approach defined in the National Data Classification Policy and in line with legislations in the State of Qatar, such as the Personal Data Privacy Protection Law and Right to Access Information Law, as well as other relevant national policies and standards.

4.4.2 Each agency's Data Classification Policy shall meet the minimum requirements set out in Appendix 1.4.

4.5 Data Privacy Policy

4.5.1 Each agency shall establish a Data Privacy Policy conforming to the applicable data privacy rules in the State of Qatar and covering various aspects of the agency's processing of data including, but not limited to, their collection, modification, storage, use, exchange, and securing, and listing the data rights of users in that context. In establishing such a Data Privacy Policy, each agency shall refer to the National Data Classification Policy and the Personal Data Privacy Protection Law, and take into consideration their specific privacy requirements for each class of data (e.g., sensitive, restricted, etc.).

4.5.2 Each agency's Data Privacy Policy shall meet the minimum requirements set out in Appendix 1.5.

4.6 Email Policy

4.6.1 Each agency shall establish an Email Policy covering security matters with regard to sending emails internally, within an agency, or to external parties. The policy shall include formal guidelines on the proper usage of official agency email accounts, and information on acceptable personal email usage practices while using work email accounts.

4.6.2 Each agency's Email Policy shall meet the minimum requirements set out in Appendix 1.6.

4.7 IT Asset Management Policy

4.7.1 Each agency shall establish an IT Asset Management Policy, encompassing a robust set of guidelines that meticulously address every facet of the agency's IT asset lifespan, from the initial stages of acquisition and deployment to the ongoing phases of utilization, maintenance, and, critically, the disposal phase of assets at the end of their lifecycle or in case of being stolen or damaged by a third-party before the end of their lifecycle.

4.7.2 Each agency's IT Asset Management Policy shall meet the minimum requirements set out in Appendix 1.7.

4.8 IT Change Management Policy

4.8.1 Each agency shall establish an IT Change Management Policy in order to plan and carry out the temporary shutdown of IT systems for planned maintenance, upgrades, or adjustments. This policy shall outline the minimum standards to be followed, with an emphasis on minimizing disruptions, ensuring smooth transitions, and optimizing system efficiency and reliability throughout the change management process.

4.8.2 Each agency's IT Change Management Policy shall meet the minimum requirements set out in Appendix 1.8.

4.9 Local Communications Policy

4.9.1 Each agency shall establish a Local Communications Policy defining procedures for the agency employees' handling of internal communication via the agency’s network systems, and the ways to exchange information within the agency.

4.9.2 Each agency's Local Communications Policy shall meet the minimum requirements set out in Appendix 1.9.

4.10 Network Security Policy

4.10.1 Each agency shall establish a Network Security Policy defining a process for periodically conducting information system and network activity reviews to ensure the confidentiality, integrity, and availability of data, by equipping the agency's IT systems with the right software, hardware, and auditing procedures.

4.10.2 Each agency's Local Communications Policy shall meet the minimum requirements set out in Appendix 1.10.

4.11 Physical and Environmental Security Policy

4.11.1 Each agency shall establish a Physical and Environmental Security Policy that set forth guidelines and procedures for IT equipment utilization by employees to guarantee that the agency’s information, resources, and premises are safe from harm, damage, or removal. The policy shall also define minimum requirements for a plan to safeguard the agency IT assets through appropriate procedures on how physical access to these assets may be permitted, regulated, monitored or denied.

4.11.2 Each agency's Physical and Environmental Security Policy shall meet the minimum requirements set out in Appendix 1.11.

4.12 Remote Access Policy

4.12.1 Each agency shall establish a Remote Access Policy to reduce the risk of any damage resulting from unapproved usage of the agency's resources by outlining guidelines for access to intranet resources and specifying the prerequisites for disk encryption and VPN access.

4.12.2 Each agency's Remote Access Policy shall meet the minimum requirements set out in Appendix 1.12.

4.13 Implementation Progress and Review

Agency Responsibilities

4.13.1 All government agencies shall put in place, within [24] months from the publication of this Policy, the following twelve (12) internal IT Policies:

- Acceptable Use Policy
- Access Authorization and Authentication Policy
- Data Backup and Recovery Policy
- Data Classification Policy
- Data Privacy Policy
- Email Policy
- IT Asset Management Policy
- IT Change Management Policy
- Local Communications Policy
- Network Security Policy
- Physical and Environmental Security Policy
- Remote Access Policy

4.13.2 Each of these policies shall meet, at a minimum, the set of requirements described under the relevant heading for that policy in Appendix 1.

4.13.3 In putting these policies in place, government agencies may choose between introducing them from scratch (if an equivalent policy is not in place) or adjusting their existing corresponding policies to the extent required to meet the relevant policy's objectives and minimum requirements set out in this document.

4.13.4 The Internal Audit Department of each government agency, or any other relevant party deemed appropriate by the agency, shall monitor implementation of this Policy and the minimum required IT policies that it defines, within the scope of their respective agency.

MCIT Responsibilities

4.13.5 MCIT may issue additional or supplementary procedures, guidelines and best practices from time to time to support one or several of these minimum internal IT policies of government agencies and may extend their scope to other entities.

4.13.6 MCIT shall review these IT policies annually. When necessary, in cases of major technological, regulatory, or organizational changes, MCIT may update one or more of these minimum IT policies before the annual review period.

4.13.7 MCIT may at any time request information and/or a detailed report (please refer to Appendix 3) on the adoption of this Policy and the minimum required IT policies it defines from the Internal Audit Department of each government agency, or any other relevant party deemed appropriate by the agency (please refer to Provision 4.13.4).

5 Glossary of Terms and Definitions

Term	Definition
Data	All data and information in electronic form that government agencies capture, retrieve, share or process for the provision of services to public, visitors and businesses.
Entity	Refers to a government agency including any third parties supporting the government agency in providing services. The context of usage will provide additional meaning.
Government agency	Refers to all ministries and public institutions under ministries or the Council of Ministers in the State of Qatar, unless the context of usage clearly indicates a different meaning.
Personal data	Refers to the data of an individual whose identity is defined or can be reasonably defined, whether through such personal data or through the combination of such data with any other data.

6 Related Legislation and Documents

The following table provides links to all documents and papers related to, or referred to, in this policy. Every effort has been made to ensure these links are valid, but there may be times when some or all of their resources may not be available due to their source having been deleted, moved, or replaced.

Legislation	Amiri Decision No. (57) of 2021 (Article 17) Amiri Decision No. (47) of 2022 Law No. (13) of 2016 on Personal Data Privacy Protection Law No. (9) of 2022 Regulating the Right to Access Information
Policies, Standards, or Frameworks	National Data Classification Policy (2023) National Information Assurance Standard (2023) Cloud First Policy (2024)
Other Links	Qatar National Vision 2030

APPENDICES

Appendix 1: Minimum Requirements per Policy

This Appendix outlines the minimum requirements that government agencies must meet for each internal IT policy mandated by this document. Individual templates for these internal IT policies are provided in Appendix 2 and are available for agency use. Agencies may either develop their own policies or modify the provided templates by adapting, omitting, or adding provisions to address overlaps, gaps, and specific contextual needs to ensure alignment with their own unique requirements.

1.1 Acceptable Use Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements regarding their Acceptable Use Policy:

- Define the Policy's purpose as one aiming to:
  - Safeguard the availability, confidentiality, and integrity of the IT resources owned or used by the agency; and
  - Encourage ethical and responsible use of those resources.
- Outline the scope of the situations to which the policy applies and, to the extent possible (through examples), those to which it does not apply.
- Define Acceptable Use criteria for the agency's IT equipment, such as:
  - Compliance with applicable laws and regulations;
  - Utilization of IT resources only within the scope of daily work; and
  - Respect of the privacy of data by avoiding unauthorized access to the resources.
- Define unacceptable use criteria for the agency's IT equipment, such as:
  - Violation of the rights of users;
  - Illegally copying of material leading to copyright issues; and
  - Providing unauthorized third parties with government information.
- Define criteria for the use of social media by the agency's employees, agents or contractors insofar as these include any reference to the agency or their present or past role within or in relation to the agency.
- Define the consequences of any breach of this policy, depending on their gravity and duration, such as:
  - Administrative fines or other penalties;

  - Termination of the employee’s contract; and
  - Legal action to be taken against the employee concerned.
- Mention any cloud services that shall or may be used within the scope of defined work categories.
- Restrict the installation and utilization of any program that violates government regulations or other laws, such as intellectual property laws.

1.2 Access Authorization and Authentication Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements regarding their Access Authorization and Authentication Policy:

- Define the purpose of this policy as one aiming to put in place procedures to safeguard information and grant access to privileged accounts as well as to equipment, infrastructure, services, and software.
- Outline the scope of the policy as one that includes all agency employees, agents and contractors with access to government information and the agency's IT systems.
- Refer to, and ensure, full alignment with the National Data Classification Policy.
- Establish access controls by allocating them under the "Principle of Least Privilege" and agency needs: Users shall only be granted the minimum of access rights, authorizations, as well as resources to systems, services, data, and information strictly required for them to carry out their designated roles.
- Include procedures to periodically review user access in coordination with business owners and the information security team to identify and eliminate, if any, redundant or inactive accounts, by setting a specific retention period for these accounts as stated in Qatar's Personal Data Privacy Protection Law.
- Establish password management procedures as follows:
    - Require and define password complexity by providing strong password guidelines (e.g., use of both lower-case and upper-case letters, special characters, etc.).
    - Define password length requirements.
    - Inform users about the consequences of choosing an easy term or putting personal information in the password (e.g., easily broken password, potential data breaches).
    - Set password reset periods (e.g., 90 days).
    - Consider multi-factor authentication while setting up a government account on behalf of employees to add an extra layer of security.

1.3 Data Backup and Recovery Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements regarding their Data Backup and Recovery Policy:

- Define the purpose of this policy as one aiming to ensure that all agency data and information will be recoverable in case of any damage or accident.
- Outline the scope of the policy as one including all agency personnel and third parties that interact with agency data and information.
- Refer to and ensure full alignment with the National Data Classification Policy.
- Define the data backup standards for each of the different data levels mentioned in the National Data Classification Policy (i.e., public, internal, restricted, secret and top secret).
- Describe data retention periods for backup (i.e., daily, weekly, etc.).
- Determine a backup schedule including its frequency and time of day for running it.
- Define vendor-agnostic data backup procedures:
    - Identify either manual or automatic backup and the procedures applying to it; and
    - Identify either centralized or decentralized backup and the procedures applying to it.
- Establish an emergency plan to take action in case of any lost data situation.
- Test backup and recovery systems regularly to ensure their functioning.

1.4 Data Classification Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements about their Data Classification Policy:

- Define the purpose of the policy which aims to establish a data classification approach at the agency level in line with that defined in the National Data Classification Policy.
- Outline the scope of the policy which includes all data collected, owned or used by the agency.
- Ensure alignment with the legislations in the State of Qatar, such as the Personal Data Privacy Protection Law and the Right to Access Information Law.
- Define roles and responsibilities within the agency about data classification and how to protect data.
- Outline a step-by-step description of the data categorization process by specifying the responsible in each stage, how data sensitivity is evaluated, and the actions to take if data doesn't fall into a predetermined category.

1.5 Data Privacy Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements regarding their Data Privacy Policy:

- Define the purpose of this policy as one aiming to establish data privacy rights for different data classification levels within the government agency.
- Outline the scope of the policy as one encompassing all data that is processed, stored, updated, or transmitted, in compliance with NCSA's privacy regulations and (for personal data) the Personal Data Privacy Protection Law.
- Refer to the data classification levels defined in the National Data Classification Policy (i.e., public, internal, restricted, secret and top secret) and their respective definitions.
- Establish a role-based access control (RBAC) mechanism defining roles and responsibilities of data owners and users.
- Define data retention procedures for data owners and users.
- Define the data types that will be included to the following classification levels: internal, restricted, secret and top secret.
- Define any personal data types owned or processed by the agency that may qualify as, or include, data of a special nature under Article 16 of the Personal Data Privacy Protection Law and the special procedures that shall apply to them.
- Describe rules to safeguard internal, restricted, secret and top-secret data, as well as the results of noncompliance with these rules.
- Define criteria for the disclosure or use of any agency or other data through social media by the agency's employees, agents or contractors.

1.6 Email Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements regarding their email policy:

- Define the purpose of this policy as the setting of adequate, vendor-agnostic, guidelines for safe and appropriate email use.
- Outline the scope of the policy as one that includes the use of any IT resources, including hardware, software and networks, in use by or in the agency for the purpose of sending or receiving email messages and attachments.
- Clarify the applicability of the policy to BYOD (Bring Your Own Device) and third-party usage.
- Define requirements for acceptable use of agency email, which shall include:
  - The usage of proper professional language and email etiquette;
  - Not sending any sensitive/restricted information to third parties that are not allowed to receive that information; and
  - When sending sensitive/restricted information to third parties that are allowed to receive such information, labelling such information as may be appropriate (e.g., "confidential", "for strict internal purposes", etc.).
- Set limitations for personal use of the agency's email system, in particular by emphasizing that the agency's email system and domain shall be used only in line with the agency's Acceptable Use Policy.
- Include email retention and backup rules in case of forgotten password or lost/stolen IT assets (e.g., computer, phone, laptop, etc.).
- Develop security measures against cyber threats by including regular warnings against phishing.
- Inform all users of the consequences of violating the agency's email policy.

1.7 IT Asset Management Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements with regard to their IT Asset Management Policy:

- Define the purpose of this policy as one aiming to establish clear rules for the proper and efficient management of IT equipment, from purchase to disposal, in the government agency.
- Outline the scope of the policy as one including all IT assets procured by the government agency, comprised of both hardware assets (e.g., laptops, printers, servers) and software assets (e.g., programs, licenses).
- Define the process for the acquisition of any new IT assets (e.g., software, computers, screens, tablets, etc.). Although the process will most likely be agency specific, it must include an approval process by MCIT.
- Provide the set of IT assets that are assigned to specific roles within the agency.
- Define asset maintenance requirements combining the agency's specific and MCIT's general maintenance requirements.
- Encourage minimum/appropriate inventory/stock keeping of the agency's IT assets to keep track of the number of different IT assets, their quantities and useful life.
- Describe specific procedures for the disposal of frequently changing IT assets (e.g., laptops, tablets, etc.) and other IT assets for both:
  - A planned disposal (i.e., end of life cycle of the asset); and
  - An unplanned disposal (i.e., lost/stolen asset).
- Define rules for third-party IT or physical access to the agency's assets and include RACI Matrices defining the role and responsibilities of the parties involved.
- Establish processes for the periodic review of software licenses and the appropriate actions to consider after review in case any license is outdated, including:
  - Renewal process of license for software that are still relevant for the agency's business;
  - Removal process of unused licenses procured under government framework agreements to MCIT; and
  - Negotiation process with vendors for terminating the support services.

1.8 IT Change Management Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements regarding their IT Change Management Policy:

- Define the purpose of this policy as one aiming to minimize disruption and errors during IT service changes within the agency.
- Outline the scope of the policy as one applying to all of the agency's employees, agents and contractors working on operational and project-based IT system upgrades, patches, or modifications related to the agency.
- Document all basic setups for current information systems, including component configurations, and ensure protection of the Change Management Database.
- Establish a mechanism or tool that must be used to initiate modifications or change requests.
- Establish and define the roles and responsibilities of a Change Advisory Board responsible for change management within the agency, which shall include:
    - Assessing and approving change requests;
    - Prioritizing change requests based on their impact and criticality; and
    - Communicating the changes with relevant stakeholders within the agency.
- Define possible rejection criteria for change requests.
- Define different types of changes and the respective procedures to be followed for each of them, such as standard change, emergency change, etc.

1.9 Local Communications Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements regarding their Local Communications Policy:

- Define the policy's purpose as the utilization of various communication channels within the agency as well as the roles and responsibilities of employees in having access to them.
- Outline the scope of the policy which covers all agency personnel communicating with each other through agency's communication channels and IT equipment.
- Refer to and ensure full alignment with the National Data Classification Policy.
- List all different internal communication channels of the agency.
- Provide principles and procedures of communicating through the listed communication channels including business as usual and during emergency/crisis situations.

1.10 Network Security Policy – Minimum Requirements

Government agencies shall fulfil the following minimum requirements regarding their Network Security Policy:

- Define the purpose of this policy as the protection of the entire government agency network's security (including cloud networks used) by ensuring confidentiality, integrity and availability.
- Outline the scope of the policy as one applying to the entire network of the government entity but also to all its employees, agents, contractors and third parties that interact with or within this network.
- Refer to and ensure full alignment with the National Data Classification Policy and Cloud First Policy.
- Protect the physical and environmental security of the network.
- Define processes for the following periodical activities on securing information systems:
  - Audit events such as failed attempts at logging in, information opening or closing, and the use of privileged accounts; and
  - Log and record events (with the date, time and place of origin) such as anomalies in the firewalls, activity on the routers and switches, and newly added or deleted devices from the network.
- Define specific network requirements for:
  - Router and switch security;
  - Wireless connection;
  - Virtual Private Network (VPN); and
  - Firewall security.
- Set data backup and restoration protocols.

1.11 Physical and Environmental Security Policy – Minimum Requirements

Government entities shall fulfil the following minimum requirements regarding their Physical and Environmental Security Policy:

- Define the purpose of this policy as one aiming to safeguard information assets and systems from illegal access and to defend them against environmental risks, by enforcing physical and environmental restrictions.
- Outline the scope of the policy as one applying to all employees of the entity, its entities and contractors (such as consultants visiting the entity) and any other person with access to any physical IT equipment of the entity.
- Define all the IT equipment owned or otherwise used by the entity, both within and outside its premises.
- Establish specific security measures for all defined IT equipment.
- Elaborate access rights to IT equipment, based on job requirements and the employee's level of security clearance.
- Elaborate access rights to IT equipment for external and temporary staff as well as maintenance responsible with access to the sites.
- Define the necessary physical requirements, environmental conditions and access controls to secure and protect the agency server rooms.

1.12 Remote Access Policy – Minimum Requirements

Government entities shall fulfil the following minimum requirements about their Remote Access Policy:

- Define the purpose of the policy as the laying down of guidelines and conditions for connecting from any host (i.e., laptops, tablets, and mobile phones) to the government entity network.
- Outline the scope of the policy applicable to all staff members, agents and contractors who use government agency equipment, but also remotely access, deploy, and administer governmental information and information systems.
- Define device types eligible for remote access (e.g., tablets, computers), differentiating between BYOD and third-party scenarios as well.
- Indicate agency IT systems that will allow for remote access.
- Set protocols to protect sensitive information while accessing remotely.
- Mention that remote access shall be allowed only when necessary, and shall be quickly withdrawn when no longer needed, also including the withdrawal of all data retained for the purpose of this remote access.
- Recognize that access via a Virtual Private Network (VPN) shall proceed with an appropriate multi-factor authentication mechanism, and that multiple attempts shall generate alerts.

Appendix 2: Policy Templates

This Appendix outlines the policy templates for each internal IT policy mandated by this document, to support government agencies in developing each of them for their organization.

The specific templates for each internal IT policy are provided in the following sub-sections. Agencies may adapt these sections or incorporate additional ones to address their unique needs and requirements related to their internal IT policies.

2.1 Acceptable Use Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Acceptable Use Policy defines appropriate usage of information technology resources within government agencies. It is designed to ensure that all employees, contractors, and affiliates use these resources in a manner that is ethical, lawful, and supportive of the agency's mission. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Safeguard the availability, confidentiality, and integrity of the IT resources owned or used by [agency name],*
- *Encourage ethical and responsible use of such IT resources,*
- *[…]*

Policy Scope and Application

The scope of this policy is all IT equipment owned and/or used by [agency name], as well as the situations where such equipment is used.

Policy Provisions

The acceptable use criteria for the [agency name]'s IT equipment within the scope of this policy is defined as follows:

- *All IT equipment and relevant processes using such equipment shall be compliant with applicable laws and regulations within the State of Qatar [, which includes but is not limited to law/regulation name, law/regulation name, …].*
- *All IT equipment and relevant processes using such equipment shall be utilized only within the scope of [agency name]'s daily work as per their job description. As such, no [agency name] personnel shall use such equipment and resources for personal matters.*
- *All IT equipment and relevant processes using such equipment shall respect the privacy aspect of the data being used by the relevant IT resources by prohibiting unauthorized access.*
- *[…]*

The unacceptable use criteria for the [agency name]'s IT equipment within the scope of this policy is defined as follows:

- *It is prohibited to install and utilize any IT resource that violates government regulations or other laws, such as intellectual property laws.*
- *No IT resource shall violate the rights of service beneficiaries, in accordance with the laws and regulations in the State of Qatar [, which includes but is not limited to law/regulation name, law/regulation name, …].*
- *Unauthorized access to government information by third parties shall be prohibited, and authorization should be given to relevant parties as defined in the [title of agency's Access Authorization and Authentication Policy].*
- *Copying materials that may lead to copyright issues shall be prohibited.*
- *[…]*

The criteria for the use of social media by [agency name] and relevant stakeholders is defined as follows:

- *Criteria for [agency name] employees:*
  - *[…]*
- *Criteria for third parties contracted by [agency name]:*
  - *[…]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*

- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

2.2 Access Authorization and Authentication Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Access Authorization and Authentication Policy defines measures to protect the [agency name]'s proprietary information from breaches or compromises caused by inappropriate access and authentication management practices. It is designed to ensure that all employees, agents and contractors only have access to the [agency name] services, data, and information that are strictly required for them to carry out their designated roles. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Put in place procedures to safeguard information and grant access to privileged accounts as well as to equipment, infrastructure, services, and software.*
- *[…]*

Policy Scope and Application

The scope of this policy is all [agency name] employees, agents and contractors with access to government information and the [agency name]'s IT systems.

Policy Provisions

The access controls are defined as follows within the scope of this policy:

- *Access rights, authorizations, and resource allocations shall be governed by the Principle of Least Privilege.*
- *Users will be granted the minimum necessary access to systems, services, data, and information strictly required for the performance of their designated roles.*

The procedures below to periodically review user access in coordination with business owners and the information security team are consistent with Qatar's relevant laws and regulations which include but are not limited to Personal Data Privacy Protection Law [, law/regulation name, law/regulation name…]:

- *Identify and eliminate redundant accounts once the retention period of XXX days is over.*

- *Identify and eliminate inactive accounts once the retention period of XXX days is over.*
- *[…]*

The password management procedures regarding access to [agency name] accounts are defined as follows within the scope of this policy:

- *The password should include at least one of the following:*
  - *Lower-case letter*
  - *Upper-case letter*
  - *Special character*
  - *Number*
  - *[…]*
- *The password length should be between XXX and XXX characters.*
- *The password should be renewed once every XXX days.*
- *The password should not be similar to the previous XXX number of passwords used.*
- *[…]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

2.3 Data Backup and Recovery Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Data Backup and Recovery Policy defines the minimum required data backup procedures that should be adopted by the [agency name]. It is designed to ensure information security in the event of loss or damage to original [agency name] data. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Ensure that all [agency name] data and information will be recoverable in case of any damage or accident,*
- *[…]*

Policy Scope and Application

The scope of this policy is all [agency name] employees and third parties that have access to [agency name] data and information.

Policy Provisions

All data backup standards within the [agency name] must comply with the classification levels outlined in the National Data Classification Policy, including Public Data (C0), Internal Data (C1), Restricted Data (C2), Secret Data (C3) and Top-Secret Data (C4).

The emergency response plan to be activated during incidents interrupting data shall include the following within the scope of this policy:

- *An escalation matrix to ease communication during emergencies:*
  - *[…]*
- *Contingency measures:*
  - *[…]*

- *Recovery options:*
  - *[…]*
- *[…]*

Periodic data backups are defined based on their classification levels within the following data backup frequencies within the scope of this policy:

- *Daily backups.*
- *Weekly backups.*
- *Monthly backups.*
- *[…]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State* of Qatar.

Related Documents / References

- *[…]*

2.4 Data Classification Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Data Classification Policy defines the data classification methodology outlined in the National Data Classification Policy and how it is applied in the [agency name]. It is designed to ensure full compatibility with Qatar's relevant laws and regulations [including law/regulation name, law/regulation name, …] […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Establish a data classification approach at the [agency name] level in line with that defined in the National Data Classification Policy.*
- *[…]*

Policy Scope and Application

The scope of this policy is all data collected, owned or used by the [agency name].

Policy Provisions

All data classification and protection procedures within the [agency name] must comply with the applicable laws and regulations of the State of Qatar, including but not limited to:

- *National Data Classification Policy*
- *Right to Access Information Law*
- *Personal Data Privacy Protection Law*
- *[…]*

The [agency name] should at least have defined clear responsibilities for the following roles within the scope of this policy:

- *Data owners are in charge of classifying data based on their sensitivity and ensuring that proper safeguards are in place.*

- *The information security team provides supervision, creates classification rules, and ensures legal and regulatory compliance.*
- *Business owners should work with data owners and custodians to match data classification with operational requirements and regulatory demands.*

The data classification process is defined as follows within the scope of this policy:

- *Check sensitivity of government data and information by the responsible personnel.*
- *Checked data and information is classified by the responsible personnel In line with National Data Classification Policy as Public Data (C0), Internal Data (C1), Restricted Data (C2), Secret Data (C3) or Top-Secret Data (C4).*
- *Periodic review of the data classes by the responsible personnel.*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

2.5 Data Privacy Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Data Privacy Policy defines applicable data privacy rules in the State of Qatar. It is designed to ensure full compatibility with the specific privacy requirements for each data category including sensitive data, restricted data, […] outlined in the National Data Classification Policy and the Personal Data Privacy Protection Law. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Establish data privacy rights for different data classification levels within the [agency name],*
- *[…]*

Policy Scope and Application

The scope of this policy is all data processed, stored, updated, or transmitted by the [agency name].

Policy Provisions

All data privacy standards within the [agency name] must comply with the classification levels outlined in the National Data Classification Policy, including Public Data (C0), Internal Data (C1), Restricted Data (C2), Secret Data (C3) and Top-Secret Data (C4).

The criteria for the disclosure or use of any [agency name] or other data through social media or any other communications channel by the [agency name]'s employees, agents or contractors are defined as follows:

- *Criteria for [agency name] employees:*
  - *[…]*
- *Criteria for third parties contracted by [agency name]:*
  - *[…]*

The [agency name]'s Role-Based Access Control (RBAC) mechanism establishing the roles and responsibilities of different stakeholders handling [agency name] data is defined as follows in the scope of this policy:

- *The data owners hold responsibility for:*
  - *Defining access rights and approval processes for the data they control.*
  - *Ensuring periodic reviews to update user access rights, if necessary.*
  - *[…]*
- *Users (i.e., [agency name]'s employees, agents or contractors) are allowed access based on the scope of their day-to-day business activities within the [agency name] and they are responsible for:*
  - *Using data and resources only in the context of their allocated tasks.*
  - *Adhering to data privacy and protection requirements.*
  - *[…]*
- *[…]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

2.6 Email Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Email Policy defines guidelines on the appropriate use of personal email conduct with regard to [agency name] email accounts, as well as standards for the correct use of official [agency name] email accounts. It is designed to ensure that all mails sent by [agency name] employees containing information about [agency name]'s business, comply with the security, confidentiality and privacy standards of the [agency name]. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Set adequate, vendor-agnostic, guidelines for safe and appropriate email use,*
- *[…]*

Policy Scope and Application

The scope of this policy is all [agency name] employees making use of any IT resources, including hardware, software and networks, for the purpose of sending or receiving email messages and attachments.

Policy Provisions

The acceptable use criteria for all mails sent by [agency name] employees are defined as follows within the scope of this policy:

- *Employees must follow the [agency name]'s email etiquette guidelines and use appropriate language in all email correspondence in order to maintain professionalism.*
- *The [agency name]'s email system and domain must be used only for official purposes, in accordance with the agency's Acceptable Use Policy.*
- *Sensitive or restricted information must be properly labeled (e.g., confidential) when shared with approved recipients so as to ensure appropriate handling.*
- *[…]*

The unacceptable use criteria for all mails sent by [agency name] employees are defined as follows within the scope of this policy:

- *It is prohibited to use the [agency name]'s email system for personal matters.*
- *Sending private or restricted information to unauthorized individuals is strictly prohibited for employees.*
- *Disciplinary actions for breaking this policy include, but is not limited to, losing access rights, official warnings and, in serious cases, possible legal repercussions.*
- *[…]*

The cybersecurity awareness increasing activities of the [agency name] include, but are not limited to:

- *Every employee is required to take an annual cybersecurity awareness training, which include the following topics prepared by the [agency name]:*
    - *Recognizing phishing emails and fraudulent websites.*
    - *Secure procedures for managing private data.*
    - *Being aware of the risks of attacks using social engineering.*
- *The [agency name] will periodically evaluate staff preparedness through simulated phishing tests. Employees will need to receive more training if they are unable to identify simulated phishing attempts.*
- *[…]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

2.7 IT Asset Management Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This IT Asset Management Policy defines a comprehensive set of rules for the efficient management of the [agency name]'s IT equipment. It is designed to ensure that every phase of the [agency name]'s IT hardware or software asset lifecycle is addressed, from the procurement and implementation to the utilization, maintenance and, ultimately, the disposal phase. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Establish clear rules for the proper and efficient management of IT equipment, from purchase to disposal, in the [agency name],*
- *[…]*

Policy Scope and Application

The scope of this policy is all IT assets procured or owned by the [agency name], including hardware and software assets.

Policy Provisions

The procedure for the acquisition of any new IT assets is defined as follows within the scope of this policy:

- *[Agency name] teams to determine the need for new IT assets based on operational requirements, technical improvements, or replacement schedules.*
- *[Agency name] to implement a plan specifying the assignment of specific IT assets based on job roles:*
  - *Executives can be assigned the following IT assets:*
    - *[…]*
  - *Administration staff can be assigned the following IT assets:*
    - *[…]*

  - *[…] can be assigned the following IT assets:*
    - *[…]*
- *All asset acquisitions must go through an approval procedure, which includes:*
  - *[Agency name] approval by appropriate department heads.*
  - *MCIT approval.*
- *For vendor selection, follow the procurement standards, taking into account approved vendors and MCIT-established framework agreements.*
- *[…]*

Asset maintenance integrating the [agency name]'s unique requirements with general maintenance good practice are defined as follows within the scope of this policy:

- *Requirements for preventive maintenance for [agency name] assets are:*
  - *[…]*
- *Requirements for corrective maintenance for [agency name] assets are:*
  - *[…]*
- *Requirements for third-party assets maintenance:*
  - *[…]*

Procedures for disposing IT assets are defined as follows within the scope of this policy:

- *Requirements for planned disposal of [agency name]'s IT assets at the end of their lifecycle are:*
  - *[…]*
- *Requirements for unplanned disposal of [agency name]'s IT assets (lost or stolen) are:*
  - *[…]*

Rules for third-party IT or physical access to the [agency name]'s IT assets are defined as follows within the scope of this policy:

- *Only authorized third parties may access IT assets or physical sites after a thorough verification procedure.*
- *All third-party access activity should be monitored and logged.*
- *Responsibility Assignment Matrices (RACI) should be designed for all third parties accessing the [agency name]'s IT assets.*
  - *The Responsible personnel for this third-party access is XXX.*
  - *The Accountable personnel for this third-party access is XXX.*

- *The Consulted personnel for this third-party access is XXX.*
- *The Informed personnel for this third-party access is XXX.*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

2.8 IT Change Management Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This IT Change Management Policy defines procedures for temporarily shutting down IT systems during planned maintenance, upgrades, or changes. It is designed to ensure minimal interruption and errors during IT service improvement activities within the [agency name]. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Minimize disruption and errors during IT service changes within the [agency name].*
- *[…]*

Policy Scope and Application

The scope of this policy is all [agency name] employees, agents and contractors working on operational and project-based IT system upgrades, patches, or modifications related to the agency.

Policy Provisions

The Change Management Database (CMDB) should be maintained live for recording and tracking settings and changes by ensuring that the database is secured from unauthorized access and alterations by using suitable security measures.

The Change Advisory Board is responsible for leading the change management process within the [agency name], which consists of the following phases within the scope of this policy:

- *[Agency name] teams to apply to the Change Advisory Board for a change request regarding any IT asset that needs to be renewed within their respective team.*
- *Change Advisory Board to assess, approve and prioritize change requests based on their impact and criticality.*
- *Change Advisory Board to communicate the changes with relevant stakeholders within the [agency name].*

- *[…]*

The rejection criteria for the IT change management requests within the scope of this policy are defined as follows:

- *The request is exceeding or using the majority of the [agency name] budget for IT equipment.*
- *The request does not match up with the overall strategy of the [agency name].*
- *The request is declined by MCIT.*
- *[…]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

2.9 Local Communications Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Local Communications Policy defines procedures for [agency name] employees to handle internal communication via the [agency name]'s network systems, as well as methods for exchanging information inside the agency. It is designed to ensure full alignment with the principles outlined in the National Data Classification Policy. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Define various communication channels utilized within the [agency name] as well as the roles and responsibilities of employees in having access to them.*
- *[…]*

Policy Scope and Application

The scope of this policy is all [agency name] employees communicating with each other through [agency name]'s communication channels and IT equipment.

Policy Provisions

All local communications procedures within the [agency name] must comply with the applicable laws and regulations of the State of Qatar, [including law/regulation name, law/regulation name, …].

The local communications channels handled within the scope of this policy are defined as follows:

- *[Agency name]'s email platform and collaboration workspaces.*
- *[Agency name]'s intranet portal.*
- *[Agency name]'s phones.*
- *Official text messaging tools used by the [agency name].*
- *[…]*

Principles and procedures of communicating through the listed communication channels within the scope of this policy are defined as follows:

- *All communications must be precise, short, and polite, with professional language appropriate for the [agency name]'s principles.*
- *Employees should select the most appropriate communication channel for the type and urgency of the message to be delivered.*
- *Sensitive material should only be exchanged through secure methods (such as encrypted emails), with access limited to authorized individuals.*
- *[...]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[...]*

2.10 Network Security Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Network Security Policy defines the procedure for performing regular monitoring activities for the [agency name]'s IT systems and network. It is designed to ensure data security, integrity, and availability by equipping the [agency name]'s IT systems and network with appropriate software, hardware, and auditing methods. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is the:

- *Protection of the entire [agency name] network's security (including cloud networks used) by ensuring confidentiality, integrity and availability.*
- *[…]*

Policy Scope and Application

The scope of this policy is all the [agency name] employees, agents, contractors and third parties that interact with or within the government network.

Policy Provisions

All network security procedures within the [agency name] must comply with the applicable laws and regulations of the State of Qatar, [including law/regulation name, law/regulation name, …].

The physical and environmental security rules within the [agency name] include but are not limited to:

- *Physical access to network equipment should be restricted using secure mechanisms (e.g., monitored access logs).*
- *Environmental controls should be in place to ensure that network rooms have the right temperature and humidity avoiding equipment failure.*
- *[…]*

The network security requirements within the [agency name] are defined as follows:

- *Security requirements for router and switch security:*
    - *[…]*
- *Security requirements for wireless connection:*
    - *[…]*
- *Security requirements for Virtual Private Network (VPN):*
    - *[…]*
- *Security requirements for the firewall security:*
    - *[…]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

2.11 Physical and Environmental Security Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Physical and Environmental Security Policy defines procedures to be followed by the [agency name] employees while using [agency name] IT equipment. It is designed to ensure full protection of the [agency name]'s information, resources, and premises against potential damages, destruction, or removal. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Safeguard information assets and systems of the [agency name] from illegal access and to defend them against environmental risks, by enforcing physical and environmental restrictions.*
- *[…]*

Policy Scope and Application

The scope of this policy is all [agency name] employees, contractors and any other person with access to any physical IT equipment of the entity.

Policy Provisions

IT equipment categories used for [agency name] business, whether located within or outside agency premises, are defined as follows within the scope of this policy:

- *Computing systems such as:*
  - *PCs*
  - *Screens*
  - *Laptops*
  - *[…]*

- *Gateway infrastructure such as:*
  - *Firewalls*
  - *Routers*
  - *Switches*
  - *[…]*
- *[…]*

Specific security measures for all [agency name] IT equipment are defined as follows within the scope of this policy:

- *Specific security measures for computing systems include:*
  - *[…]*
- *Specific security measures for the gateway infrastructure include:*
  - *[…]*
- *[…]*

Specific access rights to IT equipment for external and temporary staff as well as maintenance responsible with access to the [agency name] premises, based on job requirements and the employee's level of security clearance equipment are defined as follows within the scope of this policy:

- *Specific access rights to IT equipment for computing systems include:*
  - *[…]*
- *Specific access rights to IT equipment for the gateway infrastructure include:*
  - *[…]*
- *[…]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

2.12 Remote Access Policy

Policy Title:	*[…]*	**Policy Version:**	*[…1.0 …]*
Issue Date:	*[…]*	**Revision Date:**	*[…]*
Policy Owner / Department:	*[…]*	**Author Name:**	*[…]*

Introduction

This Remote Access Policy defines procedures for accessing [agency name]'s intranet resources as well as requirements for accessing remotely [agency name]'s systems, including disk encryption, VPN access, […]. It is designed to ensure that the potential damages that might be caused by unapproved use of the [agency name]'s resources are minimized. […]

Definitions

- *[…]*

Policy Purpose / Objectives

The purpose of this policy is to:

- *Lay down guidelines and conditions for connecting from any host (i.e., laptops, tablets, and mobile phones) to the [agency name] network,*
- *[…]*

Policy Scope and Application

The scope of this policy is all [agency name] employees, agents and contractors who use [agency name] equipment, but also remotely access, deploy, and administer governmental information and information systems.

Policy Provisions

The accepted devices for remote access within the scope of this policy are defined as follows:

- *[Agency name]-owned devices include laptops, screens, and tablets issued by the [agency name].*
- *Personal devices approved by the [agency name] for remote access and fulfilling security standards as well as provisions defined in the BYOD Policy[3].*
- *Devices owned by agents or contractors and only accessible under certain conditions and with tight security measures.*

[3] https://qcert.ncsa.gov.qa/sites/default/files/public/documents/cs-csps_byod_policy_v1.1.pdf

- *[…]*

The accepted IT systems for remote access within the scope of this policy are defined as follows:

- *[Agency name]'s email platform and collaboration workspaces.*
- *Certain internal apps determined by role and necessity.*
- *File storage and document repositories access to be granted by the data owner.*
- *[…]*

The VPN utilization requirements within the scope of this policy are defined as follows:

- *Remote access must be made using the [agency name]'s certified VPN.*
- *VPN access requires multi-factor authentication (MFA).*
- *[…]*

Compliance Requirements

- *All parties to which this policy applies shall ensure they are fully compliant with the provisions of this policy.*
- *[Agency name] may conduct regular compliance checks to monitor implementation and compliance with this policy.*
- *If [agency name] identifies noncompliant activities by relevant stakeholders, depending on the gravity and duration of the compliance breach, it may issue administrative penalties, terminate employment / work agreements, and take legal action as per the governing laws and regulations within the State of Qatar.*

Related Documents / References

- *[…]*

Appendix 3: Policy Adoption Reports

This section provides example information that may be requested by MCIT to determine if appropriate actions have been taken to adopt this policy. The information requested will include, but not be limited to, the following:

Minimum Required Internal IT Policies for Government Agencies Checklist	*Response*
Acceptable Use Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is "yes" for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is "no" for the previous question, please list the missing requirements: • XXX	
Access Authorization and Authentication Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is "yes" for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is "no" for the previous question, please list the missing requirements: • XXX	
Data Backup and Recovery Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is "yes" for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is "no" for the previous question, please list the missing requirements: • XXX	

Minimum Required Internal IT Policies for Government Agencies Checklist	*Response*
Data Classification Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is "yes" for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is "no" for the previous question, please list the missing requirements: • XXX	
Data Privacy Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is "yes" for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is "no" for the previous question, please list the missing requirements: • XXX	
Email Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is "yes" for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is "no" for the previous question, please list the missing requirements: • XXX	
IT Asset Management Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No

Minimum Required Internal IT Policies for Government Agencies Checklist	*Response*
If the answer is “yes” for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is “no” for the previous question, please list the missing requirements: • XXX	
IT Change Management Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is “yes” for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☒ No ☐ N/A
If the answer is “no” for the previous question, please list the missing requirements: • XXX	
Local Communications Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is “yes” for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is “no” for the previous question, please list the missing requirements: • XXX	
Network Security Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is “yes” for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is “no” for the previous question, please list the missing requirements: • XXX	

Minimum Required Internal IT Policies for Government Agencies Checklist	*Response*
Physical and Environmental Security Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is "yes" for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is "no" for the previous question, please list the missing requirements: • XXX	
Remote Access Policy	
Has the agency adopted such a policy?	☐ Yes ☐ No
If the answer is "yes" for the previous question, does the concerned policy meet the minimum requirements defined in Appendix 1 of this policy?	☐ Yes ☐ No ☐ N/A
If the answer is "no" for the previous question, please list the missing requirements: • XXX	

Document Control

Version	Date	Amendments	Author
1.0.0	01/03/2025	Release of policy.	MCIT

Consultation Document

Prepared by
Digital Government Policies & Standards Department
Ministry of Communications and
Information Technology
Version 1.0.0 2025

e-Mail: policy@mcit.gov.qa
www.mcit.gov.qa