This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Asset Acceptable Use Policy Template

Choose Classification

DATE:	Click here to add date
VERSION:	Click here to add text
REF:	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated by	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This policy aims to define the requirements related to acceptable use in <organization name> in order to minimize the cybersecurity risks resulting from internal and external threats to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy applies to all information and technology assets in the <organization name> and applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1- General Requirements

1-1 Cybersecurity requirements must be followed in the policies, standards, and procedures approved by <organization name>.

1-2 Data and assets (hardware, information, or software) must be protected and handled as per their sensitivity and classification in accordance with the Data Protection Policy approved by <organization name>. Also, data confidentiality, integrity and availability must be ensured.

1-3 No printed matters should be left unattended on the shared printer.

1-4 External storage media must be kept in a secure and appropriate manner, such as ensuring that the temperature is set at a certain degree and stored in an insulated and safe place.

1-5 It is prohibited to disclose any of the <organization name> information, including systems and networks related information, to any unauthorized entity or party, whether internal or external.

1-6 It is prohibited to publish information about the <organization name> via the media and social media networks without permission of the Authorizing Official.

1-7 It is prohibited to use the <organization name> systems and assets to achieve personal benefit and business, or for any purpose not related to the activity and works of <organization name>.

1-8 It is prohibited to connect personal devices to networks and systems of <organization name> without prior authorization from the <cybersecurity function>. This should be done in accordance with Workstations, Mobile Devices and BYOD Security Policy approved by <organization name>.

1-9 It is prohibited to perform any activities intended to bypass the <organization name> protection systems, including anti-virus programs, firewall, and malware without prior authorization, and in accordance with the procedures approved by <organization name>.

1-10 The <cybersecurity function> retains its right to monitor and periodically review work-related systems, networks and personal devices, in order to monitor compliance with cybersecurity policies and standards approved by <organization name>.

1-11 The identification card of employee or visitors must visible in all facilities of <organization name>.

1-12 The <cybersecurity function> must be notified in case of loss, theft or leakage of <organization name> information.

1-13 Information and Asset Acceptable Use rules related to Information Processing systems must be followed up.

1-14 All <organization name> employees and staff must return all files, documents, information and assets in their possession upon work completion or expiry of their contract/agreement.

1-15 It is prohibited to transfer assets off-site without prior permission from relevant departments.

1-16 Assets that are off-site must be protected taking into account the various risks of working outside <organization name> buildings.

1-17 Sessions, meetings and contents related to security awareness campaigns organized by the <organization name> must be attended and should be abided by.

1-18 All staff must sign a statement of consent on Asset Acceptable Use approved by <organization name>.

1-19 All staff must approve and acknowledge the Code of Conduct and Acceptable Use Policy upon any review or update thereof.

1-20 Access to <organization name> assets must be according to roles and responsibilities required to perform tasks only.

1-21 Technical asset administrators must be alerted about cybersecurity patches to be implemented according to <organization name> Patch Management Policy.

1-22 Asset owners must review user access rights at defined and regular intervals.

1-23 The <cybersecurity function> must be notified when suspecting any activity that may harm <organization name> or its assets, such as suspected sites, cybersecurity risks or mail contents that may harm <organization name>.

1-24 In case of non-compliance with any item, <organization name> must explain and state the reasons.

1-25 Key performance indicators (KPIs) must be used to ensure correct and effective use of requirements and protect <organization name> information and technology assets.

2- Protection of Laptops

2-1 It is prohibited to use external storage media without prior authorization from <cybersecurity function>. When used, stored data must be encrypted according to <organization name> Encryption Standard.

2-2 Devices must be secured before leaving office by Sign out or Lock, whether leaving for a short time or after working hours.

2-3 It is prohibited to use or install hardware, tools, or applications unapproved by <organization name> on the laptop without prior authorization of <IT function>.

3- Internet and Software Acceptable Use

3-1 Security messages that may arise while browsing the internet or internal networks must be treated cautiously and be dealt with only after contacting <cybersecurity function>.

3-2 It is prohibited to violate the rights of any person, or company protected by copyright, patent or other intellectual property, similar laws or regulations, including, but not limited to, installation of unauthorized or illegal software for any business purposes, or use of external storage media without consent of <organization name>.

3-3 A secure and authorized browser must be used to access internal network or internet.

3-4 It is prohibited to use techniques that allow bypassing Proxy or Firewall to access Internet.

3-5 It is prohibited to upload or install Software and tools on <organization name> assets without prior authorization of <cybersecurity function>.

3-6 It is prohibited to use Internet for non-business purposes, including uploading media and files, as well as using file sharing software without prior authorization of <cybersecurity function>.

3-7 It is prohibited to conduct a security check to discover security vulnerabilities, including penetration testing, or monitoring <organization name> networks and systems, or third-party networks and systems without prior authorization of <cybersecurity function>.

4- Email Acceptable Use

4-1 It is prohibited to use email, telephone or e-fax for non-business purposes, noting that their use shall only be in accordance with cybersecurity policies and standards approved by <organization name>.

4-2 It is prohibited to exchange messages containing inappropriate or unacceptable content, including messages with internal and external parties.

4-3 Encryption techniques must be used when sending sensitive information via email or communication systems as per the <organization name> Data Protection Policy.

4-4 <Organization name> email address should not be registered at any site not related to work.

4-5 <Organization name> has the right to disclose emails' content after obtaining the necessary permits from the Representative and the <cybersecurity function> in accordance with the <organization name>'s relevant approved procedures and regulations.

4-6 It is prohibited to open suspicious or unexpected emails and attachments, even if they appear to be from reliable sources.

5- Video Conferences and Web-based Communications

5-1 It is prohibited to use unauthorized tools or software to make calls or hold video conferences related to work.

5-2 It is prohibited to make calls or hold video conferences not related to work without prior authorization to use <organization name>’s tools or software.

5-3 It is prohibited to hold meetings related to work in public places due to risk of leaking classified information.

6- Passwords Use

6-1 It is necessary to choose secure passwords and to safeguard <organization name> systems and assets passwords in accordance with <organization name> Identity and Access Management Policy. It is also necessary to choose passwords different from those of personal accounts, such as personal mail and social media accounts.

6-2 It is prohibited to share the password by any means, including electronic correspondence, voice calls, and paper writing. Users must not disclose passwords to any other party, including co-workers and employees of <IT function> and immediately notify <cybersecurity function> immediately if this occurs.

6-3 Passwords must be changed on a regular basis according to Password Policy requirements or upon obtaining a new password from the system administrator.

6-4 It is prohibited to use previously used or common passwords. It is also prohibited to share user's password with anyone.

7- Office Use

7-1 It is necessary to abide by <organization name>'s Secure and Clean Office Policy, and to make sure the desktop and screen are free of classified and sensitive information as per <organization name>'s approved classifications.

7-2 It is prohibited to leave any <organization name> classified or sensitive information in places that are easily accessible, or accessed by unauthorized persons.

7-3 It is prohibited to leave office doors and cabinets containing classified and sensitive information open.

8- Cloud Computing

8-1 Data must be classified prior to being hosted with cloud computing and hosting service providers, and returned to the organization (in a usable format) upon service completion.

8-2 <Organization name> environment (especially virtual servers) must be separated from other cloud computing environment of other organizations.

8-3 Location for hosting and storing <organization name> information must be inside the Kingdom and storing must be in accordance with the relevant legal and regulatory requirements.

8-4 Cybersecurity requirements for protection of cloud computing subscribers' data and information must be covered in accordance with the relevant legal and regulatory requirements, as a minimum:

8-5-1 Guarantees for ability to delete data safely upon expiry of relationship with service provider (Exit Strategy).

8-5-2 Use secure means to export and transfer data and virtual infrastructure.

Roles and Responsibilities

1- **Policy Owner:** <head of the cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <human resources function>

4- **Policy Compliance Measurement**: <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this policy on a regular basis.

2- All personnel at <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action as per <organization name>'s procedures.