Insert the organization logo by clicking on the image icon

Acceptable Use Policy Template

Date:

**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Title:** | Acceptable Use Policy Template | | |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  | |
| **Publish Date:** |  | | |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Objective 3](#_Toc97211288)

[2. Scope 4](#_Toc97211289)

[3. Policy 4](#_Toc97211290)

[3.1 General Requirements 4](#_Toc97211291)

[3.2 Unacceptable Use 5](#_Toc97211292)

[4. Exceptions 8](#_Toc97211293)

[5. Enforcement 8](#_Toc97211294)

[6. Roles and Responsibilities 8](#_Toc97211295)

[7. Policy Commitment 8](#_Toc97211296)

# Objective

The purpose of this policy is to outline the acceptable use of Information Technology (IT) resources. These rules are in place to protect the entity employees (users) from unacceptable uses and practices that can expose them to the risks including virus attacks, compromise of network, application systems and services, and legal issues.

# Scope

This policy applies to all entity employees, contracted personnel, trainees, third party's representatives who have been provided access to the IT assets at entity. This policy covers all information systems (Environments operated by the IT team).

# Policy

## General Requirements

1. Use of the IT systems and resources at <entity name> must at all the time be performed in a professional and accountable form.
2. It considered to understand the baseline information security controls to protect the information confidentiality, integrity, and availability in the <entity name>.
3. Users are responsible for protecting any information used and/or stored/accessible through their individual user accounts in the <entity name> from unauthorized use or disclosure.
4. Users shall access, use, or share <entity name>’s proprietary assets only to the extent it is authorized and necessary to fulfil their assigned job duties.
5. Users are responsible to promptly report any theft, loss, or unauthorized disclosure of proprietary information.
6. It shall be considered an offence for one or a group of employees, to be involved in activities that disrupt the organisation’s ability to pursue its business objectives as per the laws of Bahrain. Actions such as the deliberate disruption of (entity) IT systems, theft and/or destruction of equipment or data services, are serious offences.
7. Users shall not attempt to access any data or programs contained on any system for which they do not have authorization or explicit written consent of the owner of the system.
8. Each user is responsible for adherence this policy in its letter and spirit in the <entity name>.
9. Users shall not disclose <entity name> information to everyone within the <entity name> and to anyone outside the <entity name> without proper authorisation. All information available to the user in his/her business area or account will be in accordance with Law No. (16) Of 2014 concerning Protection of State Information and Documents.
10. Users shall not attempt to access any data or programs contained on any system for which they do not have authorization or explicit written approval from system owner.
11. Users shall report any weaknesses they discover in systems and any incidents of possible misuse or violation of <entity name>’s policies, to the proper authorities by contacting the IT team.
12. The email system is an entity resource and users are expected to utilize this in accordance with Email Security Policy.
13. Under no circumstances will the user account be used to participate in a personal financial activity, investments, promotional contests, etc.
14. All accesses to email shall be duly authorized by user’s management.
15. IT team shall implement suitable virus and spam control measures to minimise/reduce the chances of these infesting into the user’s mailbox or spreading unwanted messages from a user’s mailbox. This will be done through automatic scan for virus and spam. The findings and infections will be blocked or quarantined depending on the severity level.
16. IT team has the right to reject any recovery of Infected/Quarantined emails that might compromise the system or network.
17. Entity shall obtain all hardware and software from official corporate sources, to prevent the introduction of malicious code.
18. All users shall abide by software copyright laws and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements.
19. The entity shall use encryption software approved by official corporate sources.
20. Users shall not use a software for personal use on the entity information resources.
21. User shall use Internet to conduct business duties and tasks. Also, personal internet use shall be permitted if it does not interfere with user job duty or tasks.

## Unacceptable Use

1. The following practices are prohibited with no exceptions:
2. Downloading, posting, and storing obscene materials and pornography.
3. Circumventing user authentication or security of any host, network, or account.
4. Copying of confidential business-related data to any removable media such as USB Flash Drive or External Hard Drive without approval.
5. Introduction of destructive programs (e.g., viruses, self-replicating code) to cause intentional damage, interfere with others, gain unauthorized access, or inhibit production to entity’s/organization information systems.
6. Concealingown identity or masquerading as other user/s “Identity Theft”.
7. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
8. Using <entity name>’s systems to transmit any communication where the meaning of the message, or its transmission or distribution, is intended to be or is likely to be perceived as being abusive, defamatory, obscene, offensive, or harassing to the recipient or recipients thereof.
9. Users shall not download, install, or run security programs or utilities, which reveal weaknesses in the security of a system.
10. Users shall not log into a server, unless they are authorized, and it is within the scope of their job/regular duties. For purposes of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless this activity is a part of the employee's normal job.
12. Users cannot execute any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job.
13. Users shall not make copies of system configuration files for their own, unauthorised use or to provide to other people/users for unauthorised use.
14. Interfering with or denying service to any user (for example, denial of service attack).
15. Usage of <entity name> information systems and resources for personal usage or on behalf of a third party (i.e., personal client, family member, political or religious or charitable or school organization, etc.).
16. Attempting to access systems without proper authorizations.
17. Internal relay chat and P2P services.
18. The access to another individual’s email should be in accordance physical Security and Access control Policy.
19. The email exchange administrator should implement security complied strategy to ensure the security in every process.
20. All broadcast emails and accounts must be approved by the relevant directorate management.
21. Broadcasting unwanted emails containing personal views on social, political, religious, or other non-business-related matters are strictly prohibited.
22. IT team will ensure regular backup of e-mail messages on a daily basis
23. Entity e-mail addresses must be used primarily for business purposes only and strictly prohibited from using to set up personal businesses, social media or send chain letters.
24. Users shall not post sensitive/critical information on social media sites that clearly reflect on the individual and may also reflect on the individual’s professional life.
25. Users shall not post any information of other user/staff on social media sites without their permission including but not limited to, names, addresses, photos, videos, email addresses, and phone numbers.
26. Posting comments on social media sties may be held accountable.
27. User shall not use their personal user account for businesses purposes, except if it is authorized by the entity.
28. Users shall be discouraged from using the same passwords/PINs on their social media accounts being processed on the <entity name> devices and IT resources.
29. The user is responsible for evaluating both the appropriateness and the form of the broadcast emails.
30. The email service is for the sole use by authorised user. Users are authorised to access, use, copy, modify or delete files and data only on their own accounts and/or accounts to which they have been authorized to access.
31. All the issues related the password to use and access email services should be in accordance with password policy.
32. The email system is an <entity name> resource, and they are expected to utilize this for personal use only on a limited scale. Email will not be used for personal reasons if it may interfere with the performance of the system or the employee’s employment or other obligations. All messages and files composed, sent, or received using entity’s email system are and will remain the property of the entity.
33. Users will not use the e-mail system to send, receive, store, redistribute or display emails or files that are illegal or unethical.
34. Users will not alter the date, time, source/destination and/or any other information that is part of the header information of an email message.
35. Users are strictly prohibited from using third-party email systems and storage servers such as Google, Yahoo, and Hotmail etc. to conduct entity businesses.
36. In case of offensive emails received, the originator of the offensive e-mails should be communicated by affected user and asked to stop sending such messages or report such offensive e-mails directly to IT team.

# Exceptions

1. All exceptions to this policy shall be explicitly reviewed by the chief of cyber policies and regulations and approved by the general director of information security. The exceptions to this policy if any shall be approved and valid for a specific period and shall be reassessed and re-approved if necessary.

# Enforcement

1. Penalties for breaches of Acceptable Usage Policy will be based on the severity of the breach but can include:

* Loss of access privileges to information assets.
* Other actions as deemed appropriate by civil services Bureau (CSB) rules.

# Policy Enforcement

1. Policy document sponsor and owner: <Head of Cyber Security Department>.
2. Policy implementation and enforcement: <Department Concerned with Information Technology>.
3. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-