Organization:	Government Technology Agency, Thimphu: Bhutan
Department/Division:	Department of Digital Infrastructure, Government Network Division
Document Name:	Acceptable Use Policy

MANAGEMENT APPROVAL

Name	Signature	Date of Approval

REVISION DETAILS

Version No.	Issue Date	Change Details	Approved by	Released by

Table of Contents

1. Purpose

This Acceptable Use Policy (AUP) sets forth the principles and ethics that govern the use of ICT Services. It is designed to help protect other users, and the Internet community, from irresponsible, abusive, or illegal activities.

2. Scope

The AUP applies to all GovNETs (DrukREN and GovNet) users.

3. AUP recommendations:

- Users are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only.
- Any official document/information that is composed, transmitted, and/or received by the user's computer systems is considered to belong to the government and is recognized as part of its official data.
- The services and technology used to access the Internet are the property of the government and the government reserves the right to monitor Internet traffic and access data that is composed, sent, or received through its online connections.
- Official emails should not contain content that is deemed offensive. This includes, though not restricted to, the use of vulgar or harassing language/images.
- All sites and downloads may be monitored and/or blocked by the ICT section if they are deemed harmful and/or not productive to public service delivery.
- Keep your login accounts and password secure. Users must follow best practices for password security, including:
    i. Changing passwords regularly.
    ii. Using unique passwords for each system.
    iii. Enabling multi-factor authentication where available.
- Passwords should not be shared or stored in easily accessible locations.

4. AUP Prohibits the following but not limited to:

- Stealing, using, or disclosing someone else's password without authorization.
- Sharing confidential material, trade secrets, or proprietary information outside of the organization.
- Introducing malicious software onto the GovNETs and/or jeopardizing the security, sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via official email.
- Passing off personal views as representing those of the organization.
- Using computers to perpetrate any form of fraud, and/or software, film, or music piracy.
- Users are strictly prohibited from downloading software or any digital content that would result in infringement of copyright and licenses. Users shall be answerable to all legal actions thereof for violating the policy.
- Sending or posting information that is defamatory to the organization, its products/services, colleagues, and/or customers of the organization's electronic communications systems.
- Deliberate unauthorized access to government network facilities or services.
- Configuration or modification of the existing network through the introduction of unauthorized software and/or hardware.
- Creation or transmission or causing the transmission of pornographic, racist, or extreme political nature, or which incites violence, hatred, or any illegal activity.
- Adding, removing, or modifying identifying network header information in an effort to deceive or mislead.
- Attempting to impersonate any person by using forged headers or other identifying information.
- Sending unsolicited commercial emails or unsolicited bulk emails (spam) or junk-mails.

- Attempting to circumvent user authentication or security of any host, network, or account. This includes but is not limited to, accessing data not intended for the customer, logging into a server or account that the customer is not expressly authorized to access, or probing the security of service provider servers and networks.
- Using any program/script/command, or sending messages of any kind, designed to interfere with a user's session.
- Using the internet as a tool to exploit minors, and children or as an abusive tool.
- It is not advisable for residential connections from the main fiber link/office without obtaining proper authorization from the relevant authority.
- Upon retirement, separation, or resignation, all employees are mandated to return all system accesses, including email IDs and organization-related credentials, to the organization.
- Intentional physical damage to the networking equipment.
- Deliberate activities having, with reasonable likelihood, any of the following characteristics:

    i. Wasting service provider's staff effort or networking resources, including time on end systems and the effort of staff involved in the support of those systems;
    ii. Corrupting or destroying other users' data;
    iii. Violating the privacy of other users;
    iv. Disrupting the work of other users;
    v. Denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment);
    vi. Continuing to use an item of networking software or hardware after the ICT section has requested the user not to use it because it is causing disruption to the correct functioning of services.

5. Reporting Violation of the AUP

- Any user, who believes that there is a violation of this AUP, shall direct the information to the ICT section or the relevant agency with all relevant information and evidence.
- The concerned authority shall take necessary action such as warnings, account cease, or account termination to the violator.

6. Revision of the AUP

- GovTech Agency reserves the right to revise, alter, or modify this AUP
- Any revision made to this AUP shall be made available to clients and agencies through postal mail or other certified / registered mail.

7. Monitoring

- The GovTech Agency usually does not monitor Internet services under normal circumstances; however, the section reserves the right to monitor Internet activities if necessary to protect the networks in general.

I understand and will abide by this AUP. I further understand that should I commit any violation of this policy, my access privileges may be revoked, and disciplinary action and/or appropriate legal action may be taken against me.

_____ _____

Employee signature Date