

Thimphu Thromde ICT Services Acceptable User Policy

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

1. Scope

The AUP is applicable to all Thromde Network users.

2. AUP recommendations:

- Users are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only.
- All Internet data that is composed, transmitted and/or received by the user's computer systems is considered to belong to the Thromde and is recognized as part of its official data.
- The services and technology used to access the Internet are the property of Thromde and the Thromde 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 to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
- All sites and downloads may be monitored and/or blocked by ICT section if they are deemed to be harmful and/or not productive to public service delivery.
- Users are expected to respect the legal protections to data and software provided by copyright and licenses.
- Keep your login accounts and password secure.

3. 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 Thromde network and/or jeopardizing the security
- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via official email



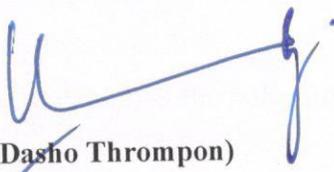
- Passing off personal views as representing those of the organization
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sending or posting information that is defamatory to the organization, its products/services, colleagues and/or customers of the organization's electronic communications systems
- Deliberate unauthorized access to Thromde networked facilities or services.
- 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 email 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, children's or as an abusive tool.
- Deliberate activities having, with reasonable likelihood, any of the following characteristics:
 - i) Wasting service provider's staff effort or networked 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;

[Handwritten signature]



- 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 ICT section has requested the user not to use it because it is causing disruption to the correct functioning of services.
- 4. Reporting Violation of the AUP**
- 4.1. Any user, who believes that there is a violation of this AUP, shall direct the information to the ICT section with all relevant information and evidence.
- 4.2. ICT section shall take necessary action such as warnings, account cease or account termination to the violator.
- 5. Revision of the AUP**
- 5.1. Thromde reserves the right to revise, alter or modify this AUP.
- 5.2. Any revision made to this AUP shall be made available to clients and agencies through postal mail or other certified / registered mail.
- 6. Monitoring**
- 6.1. Thromde ICTs usually do not monitor Internet services under normal circumstances; however, the section reserves the right to monitor Internet activities if seen necessary to protect the network in general.

In case of violation of this policy, access privileges for the particular user(s) shall may be revoked, disciplinary action and/or appropriate legal action may be taken.


(Dasho Thrompon)

Copy to:

1. Executive Secretary for kind information
2. All officials under Thimphu Thromde for strict compliance