Government Network (GovNet)

Guidelines

Department of Information Technology and Telecom

Ministry of Information and Communications

Thimphu, Bhutan

Version Control

Version	Date	Change	By
1.0	20 July 2018	Initial Document	DITT, MoIC

Executive Summary

For internal communication across the Government agencies, the Government Network (GovNet) has played most critical role. The infrastructure setup has eased dependence on ever increasing demand for Internet bandwidth for our internal accessibility making Government to Citizen/Government/Business systems accessible with minimal glitches.

The main purpose of a GovNet is to provide reliable, fast and safe communication across government agencies within Bhutan. The Ministry in an effort to derive similar benefit of the network is increasing GovNet penetration, improve application performance, improve data protection, and minimize costs. GovNet inter-connects Ministries, Departments and other government agencies, Thromdes, Dzongkhags, Drungkhags or Gewogs narrowing the geographical barrier.

This guideline document outlines the procedure for end users of this network to uphold security, efficiency and reliability.

1. Background:

The Department of Information Technology & Telecom (DITT) under the Ministry of Information and Communications(MoIC) have established a dedicated high speed fiber network – Government Network (GovNet) – interconnecting government agencies in the Ministries, Dzongkhags, Dungkhag and Gewogs. The network caters to the government agencies' needs for a reliable and high speed communication network to facilitate effective and efficient delivery of services at very economical cost. Today, the network has over 600 agencies availing more than 100 services ranging from critical services such as pems, myrb, audit security clearance to the simplest form of services as viewing citizens information within the network.

As we gear and transform into "ICT enabled society", there will be many more service offered on the network which would further add to the sensitive and significance of the network. More so, it is expected to generate huge amount of sensitive information with more number of services introduced online and transmit it over the network. The Ministry is committed in providing efficient and effective management of the network.

2. Definitions:

2.1. Government Network (GovNet)

For the purposes of this guidelines, the GovNet is defined to include all links and devices used to terminate or initiate data communication services. The devices may include hubs, routers, switches, wireless devices, or other devices that creates the point of presence (PoP) of GovNet.

2.2. Agency Network

For the purposes of this guidelines, the Agency Network shall include other WAN (Thromde WAN and Thimphu WAN) and LAN including file servers, personal computers, printers, and other computing or data communications devices that are used by any department, office, agency, board, or commission within the Government.

2.3. External Entity Network

Any other organization such as Financial Institutions, State Owned Corporations, Non Government Agencies and other is considered as an external entity requiring specific authorization to connect and access the GovNet and further extension. Such extension is required to abide by the GovNet Guidelines and Standards, including any revisions, while connected.

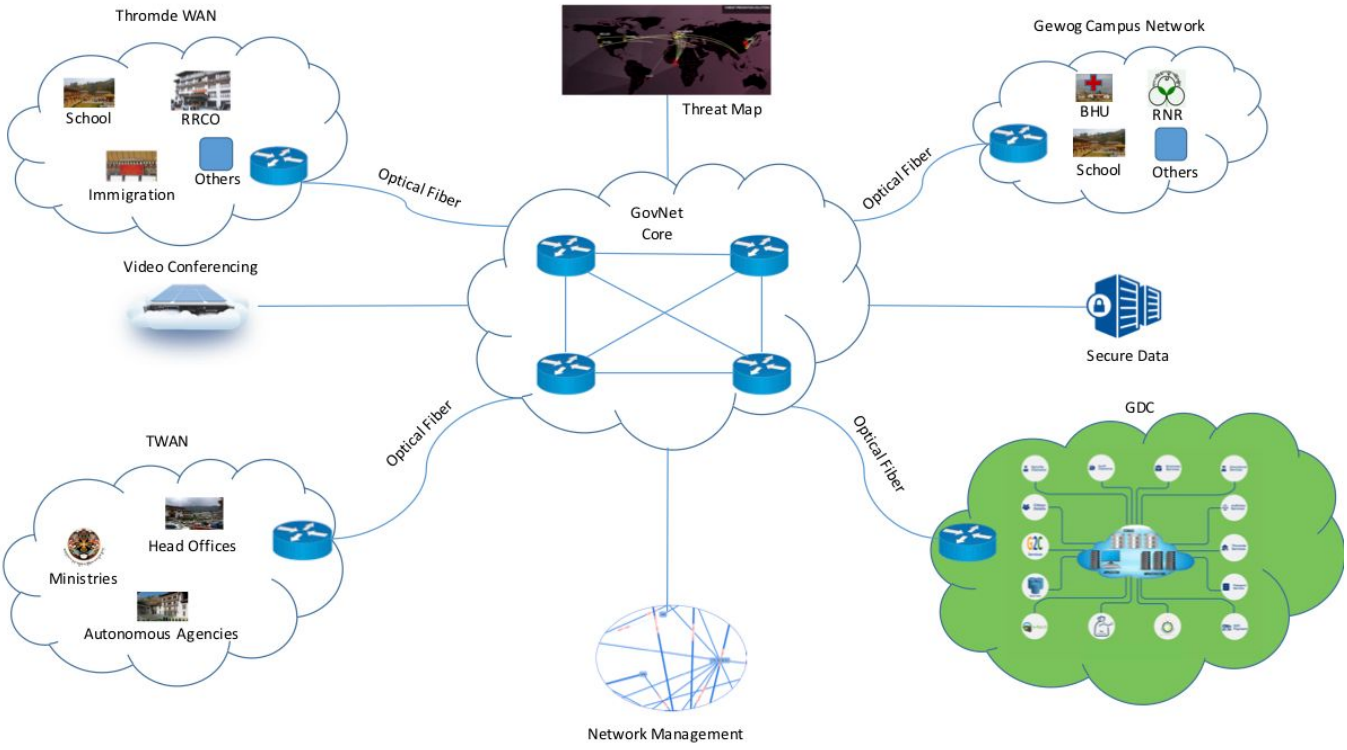

Figure 1. Overview of GovNet

3. Guidelines Objectives

The objectives of this guidelines are to:

a. Contribute to a secure GovNet environment for all connected departments, offices, agencies, and commissions.

b. Provide a uniform security framework to secure the integrity, confidentiality, and availability of information and information systems, at the WAN level.

c. Provide, in balance with operational requirements, legislative requirements, and the minimum GovNet security requirements.

d. Raise awareness of information and information technology security needs for all users of the GovNet by providing the security principles, requirements, and rules of use.
e. Define the clear roles and responsibilities of all users of the GovNet
f. Provide a foundation to develop and implement additional guidelines and standards as may be required to address specific network requirements and security issues.

All users availing GovNet facilities and services shall use responsibly with compliance with Acts of Media, other guidelines and procedures of the Ministry's own and those set forward by MoIC, and with normal standards of professional and personal courtesy and conduct.

4. Ownership

a. The ownership of the GovNet systems and services shall reside with the Ministry.
b. It shall include any networking address, site, number, account, or other identifier associated with the network.
c. The ownership of agency network and external entity shall remain with the respective agencies, and thereof all issues pertaining to the specific network shall be the responsibility of the custodian.

5. Application

This guidelines applies to all connected agency network; regional departments, offices, agencies, and commissions (Client Organizations), and other authenticated users in an authorized area of the GovNet such as municipalities, academic institutions and others.

Any content covered by departmental guidelines also covered by or in conflict with any content in this guidelines is superseded by this guidelines. Additionally, this guidelines supersedes any prior guidelines related to GovNet network requirements and security.

6. Guidelines Directives

guidelines directives are the minimum mandatory requirements that shall be met by Agency Network and External Entities.

6.1. Identification/Authentication

a. All accounts, user IDs and devices in the Agency Network shall be uniquely identifiable.
b. IT systems within the GovNet shall authenticate all users, applications and devices except for those designed specifically for anonymous access. These exceptions require the approval of the Ministry.

6.2. Access Controls/Authorization

a. All access points to the GovNet shall be approved by the Ministry.
b. All physical and logical connections to the GovNet intended to provide access by individuals or groups shall be approved by the Ministry.
c. All changes and configurations related to GovNet shall be approved by the Ministry.
d. Any individual, office, or network connected to the Agency Network shall require all employees to agree, through a signed or electronic agreement, to abide by the requirements outlined in the GovNet guidelines and Standards.
e. Requests for access to the GovNet for an external entity shall be done through the Ministry.
f. Personnel who have access to sensitive information or are responsible for critical IT security functions such as network administrators and technical support staff require to maintain the entry and exit log.

6.3. Remote Access

a. Any remote access over untrusted networks shall use technology approved by the Ministry to secure, monitor, and filter traffic.
b. All remote access to the GovNet shall be authenticated, logged, and restricted to minimize the security risk to GovNet assets.
c. All users who use GovNet resources remotely shall agree, through signed or electronic agreement, to abide by these requirements.

6.4. Telecommunications Service Providers

a. All service providers contracting with government such as suppliers of data communications or security services shall commit contractually to ensure that the GovNet and Agency profile is maintained.
b. All service providers contracting with government shall have access to the GovNet guidelines and Standards and agree to abide by them and ensure they are enforced within their organization.
c. Any exception to these directives shall be approved by the Ministry and included as an addendum to the contract.

6.5. Contractors

a. All contracts or service agreements involving Agency Network facilities, configuration, management or any other application or server residing on the network shall include appropriate security clauses ensuring compliance with the GovNet guidelines and Standards.
b. All persons and organizations contracting with government (i.e., consultants, third party subcontractors, and casual and student employees) shall have access to the GovNet guidelines and Standards and agree to abide by them.

6.6. Time Synchronization

a. All devices on the Agency Network shall synchronize with a common central time source.
b. NTP server shall be maintained by the Ministry, and notify of any changes made to the server to all the agencies.

6.7. Revocation/Termination Of Govnet Privileges

a. The Ministry shall take appropriate action, including termination of any connection or activity, at any time where the Ministry feels the security of the GovNet is or could be severely compromised. The Ministry shall make a full report of the actions taken and the reasons for such actions.

6.8. Change Control

a. All planned, scheduled changes to the GovNet (power up, power down, configuration changes, and reset) shall be performed or authorized by the Ministry.
b. A change control process shall be used to assess the security impact of major system upgrades and to support eGIF compliance as defined in the clause 5.11.
c. The change control process shall ensure that all system configurations and modifications are documented and retained in a secure environment for audit or future risk management considerations.

6.9. eGIF Compliance

a. IT system and security shall comply with eGIF on the Agency Network (including all hardware and software that comprises the Agency Network) throughout the planning, implementation, and operations life cycle.

6.10. Security Management

a. Appropriate logs shall be kept and reviewed as prescribed by this guidelines. All actual or suspected security incidents shall be recorded and reported to the Ministry.
b. GovNet infrastructure shall document security issues, disaster recovery operations, change control processes, diagnostic or security breach investigations, visual inspections, and security audit.
c. GovNet guidelines and security information and documentation including configuration, backups, and diagnostic information shall be password protected, physically stored under lock and key, and only released on the approval of the Ministry. If located at a contractor site the protective details and obligations shall be addressed in the contract.
d. GovNet information and documentation to be discarded, and which contains sensitive information such as passwords and IP addresses, shall be irretrievably destroyed in a secure manner by shredding, permanent electronic deletion, or by other means approved by the Ministry.

e. Security risk management based upon due diligence and due care shall be the primary basis to determine GovNet security safeguards and residual risk, and to maintain the accredited GovNet security profile.
f. Re-assessments of the security profile shall take place if risk, system, or other relevant technological or organizational changes occur.
g. Before implementation, all new systems as well as additions, deletions, or alterations to existing systems shall be reviewed to ensure that the security profile of the Agency Network is not compromised by the change.

6.11. Physical And Environmental Security

a. An adequate environment (e.g., temperature, humidity, backup power supply) shall be provided to ensure optimum operation of the GovNet and common infrastructure equipment as specified in the GovNet documentation.
b. Physical controls shall be implemented to prevent unauthorized access to GovNet point of presence and Agency Network equipment including routers, switches, wiring racks, and network access servers.
c. The Ministry shall have input into and final approval of all site design where GovNet connectivity is being provided.

6.12. Incident Reporting And Investigation

a. All Agency Network security incidents shall be reported and investigated immediately by the infrastructure or application owner. The concern agency shall notify Ministry and other clients who may or could be affected.
b. The BtCIRT may also conduct a self instituted secondary investigation as requested by the infrastructure or application owner, to determine if there are additional security issues and the appropriate solutions.
c. In case of security incidents, the concerned authority of the Agency network shall report to the BtCIRT with all digital evidences such as logs, snapshot of the system secured for further examination/investigation.

6.13. Monitoring/Surveillance And Privacy

a. Ministry shall monitor the GovNet for performance and security purposes.
b. Monitoring initiatives designed for the Govnet shall operate within the legislated requirements for protection of personal privacy.

c. Access or monitoring of LAN segments shall be in co-operation with network administrators and concern agencies.
d. No person shall operate sniffers or other monitoring devices on the Agency Network unless authorised by the Ministry.
e. Where there is reason to believe that an individual is engaging in inappropriate activity on the GovNet or Agency Network the content of individual files may be read.
f. Any investigation of data content shall be conducted in accordance with legislation.

6.14. Interference, loss and damage

a. GovNet facilities shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any networking facilities, or unwarranted or unsolicited interference with others' use of the GovNet facilities.
b. The Ministry shall not be held accountable for any loss or damage incurred by an individual as a result of personal use of GovNet facilities. Users should not rely on personal use of GovNet facilities for communications that might be sensitive with regard to timing, financial effect, or privacy and confidentiality.
c. The GovNet accepts no responsibility for the malfunctioning of any networking facility other than the GovNet itself or for the loss of any data or software, or the failure of any security or privacy mechanism. No claim shall be made against the GovNet, its employees or agents in respect of any loss alleged to have been caused by defect in the resources or by act or neglect of the GovNet, its employees or agents.
d. Users must not in any way cause any form of damage to the GovNet facilities, or to any accommodation associated with them. Agencies may be charged for the cost of remedying any damage they cause.

6.15. GovNet Training

a. The Ministry shall provide training to all Agencies and others as necessary on GovNet guidelines and Standards including interpretation and application.
b. Client Organizations are responsible for the GovNet guidelines and Standard training within their organization required to ensure performance of the agency outlined in the GovNet guidelines and Standard.

7. Unacceptable Use

GovNet facilities and services may not be used for:

a. Illegal activities, (these include the creation, display, production or circulation of offensive material);
b. Commercial purposes not under the auspices of the RGoB;
c. Personal financial gain;
d. Uses that violate other guidelines. The latter include, but are not limited to guidelines regarding intellectual property and sexual or other forms of harassment or threatening behaviour.

8. Copyright

a. The contents of all networking services shall conform to law and GovNet guidelines regarding protection of intellectual property and freedom of information, including laws and guidelines regarding copyright, patents, trademarks, and data protection.
b. Copyright-related restrictions may include copying or distributing programs or data, using programs or data for non-educational purposes or financial gain, using programs or data without an appropriate license, or disclosing information about programs.
c. Users must adhere to the terms and conditions of GovNet facilities including software, equipment, services, documentation, datasets and databases, and other goods. It is the responsibility of agencies to ensure that all network and services used on the network shall not infringe copyright laws.