Government Data Center

Policies & Procedures

Prepared by

Government Data Center Team,

Department of IT & Telecom,

Ministry of Information & Communications

Revision History

Revision[1] #	**Description [2]**	**Initials [3]**	**Date [4]**
1.0	Initial SOP draft	NG, DZ, KS	03-02-2017
1.1	Introduced onboarding security requirements	BtCIRT & NRD CS	24-05-2017
1.2	Introduced user and password management, network and system services section.	NG	30-06-2017
1.3	Introduced clauses 7 & 8 under Roles and responsibilities(System Owner) section.	BtCIRT & GDC	09-03-2020

Note

The document will be revised bi-annually.

Throughout this document, following norms will be adopted.

1. Numeric value before decimal represents version of document and after represents number of revision undergone (1.1).

2. Denote changes made in the document (e.g. definition update).

3. Changes made by and approved.

4. Format of the date will be day, month, year.

Table of Contents

Revision History **2**

1 Purpose **5**

2 Scope **5**

3 Introduction **5**

4 Definitions **6**

5 Physical Access **6**

5.1 Staff/Vendor 6

5.2 Visitor 7

6 Remote Access **7**

6.1 Virtual Private Network (VPN) 7

6.2 Secure Shell Access 8

7 Resources **8**

7.1 Hardware/Equipment 8

7.2 Application/Software 9

7.3 Allocation 9

8 Hosting **10**

9 Reporting and Documentation **10**

9.1 Emergency Contact 10

9.2 Roles and Responsibilities 11

10 Inventory Management **15**

10.1 Hardware 15

10.2 Software Library 15

10.3 Service/Applications Catalogue 15

11 Configuration and Testing **16**

12 Username and Password Management **16**

12.1 Minimum Password Length 17

12.2 Password Composition 17

12.3 Password Management 17

13 Network and System Services **18**
13.1 Network Time Protocol 18
13.2 Domain Name System 19
13.3 Simple Network Monitoring Protocol 19
14.4 Log Service 19
15 Glossary **19**
14 Annexure **21**
A. Physical Access Request form 21
B. Remote Access Request form 23
C. List of hardware models 25
The list is maintained separately for security reasons. 25
D. Software version 26
The list is maintained separately for security reasons. 26
E. GDC Service Catalogue 27
F. Emergency contact update form. 28
G. Reporting Template 29
Type of Outage(Scheduled Maintenance/Device Outage/Fibre Breakdown/System Issue) 29
Response Time/Date 29
Resolve Time/Date 29
Rectifier 29
Remarks 29
H. Work Permit Form 29

1 Purpose

These Policies and Procedures shall serve as guiding policy document to ensure smooth operations of GDC/Government network services. The objective is to achieve efficiency, quality output and uniformity of performance, while reducing miscommunication and failure to comply industrial regulations. It clarifies processes by which all current and future stakeholders for GDC shall be mandated to follow and adhere.

2 Scope

It shall apply to all GDC staffs, government agencies, contractors, vendors and the stakeholders availing GDC services. It also cover all servers, information systems (applications) hosted at GDC, computers, smartphones, tablets and all terminal equipment connected to GDC services that is being used to configure and manage service installation remotely.

3 Introduction

GDC is a critical national ICT infrastructure, which serve as a platform to efficiently and reliably deliver G2G, G2C and G2B services. It is located at TTPL, Babesa in 1000 sq.ft space in the 2500 sq.ft data center space, with state-of-art ancillary facilities including power, cooling, rack space, fire safety and other physical security feature.

4 Definitions

Application: an information system to be hosted or hosted at GDC.

Authorized Staff/User: employees who are authorized to gain access to the GDC.

Authorized Vendor: Private contractor who, through contractual arrangement and appropriate approvals, have access to the GDC.

Data Center Staff: DITT employees who work at the GDC

Server: a virtual machine in GDC infrastructure

System: see Application

Visitors: All other personnel who may occasionally visit GDC but are not authorized to be in the GDC without escort.

5 Physical Access

5.1 Staff/Vendor

Authorizations will only be approved for individual(s) who are responsible for installation and/or maintenance of equipment housed in the Government Data Center. Approval processes are as follows:

1. Concerned vendor/staff must fill up access authorization form(Annexure A) and submit to DITT/MoIC.
2. Upon approval, the authorized staff member or vendor shall be issued access permit.
3. Authorized staff/vendors shall be allowed entrance into the GDC area by a Data Center employee upon producing access permit.
4. Authorized staff/vendors are responsible for logging in/out when entering/exiting the GDC. The purpose of the visit must be documented.

5.2 Visitor

Anyone who is not a GDC employee, an authorized staff member, or authorized vendor is considered a visitor. All visitors to the Data Center must adhere to the following procedures:

1. Visitors must be accompanied by either a Data Center employee or other authorized staff member at all times while in the Data Center.

2. Visitors must log in/out when entering/exiting the Data Center. The purpose of the visit must be documented.
3. Visits should be scheduled through DITT/MoIC. Unscheduled visits to install equipment or perform other tasks shall not be entertained.

6 Remote Access

6.1 Virtual Private Network (VPN)

Only approved employees and authorized third parties (customers, vendors, etc.) shall be provided VPN clients credentials. Authorized employees or third parties must adhere to following requirement:

2. It is the responsibility of employees/authorized party with VPN privileges to ensure that unauthorized users are not allowed access to the network.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel.
5. VPN users will be automatically disconnected from network after thirty minutes of inactivity. The user must then log on again to reconnect to the network.
6. The VPN concentrator is limited to an absolute connection time of 24 hours.
7. Only GDC approved VPN clients must be used.
8. Authorized user shall protect their username and passwords even from family members.

6.2 Secure Shell Access

Only approved employees and authorized third parties (customers, vendors, etc.) shall be provided SSH credentials. Authorized employees or third parties must adhere to following requirement:

1. It is the responsibility of employees/authorized party with SSH privileges to ensure that unauthorized users are not allowed access to the network.

2. SSH users will be automatically disconnected from network after thirty minutes of inactivity. The user must then log on again to reconnect to the network.

3. Authorized user shall protect their username and passwords even from family members.

5. SSH shall be allowed from Thimphu Wide Area Network(TWAN) only. Access from global network is allowed from VPN connectivity only.

7 Resources

7.1 Hardware/Equipment

Hardware/Equipment refers to all devices(storage, compute, network), racks, cables installed within the GDC designated area. All installation, replacement and removal works shall be approved by DITT.

Authorized staff/vendor performing equipment installation must submit a work permit form(Annexure H) and get approval before carrying out any of the following tasks.

1. Installation of new hardware.
2. Replacement of hardware.
3. Removal/Decommissioning of defective equipment or expired equipment. The expired equipment shall be returned back through a buy-back policy.

7.2 Application/Software

Application/Software refers to all proprietary, in-house or outsourced software as well as all open source software being used to run the services at GDC. All installation, configuration, testing, upgrades, updates and removal of application/software must be carried out in consultation with concerned agencies and DITT/MOIC.

The authorized staff/vendor performing installation or configuration works shall submit a work permit form (Annexure H) and get approval before carrying out any of the following tasks:

1. Installation and configuration.
2. Upgrades/Updates.
3. Decommissioning/Uninstallation/Removal.

7.3 Allocation

Resource refers to all usable network, compute and storage capacities currently available and ready to be allocated. The concerned agency wishing to avail resources at GDC must follow procedures outline below:

1. Seek approval from DITT/MoIC to host services/application at GDC.
OR
2. Submit resource requirements via www.neyduetewa.gov.bt. The application must be accompanied with a comprehensive project document in case of new application/system/website.

3. Comply with security requirements for every application to be hosted at GDC. Compliance audit will be done by BtCIRT.

8 Hosting

1. Any government agency wishing to host online public service is eligible to avail GDC services. Systems intended for internal use are not permitted to host in GDC.

2. All the applications are hosted in a virtual environment. Hosting on a physical server is prohibited.

3. Co-location of any type of hardware equipment is not permitted.

4. Agencies wishing to host their application are required to submit their requirement via online portal www.neyduetewa.gov.bt/www.gdc.gov.bt.

9 Reporting and Documentation

1. A report must be compiled and maintained for review on a quarterly basis, in the format attached **(Annexure G)** along with a copy of the report generated by NMS system**.** The report shall be maintained by GDC O&M team.

2. All network communication logs must be maintained for a period of three months and archived for a period of six months.

9.1 Emergency Contact

In the event of a staff member availing leave, it should be ensured that there is a competent personale, who is capable of fulfilling all obligations during his/her absence.

Following procedures must be adopted:

1. Update contact emergency form(annexure A) and provide a copy to GDC PMU/Update emergency contact in GDC website.
2. Set auto-responder on email along with contact details of person who has been delegated the task.
3. Inform through closed/secure social media group or community, if there is any such group instituted for faster dissemination of information.

9.2 Roles and Responsibilities

		Composition	Responsibilities
	Management	1. Director, DITT 2. Head of all division, DITT	1. Provide direction and guidance in line with SKRAs and NKRAs. 2. Authorize and approve project scopes during upgrades and change management process. 3. Make decision to suspend asset's hosting in case of critical security issues.
	Project Management Unit(PMU)	1. Head, Infra Division, DITT 2. Project Team	1. Prepare project scopes based on available resources. 2. Provide technical support and guidance to concerned agencies. 3. Advise management on data center trends. 4. Liaise with O&M contractor and government agencies. 5. Manage and approve GDC service hosting. 6. Forecast and plan GDC resource capacity. 7. Liaise and coordinate with private contractor(if case of outsourcing) and relevant system/application owners. 8. Assess the resource requirement submitted by system/application owners and grant approval. 9. Plan and coordinate change management. 10. Coordinate and communicate with end users, as and when required, about application-level impacts of outages or scheduled maintenance. 11. Ensure adequate Internet and GovNet bandwidth is available.

			12. Perform systems ad-hoc backups on special request from applications owners' side 13. Escalate application's security resolution issues and recommendation to suspend asset's hosting.
	System Owner	Concerned agency	1. Configure, maintain, manage, update, patch application/databases and operating systems(OS) hosted in GDC. 2. Ensure OS/application's compliance with security requirements as per BtCIRT's baseline requirement(Annexure) 3. Patch and update application and OS vulnerabilities based on BtCIRT's security requirement. 4. Seek storage, compute and network resources to host application in the GDC. 5. Carry out migration of applications to GDC. 6. Consult with the GDC and BtCIRT team on security requirements of applications. 7. In the event of patch failure , the vulnerable-flagged system shall be taken down to minimize the risk of affecting other systems. The system owners will, however, be able to access their system on the government private network to fix the vulnerabilities. 8. Agencies failing to patch due to incompetencies or lack of resources

			shall be responsible for securing their own funding or arrangement.

	GDC Technical Support Team	Technical team of concerned contractor	1. Configure and set up new virtual platform. 2. Allocate resources such as memory, storage, processor, network. 3. Provision and manage IP addressing scheme. 4. Implement firewall security policy(ies) needed for system management and accessibility. 6. Patch and Update OS of network devices(firewall, router, switches, storage). 7. Ensure the hardware contingencies are maintained throughout operation of GDC networks and services. 8. Monitor availability and utilization of server/storage/network resources. 10. Provide 24/7 or 9/5 on-call support, as specified for each supported server or device. 11. Diagnose and rectify hardware problems. 12. Configure, maintain and monitor servers such as DNS, Log Server, NTP, NMS and other critical servers required to operate GDC infrastructure.

	BtCIRT		1. Decision on application's criticality level (basic | medium | CII) 2. Compliance audit against security requirements (initial, final, yearly) and decision for GO / Not GO 3. Periodic vulnerability scanning according asset criticality 4. Basic incident detection activities through deployed sensors. 5. Incident handling activities once incident is detected 6. Escalation to an System Owner → PMU → Management in case of major security compliance issues

10 Inventory Management

An inventory of all hardware/software/application shall be maintained.

10.1 Hardware

An up-to-date list of hardware component in GDC shall be maintained.

10.2 Software Library

An up-to-date list of applications hosted in GDC shall be maintained.

10.3 Service/Applications Catalogue

A list of software licenses/versions, Operating Systems and other critical software shall be maintained.

11 Configuration and Testing

11.1 DITT shall provide a staging server where new software/applications shall be temporarily hosted for testing before going into production environment.

11.2 All configuration and testing of hardware/software shall be carried out in the staging server.

11.3 Staging server will be a temporary provision until the end of testing phase. After completion of tests, all resource shall be held back and all configurations shall be erased.

12 Username and Password Management

The requirements in this standard apply to passwords for any computing account across any GDC resource, to the users of any such accounts, and to system administrators and developers who manage or design systems that require passwords for authentication.

Users, including administrators, must log on using their personal user accounts to enforce accountability. Use of shared accounts must not be used unless approved in written.

Default administrator or root access accounts, and in-built accounts must be secured by the following means:

1. Renamed to something other than default (Windows only)

2. Disable the renamed account (Windows only)

3. Create a secondary local administrator account

4. Set with a long and complex password

Default, anonymous and guest accounts including default vendor accounts must be disabled and/or deleted in application and related equipment and systems (if any).

Administrator's account will be locked after maximum 5 unsuccessful attempts to login into system (from server side).

12.1 Minimum Password Length

Passwords shall have a minimum of 8 characters with a mix of alphanumeric and special characters; if a particular system will not support 8 character passwords, then the maximum number of characters allowed by that system shall be used.

12.2 Password Composition

Passwords shall not consist of well known or publicly posted identification information. Names, usernames, date of birth, identity number, employee ID etc should not be used as a password.

12.3 Password Management

12.3.1 Password Storage

Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames.

Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application.

12.3.2 Password Sharing and Transfer

Passwords shall not be transferred or shared with others unless the user obtains appropriate authorization to do so.

When it is necessary to disseminate passwords in writing, reasonable measures shall be taken to

protect the password from unauthorized access. For example, after memorizing the password, one must destroy the written record.

When communicating a password to an authorized individual orally, take measures to ensure that the password is not overheard by unauthorized individuals.

12.3.3 Electronic Transmission

Passwords shall not be transferred electronically over the Internet using insecure methods. Wherever possible, security protocols including IMAPS, FTPS, HTTPS, etc. should be used.

12.3.4 Password Recovery

In the event of losing passwords, a case shall be lodged to GDC team. Temporary password will be issued , which should be changed after the first login.

13 Network and System Services

Network and System services refers to software that are installed and activated inside servers and network devices, located at GDC such as NTP, SNMP, DNS, DNS, Log etc.

13.1 Network Time Protocol

An accurate time source such as Network Time Protocol (NTP) based time keeping must be maintained by application servers. Applications hosted within GDC should synchronise system time with GDC NTP server.

13.2 Domain Name System

GDC services can be accessed both through Internet and Intranet(TWAN). It is advised to use TWAN DNS to access GDC services for better user experiences. Services within GDC shall not be permitted to use other global DNS except country DNS.

13.3 Simple Network Monitoring Protocol

All servers and network device hosted in GDC should be configured only with SNMPv3 services. Lower version protocols such as SNMPv1 and v2 are not recommended due to high security risk. Unencrypted communication protocols such as TELNET, FTP shall be disabled on servers.

14.4 Log Service

All servers and network device hosted in GDC should be configured to send log to the centralised log server.

15 Glossary

DNS Domain Name System
GDC Government Data Center
FTP File Transfer Protocol
NMS Network Monitoring System
NTP Network Time Protocol
SNMPv3 Simple Network Monitoring Protocol Version 3
SSH Secure Shell
VPN Virtual Private Network

14 Annexure

A. Physical Access Request form

This form must be filled by the person seeking approval to access GDC and submitted to GDC team/Operator. Anyone accessing the GDC must read, agree to and follow the process outlined in SOP/Policy.

Request Date:

Details of Requestor

Requestor:	Head/Supervisor:
Agency:	Division/Unit:
Contact No.	Contact No.
email	email

Reason For Access Request (Specify work)

Specific areas you require to access

Access Timeframe

Time	Date

For Administrative Use

Status

Approved	Denied

Remarks:		
Name	Signature	Date

B. Remote Access Request form

This form must be filled by the person seeking approval to access GDC and submitted to GDC team/Operator. Anyone accessing the GDC must read, agree to and follow the process outlined in SOP/Policy.

Request Date:

Details of Requestor

Requestor:	Head/Supervisor:
Agency:	Division/Unit:
Contact No.	Contact No.
eMail	email

Details of a person who will access

Name	EID
Contact No.	email
Agency	

Reason For Access Request (Specify work)

Type of Access Required

VPN	

Technical information required from Requestor

Mac Address of >>>	

Access location

Within Bhutan(Specify place)	Outside(Specify country)

Access Timeframe

Time	Date

For Administrative Use

Status

Approved	Denied	
Remarks:		
Name	Signature	Date

C. List of hardware models

The list is maintained separately for security reason.

D. Software version

The list is maintained separately for security reason.

E. GDC Service Catalogue

F. Emergency contact update form.

Name	
Email	
Contact Number	
Agency	

G. Reporting Template

Type of Outage(Scheduled Maintenance/Device Outage/Fibre Breakdown/System Issue)	Response Time/Date	Resolve Time/Date	Rectifier	Remarks

H. Work Permit Form

Type of Work	Name	Agency	Start Date/Time	End Date/Time	Signature