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
1.4	Introduced clause 14 under Roles and Responsibilities (GDC PMU) section	NG,DZ	12-10-2020
2.0	Introduced e-permit under physical access, section 5. Introduced key-based authentication recommendation clause under section 6.2. Introduced support service assurance section 10. Edited and clarified specific roles in Roles and Responsibilities section 11. Revisited the whole document and made detailed editions, clarifying points.	NG, DZ & JL	04-04-2021

Note

The document shall be revised as deemed necessary.

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

1 Purpose

These Policies and Procedures shall serve as a 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 with 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 staff, government agencies, contractors, vendors and the stakeholders availing GDC services. It also covers all servers, information systems (applications) hosted at GDC, computers, smartphones, tablets and all terminal equipment connected to GDC services that are being used to remotely configure and manage service installation.

3 Introduction

GDC is a critical national ICT infrastructure, which serves 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 features.

4 Definitions

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

Authorized staff: employees who are authorized to gain access to the GDC. Authorized staff includes O&M contractors.

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

GDC client: a government agency who has hosted their system in GDC.

GDC staff: see authorized staff.

Server: a virtual machine in GDC infrastructure

System: see Application

Test users: users identified by GDC client for using their system, feeding data, etc., during the staging for testing the system.

Third party vendor: a vendor of GDC client.

Visitors: all other personnel who may occasionally visit GDC. The visitors must be accompanied by authorized staff members at all times while in the Data Center.

5 Physical Access

5.1 Authorized Staff

Following processes are to be followed by staff:

1. Authorized staff must register when entering/exiting the GDC. The purpose of the visit must be documented.

5.2 Third Party 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 vendors must fill up and submit online access authorization form(Annexure A).
2. Upon approval, the authorized vendor shall be issued an access permit electronically.
3. Vendors shall be allowed entrance into the GDC area by a Data Center employee upon verifying the access permit.
4. Vendors must register when entering/exiting the GDC. The purpose of the visit must be documented.

5.3 Visitor

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

1. Visitors must fill up and submit an online access authorization form(Annexure A).
2. Upon approval, the visitor shall be issued an access permit electronically.
3. Visitors shall be allowed entrance into the GDC area by a Data Center employee upon verifying the access permit.
4. Visitors must register when entering/exiting the Data Center. The purpose of the visit must be documented.
5. Visitors must be accompanied by authorized staff members at all times while in the Data Center.

6 Remote Access

6.1 Virtual Private Network (VPN)

Only authorized personnels (GDC staff, GDC client, third party vendors, test users) shall be provided VPN clients credentials. Authorized personnels must strictly adhere to the following rules and guidelines:

1. It is the responsibility of authorized personnel with VPN privilege to ensure that unauthorized users are not allowed access to the network.
2. VPN users will be automatically disconnected from the network after thirty minutes of inactivity. The user must then reconnect to the network.
3. Only GDC approved VPN clients must be used.
4. It is the responsibility of the authorized users to maintain the confidentiality of their vpn credentials.
5. For a security reason, vpn credentials will be reset every 3 months in order to filter out the inactive users.
6. It is mandatory to maintain separate and exclusive vpn credentials for third party

consultants or vendors. The credential shall be surrendered upon completion of project.

6.2 Secure Shell Access

Authorized personnel must strictly adhere to the following rules and regulations:

1. It is the responsibility of authorized personnel with SSH privileges to ensure that unauthorized users are not allowed access to the network.
2. It is the responsibility of the authorized personnel to maintain the confidentiality of their ssh credentials.
3. For a security reason, ssh key-based authentication is recommended.
4. Ssh shall be allowed from agencies connected to GovNet infrastructure and over vpn 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 performing equipment installation must submit an online 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. Repairing of hardwares.
4. Removal/Decommissioning of defective equipment or expired equipment.

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 operate GDC infrastructure. All installation, configuration, testing, upgrades, updates and removal of application/software must be carried out in consultation with DITT/MOIC.

The authorized staff/vendor performing installation or configuration works shall seek online work permit approval form (Annexure H) prior to undertaking following tasks:

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

7.3 Compute, Storage & Network

7.3.1 Compute

A virtual machine with base spec of 4 cpu and 4 GB RAM shall be provided for a new system in a staging environment. The resources can be increased upon requirement and utilization analysis.

7.3.2 Storage

A virtual machine with base spec of 50 GB hard disk shall be provided for a new system in a staging environment. The resources can be increased upon requirement and utilization analysis.

7.3.3 Network

A virtual machine for a new system shall be assigned a local staging IPv4 address. Upon migrating to the production environment, it shall be replaced with a new local production IPv4 address which shall be mapped with a global IPv4 address.

8 System Hosting

8.1 Prerequisites

1. Any government agency wishing to host online public service is eligible to avail GDC services. Systems intended for internal use shall not be permitted to be hosted in GDC.
2. All the systems shall be hosted in a virtual environment. Hosting on a physical server is prohibited.
3. Aspiring eligible government agencies shall produce egif clearance while requesting for server space in GDC.
4. Systems with academic/educational contents shall not be permitted in GDC.

5. Co-location of any type of hardware equipment shall not be permitted.

6. Agencies wishing to host their application must strictly follow the procedures outlined in GDC Space Request and Allocation SoP.

8.2 Compliance

8.2.1 Security compliance - adhere to security standards and best practices
8.2.2 Support and services - adhere to SoP for seeking support and services

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,vCenter,Firepower…**.** The report shall be compiled and submitted by the GDC O&M team to GDC PMU.

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

10 Support Service Assurance

In the event of a staff member availing leave, following must be strictly adhered to:

1. It should be ensured that there is a competent personnel, who is capable of fulfilling all obligations during his/her absence. (may develop and submit support service assurance plan)
2. Inform through email or closed/secure social media group or community, if there is any such group instituted for faster dissemination of information.

11 Roles and Responsibilities

		Composition	Responsibilities
	Management	1. Director, DITT 2. Head, Infra Div, DITT 3. Head, AMD, DITT. 4. Head, BtCIRT 5. GDC/PMU	1. Provide direction and guidance in line with SKRAs and NKRAs. 2. Authorize and approve project scopes involving major upgrades and change management processes.
	Project Management Unit (PMU)	1. Head, Infra Division, DITT 2. Project Team	1. Prepare project scopes based on available resources. 2. Advise management on data center trends. 3. Forecast and plan GDC resource capacity. 4. Assess the resource requirement submitted by system/application owner and grant approval. 5. Facilitate hosting/migration of approved systems in GDC. 6. Monitor the resource utilization by the systems hosted in GDC. 7. Provide technical support and guidance to the concerned agencies; Technical support on compute, network, storage and operating system. 8. Liaise with O&M contractors and government agencies (relevant system/application owners). 9. Plan and coordinate change management. 10. Coordinate and communicate with GDC system owners, as and when required, about the application-level impacts of

			outages or scheduled maintenance. 11. Ensure adequate Internet and GovNet bandwidth is available. 12. Maintain system backups as per GDC Backup & Recovery Policy. 13. Escalate application’s security resolution issues, and suspend system hosting. 14. Facilitate in conducting Vulnerability Assessment with BTCIRT.
	System Owner	Concerned agency	1. Configure, maintain, manage, update, patch application/databases and operating systems(OS) hosted in GDC. 2. Ensure OS/application’s security compliance as per BtCIRT's baseline requirement(Annexure) 3. Patch and update application and OS vulnerabilities based on BtCIRT's security requirement. 4. Seek the support of the GDC team before making any major updates and changes to prevent system failure. 5. Seek storage, compute and network resources to host applications in the GDC. 6. Carry out migration of the application to GDC. 7. Consult with the GDC and BtCIRT team on security requirements of applications. 8. 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. 9. Agencies failing to patch due to incompetencies or lack of resources shall be responsible for securing their own funding or arrangement. 10. Liaise with the outsourced vendor and GDC team for consultation during the application development. 11. Liaise with the outsourced vendor and GDC team for resolving issues pertaining to hosting the application in GDC.

	GDC Technical Support Team	Technical team of concerned contractor	The responsibilities of the GDC technical support team will be as agreed in SLA. To highlight key responsibilities: 1. Configure and set up a 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. 5. Patch and Update OS of network devices(firewall, router, switches, storage). 6. Ensure the hardware contingencies are maintained throughout operation of GDC networks and services. 7. Monitor availability and utilization of server/storage/network resources. 8. Provide 24/7 or 9/5 support to GDC PMU to resolve pertinent, upcoming ad hoc issues. 9. Resolve issues raised through the GDC ticketing system as per terms and conditions stipulated in SLA. 10. Diagnose and rectify hardware problems. 11. Configure, maintain and monitor servers such as DNS, Log Server, NTP, NMS and other critical servers required to operate GDC infrastructure. 12. Submit reports as per Section 9- Reporting and Documentation

	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

12 Inventory Management

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

12.1 Hardware

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

12.2 Software Library

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

12.3 Service/Applications Catalogue

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

13 Configuration and Testing

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

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

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

14 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.

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 a maximum of 5 unsuccessful attempts to login into the system (from server side).

14.1 Minimum Password Length

Passwords shall have a minimum of 14 characters with a mix of alphanumeric and special characters.

14.2 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.

14.3 Password Management

14.3.1 Password Storage

Passwords shall not be 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.

14.3.2 Password Sharing and Transfer

Passwords shall not be transferred or shared with others.

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

14.3.3 Electronic Transmission

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

14.3.4 Password Recovery

In the event of losing passwords, a case shall be lodged to the GDC team through the GDC ticketing system. A temporary new password shall be issued , which should be changed after the first login.

15 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.

15.1 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.

15.2 Domain Name System

GDC services can be accessed through the Internet and Intranet (GovNet/TWAN). It is advised to use GovNet/TWAN DNS to access GDC services for better user experiences. Services within GDC are first advised to use in-country DNS than open global DNS.

15.3 Simple Network Monitoring Protocol

All servers and network devices 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.

15.4 Log Service

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

16 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

17 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 reasons.

D. Software version

The list is maintained separately for security reasons.

E. GDC Service Catalogue

left blank intentionally

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