GENDER LINKS
FOR EQUALITY AND JUSTICE

INFORMATION TECHNOLOGY POLICY AND PROCEDURES

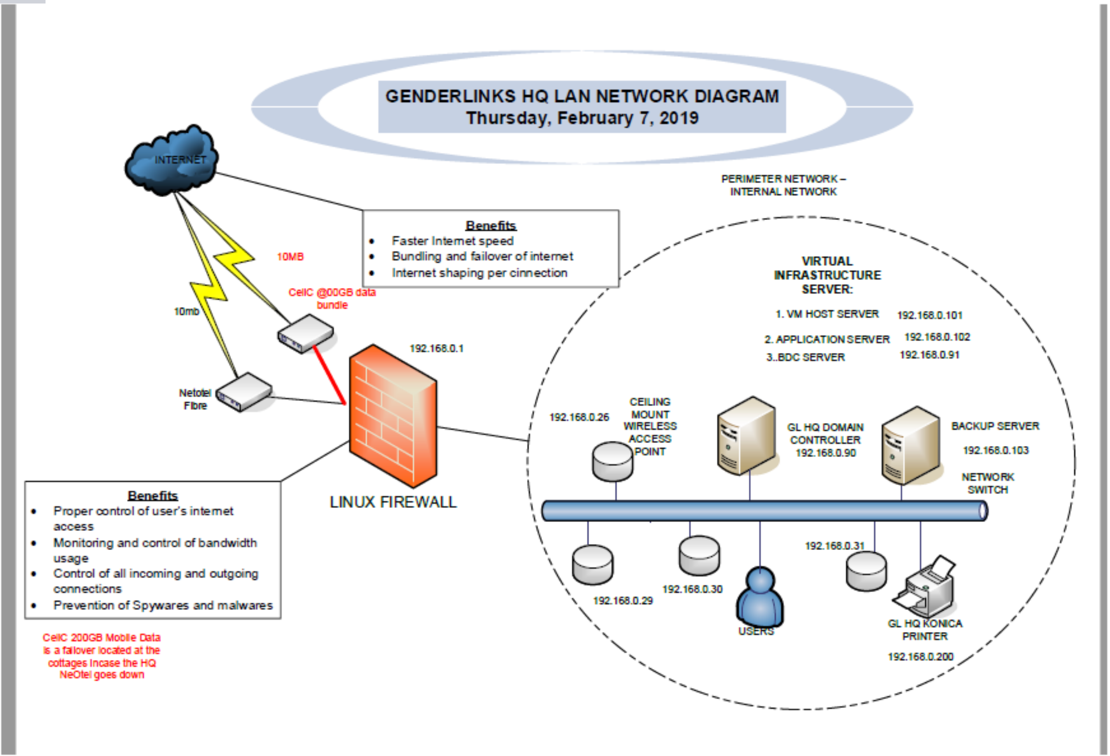
These Policies and Regulations take account of the laws prevailing in all the GL countries of operation. Should there be a contradiction between the Policies and Regulations and national laws, the later will take precedence except where, in the interest of fairness policies have been standardised across countries.

ACRONYMS	
SNB	Sinebhongo Technologies
DOO	Director of Operations
D&S	Desktop and Server
GL	Gender Links
NET	Networks
SA	Site Account
SD	Service Desk
CCC	Command And Control Centre
LPC	Local Production Centre

I. SECURITY

General

1. IT is a critical tool for the achievement of the GL mission and vision, as well as for cost savings and ensuring maximum efficiency. Covered in this Policy document are the Information Technology Policies and Procedures.



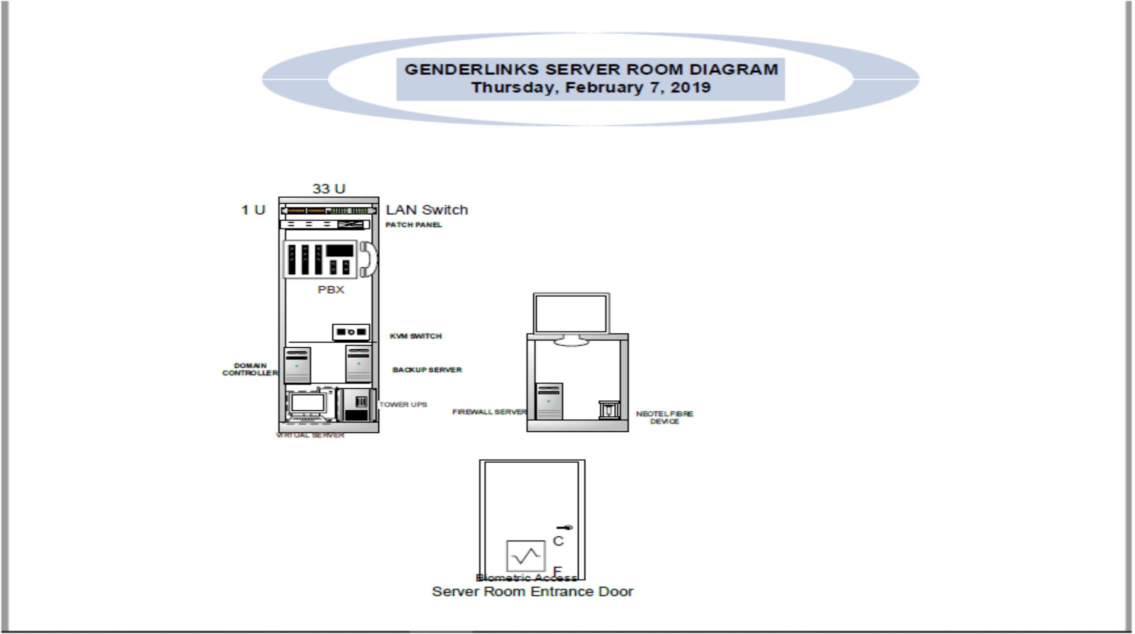
GENDERLINKS HQ LAN NETWORK DIAGRAM
Thursday, February 7, 2019

Benefits
- Faster Internet speed
- Bundling and failover of internet
- Internet shaping per cinnection

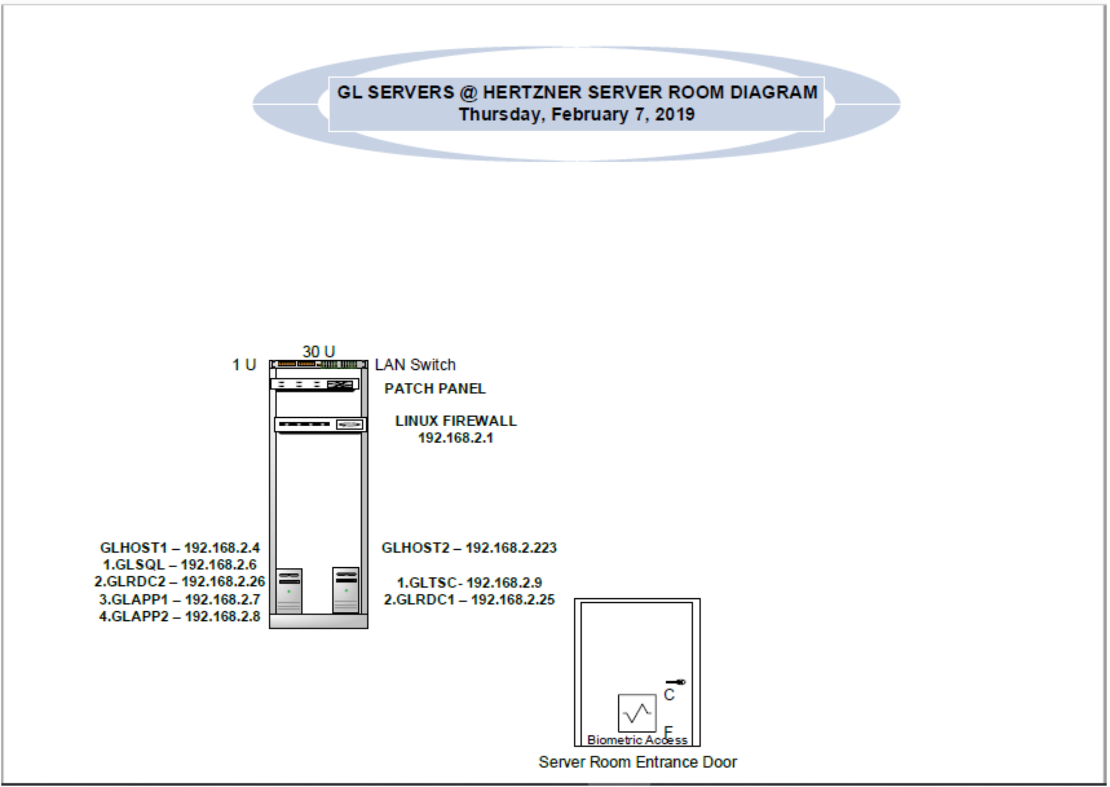
Benefits
- Proper control of user's internet access
- Monitoring and control of bandwidth usage
- Control of all incoming and outgoing connections
- Prevention of Spywares and malwares

CellC 200GB Mobile Data is a failover located at the cottages Incase the HQ NeOtel goes down

INTERNET
10MB
10mb
CellC @00GB data bundle
Netotel Fibre
192.168.0.1
LINUX FIREWALL
PERIMETER NETWORK – INTERNAL NETWORK
VIRTUAL INFRASTRUCTURE SERVER:
1. VM HOST SERVER 192.168.0.101
2. APPLICATION SERVER 192.168.0.102
3..BDC SERVER 192.168.0.91
192.168.0.26
CEILING MOUNT WIRELESS ACCESS POINT
GL HQ DOMAIN CONTROLLER 192.168.0.90
BACKUP SERVER
192.168.0.103
NETWORK SWITCH
192.168.0.29
192.168.0.30
USERS
192.168.0.31
GL HQ KONICA PRINTER
192.168.0.200



GENDERLINKS SERVER ROOM DIAGRAM
Thursday, February 7, 2019



2. Every GL staff Member must undergo orientation on GL IT Protocol.

3. Failure to adhere to the provisions of this policy may result in the suspension or loss of access to GL resources.

4. Should an individual's access be suspended, GL shall inform the individual immediately and shall afford the individual an opportunity to respond. GL shall then determine whether some alternative course of action, is warranted and shall follow the procedures established for such cases.

5. Any IT-related service calls that are not of a routine maintenance nature shall be authorised by the Director of Operations.

6. GL can contract IT companies and service providers for the provision of IT and related services who shall be referred to as IT Service Provider(s) or Systems Administrator(s).

Gender Links Information Security

7. The security at GL shall be guided by the principles of confidentiality, integrity and availability.

8. Users shall be created by IT Service Provider. The IT Service Provider will consult the Director of Operations to determine on which workgroups in

the domain the user shall belong to, based on the shared folders that each user can access.

9. Access to the shared folders like the main One Drive and SharePoint will be limited to Users unless they fall under site admins. The rest of storage site will be on read only basis by users without admin rights.

10. A weekly and monthly domain activity report (containing security Audits, user activities, Phishing campaigns and Malware detections) shall be prepared by the IT Service Provider to be signed off by Director of operations.

11. The online storage facility or SharePoint, contains information about Gender Links and its operations, its customers, products, supplier information, and its managers and employees. It must therefore be securely managed with monthly routine change of access passwords.

12. This information is classified as confidential and sensitive information and may not be accessed unless for work related to the user role, and no other information may be accessed without written explicit and specific management permission.

13. Users who come into possession of such information may not disclose this to any other person without written explicit and specific management permission.

14. No user may make any statement to any form of external media – including placing information on the Internet – without the written explicit and specific management permission.

Passwords and Security

15. All users are issued with an individual password which will provide the access to the systems, such as Pastel Evolution, VIP Payroll, Pastel Server, Microsoft Outlook and SharePoint, Survey Gysmo, appropriate to the user's role. It is the responsibility of the user to ensure that their password is secure from external users and changed on a monthly basis, and that the password is not shared.

16. User access is given for the purposes of the user performing a defined role, and no attempt should be made by the user to gain any additional access to the information systems.

17. The password should be kept secret and not given to any other user.

18. Any contravention of policy while using the password will be deemed to be a breach of the policy by that user.

19. Users should ensure that they log out of their systems they may be working on when moving away from their desk or when working on machines outside GL Offices for any purpose.

Passwords and Authorised Access

20. Only GL staff members are allowed to use the computers and their laptops that are linked to the domain. The Internet Service Provider in consultation with DOO, may authorize access to the Guest computers or pool laptops.

21. All staff members shall be supplied with E Mail addresses; shall be required to be conversant with its use and with use of the Internet; shall be required to run weekly virus checks on their computers and report any dysfunctional computers to the Systems Administrator when necessary to ensure these are attended to or un order to receive appropriate advise if it's a personal laptop requiring personal repair work.

22. All user-level and system-level passwords must conform to the *password construction guidelines*. **(See Annex A)**

23. Password cracking or guessing may be performed on a periodic or random basis by the IT Service Provider. If a password is guessed or cracked during one of these scans, the user will be required to change it in order to comply with the password construction guidelines.

24. Passwords must not be inserted into email messages, or other forms of electronic communication.

25. **Do not use the "Remember Password" feature of applications (for example, web browsers).**

26. **Application development:** GL application/survey developers must ensure that their programmes contain the following security precautions and that applications must:
    - Support authentication of individual users, not groups.
    - Not store passwords in clear text or in any easily reversible form.
    - Not transmit passwords in clear text over the network.
    - Provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

27. Users will not use another person's computer account without permission. Passwords will be kept private and users should not allow unauthorized use of their accounts.

28. GL computing infrastructure and facilities are for GL purposes only; these purposes include administrative, instructional, and professional activities (e.g., research) integral to the mission of the organisation.

29. Use of the Internet at the office for any purpose other than work related is strictly prohibited. In particular surfing of the Internet for pornography is forbidden and constitutes a grave disciplinary offence. Should a

supervisor or the CEO have any cause to believe that the Internet is being abused, he or she is entitled to obtain information on how particular staff members are using the Internet from the systems Administrator and to take action accordingly.

30. GL computing facilities and networks cannot be used for personal business or compensated outside work, or for the benefit of organizations not related to GL except in connection with scholarly pursuits (e.g. organization publishing activities), consulting activities, and services that do not violate GL or GL policies or State regulations and laws.

31. The origination of "junk mail," chain letters, or otherwise flooding the network with huge volumes of unsolicited electronic mail is not appropriate use of network resources and will not be tolerated. GL reserves the right to permanently block unwanted mail and further suspend email addresses sending out Spam.

32. GL shall monitor Internet usage on a monthly basis per user, and shall raise any excessive or inappropriate use of the Internet with users in accordance with rules set out here, and take disciplinary action as appropriate. GL reserves the right to charge for excessive inappropriate use of the internet that has no relation to the work of the organisation during working hours. GL further reserves the right to block websites that are purely of an entertainment nature or that contradict the values of the organization that feature in the 100 most visited websites in the monthly statistics.

33. GL reserves the right to block use of certain Internet websites that have no relevance to its work and which records show are being excessively visited by staff against the principles of the organization, or to the detriment of time management. Examples are dating sites, Movie and Music Download sites as well as pornography sites.

34. Information stored on the GL server is deemed to be private and confidential. Logins and passwords are confidential and cannot be shared with anyone outside the organisation. Anyone who is found to be in breach of this condition will be subject to GL’s disciplinary procedure.

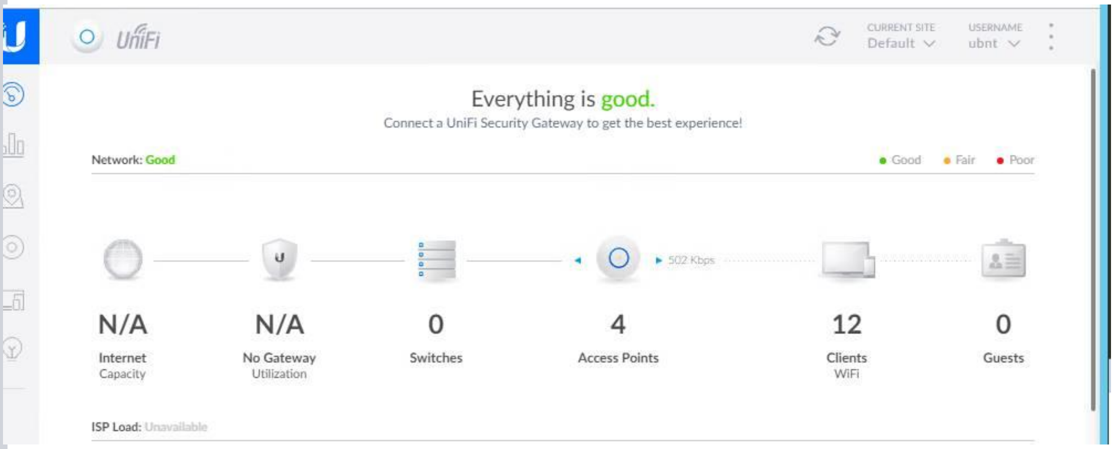
Set-up of Guest Network and Access

35. The System Administrator shall connect all external users and devices to the GL guest network upon authorisation.

36. The systems administrator shall ensure that Password for Guest Network must be changed on a monthly basis. Should there be a security breach or unauthorised access to the network, a new password must be effected immediately.

37. GL Geust network separates guests from Office Staff. The password to access the Guest network is knowledge.2019

38. The Overview below will always indicate how many users or guests are connected



Everything is good.

Connect a UniFi Security Gateway to get the best experience!

Network: Good

● Good ● Fair ● Poor

N/A Internet Capacity

N/A No Gateway Utilization

0 Switches

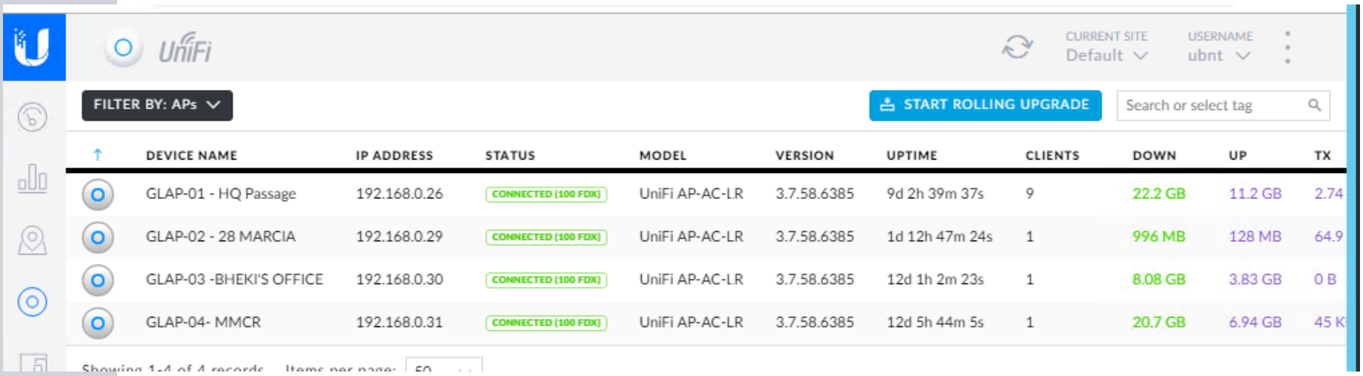
4 Access Points

12 Clients WiFi

0 Guests

ISP Load: Unavailable

The below will show how much is been downloaded by users and guests with live monitoring capabilities.



↑	DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION	UPTIME	CLIENTS	DOWN	UP	TX
	GLAP-01 - HQ Passage	192.168.0.26	CONNECTED (100 FDX)	UniFi AP-AC-LR	3.7.58.6385	9d 2h 39m 37s	9	22.2 GB	11.2 GB	2.74
	GLAP-02 - 28 MARCIA	192.168.0.29	CONNECTED (100 FDX)	UniFi AP-AC-LR	3.7.58.6385	1d 12h 47m 24s	1	996 MB	128 MB	64.9
	GLAP-03 -BHEKI'S OFFICE	192.168.0.30	CONNECTED (100 FDX)	UniFi AP-AC-LR	3.7.58.6385	12d 1h 2m 23s	1	8.08 GB	3.83 GB	0 B
	GLAP-04- MMCR	192.168.0.31	CONNECTED (100 FDX)	UniFi AP-AC-LR	3.7.58.6385	12d 5h 44m 5s	1	20.7 GB	6.94 GB	45 K

Showing 1-4 of 4 records Items per page: 50

Encryption Key Security and Integrity

39. Employees (other than management in the circumstances mentioned above) are prohibited from the unauthorised use of the password and encryption keys of other employees to gain access to the other employee's e-mail messages.

Violations

40. Management will investigate any alleged contraventions of this policy, and all users are required to report any contravention of the policy which comes to their attention. Appropriate disciplinary action will be taken against any user found to have contravened the system and this may lead to dismissal, or termination of a contractor contract. If necessary, Gender Links also reserves the right to advise appropriate legal officials of any illegal violations.

II. DOCUMENT MANAGEMENT

SharePoint

41. All documents generated within the organisation or received must be filed in one drive on the desktop of the individual employee's computer and must be synchronised to mirror files in SharePoint. This forms the basis of organisation filing system and back-up of organisational data and information.

42. ***SharePoint Online***. This is the public online drive on which all public documentation and reports are stored, this enables all staff to have access to any of the programme work, institutional information, administrative information etc. This is a cloud-based service, hosted by Microsoft, for businesses of all sizes. Instead of installing and deploying SharePoint Server on-premises, Gender Links has subscribed to an Office 365 plan, which is an online service.

43. Any information that relates to the organisation should be put onto SharePoint and OneDrive in its final form so that it can be accessed by anyone when it is needed.

44. **OneDrive for Business sync.** This is a desktop and online program that Gender Links uses to sync documents from a team site or OneDrive to computers for offline use. It is the duty of the systems administrator to ensure that all users are granted access to sections of the team site. Some sites may contain confidential information and therefore have restricted access.

45. The Internal Public files on the Intranet are:
    1. Strategy, Planning & Funding
    2. Governance
    3. Communications
    4. Finance, HR & IT
    5. Programmes
    6. Results for Change
    7. GL Services and Cottages
    8. Country Offices

Naming files

46. GL has developed a file naming system for all word and image files. It is:

47. What the file is about_initials of originator and reviewer_date.

48. EG: QuickguidetoGL_bnclm_05022019

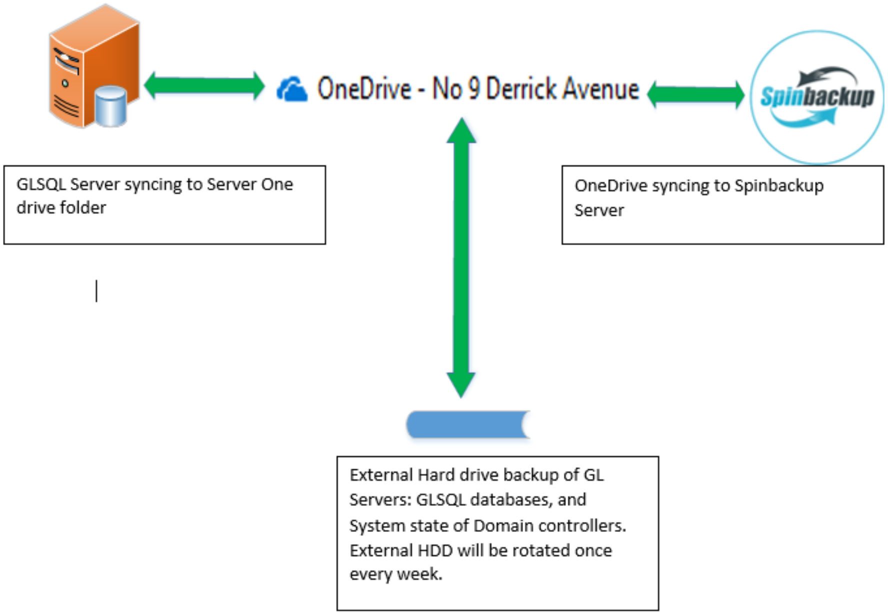
III. BACKUP

49. Backup Server is Running Symantec Backup Exec 2010 R3, Windows Server Backup, Disk2VHD and VEEAM Backup software for Hyper V

50. SNB IT Administrator will be responsible for making backups of data stored on the entire GL Servers. Backups are made on to local drive daily and weekly, then transferred to an external HDD for offsite backup. These backups are made according to a schedule. The Grandfather/Father/Son rotation scheme will be used to make data backups.

51. All critical data must be stored in GL Systems, Departmental Directories or User Directories on the provided Servers Storage, otherwise such data cannot be backed up. If Server Storage is not available then arrangements must be made with Unit or approach SNB to investigate or provide.

52. SNB will not take responsibility for data lost from Desktop's or Notebook's hard drives, nor personal or illegal data / files stored on Server Storage.



GLSQL Server syncing to Server One drive folder

OneDrive syncing to Spinbackup Server

External Hard drive backup of GL Servers: GLSQL databases, and System state of Domain controllers. External HDD will be rotated once every week.

Daily Backups

53. These backups are made daily from Monday to Thursday. The Daily External Hard drives are replaced daily at 8am (Mon – Thurs). This process is used to backup all information or data stored on Servers as per the ***BACKUP FILE SELECTION*** section that have been modified since the last ***FULL*** backup. A cycle of one (1) Media set is used, thus one can recover data with a maximum of eight 8 working days.

Weekly Backups

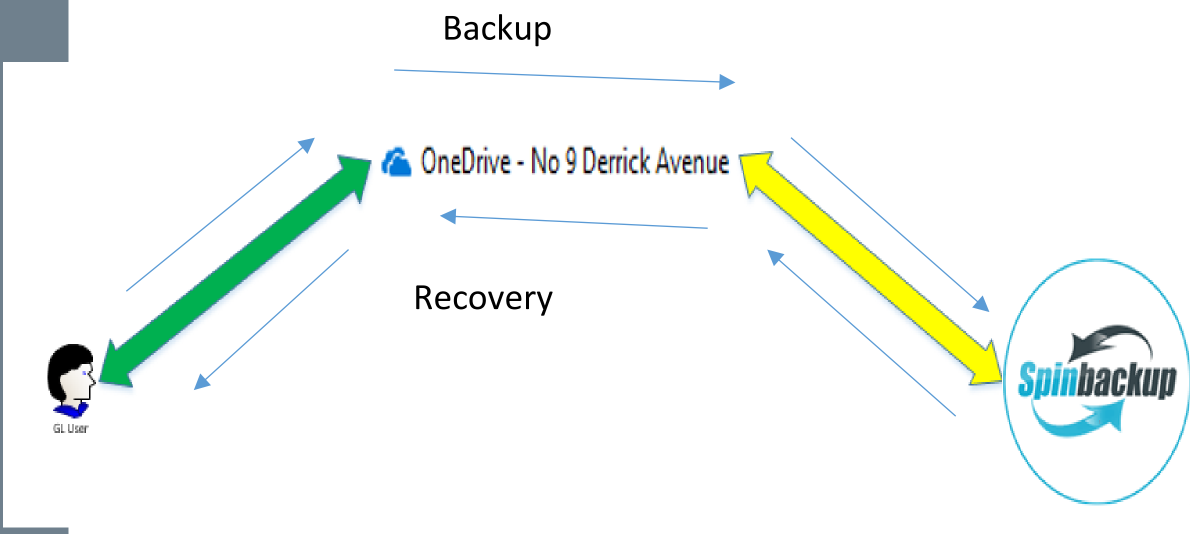
54. These backups are run every weekend with the exclusion of Monthly Backups. This process is used to backup all information or data stored on Servers as per the ***BACKUP FILE SELECTION*** section. A cycle of three (3) Media sets are used per month, thus one can recover data with a maximum period of three (3) weeks. Weekly External hard drives are replaced every Friday at 8am.

Monthly Backups

55. These backups are made once a month on the last weekend of the every month. The process is used to backup all information or data stored on Servers as per the ***BACKUP FILE SELECTION*** section. A cycle of twelve (12) Media sets are used annually; hence one can recover data with a maximum age of 12 months. Monthly External hard drives are swopped once a month for backup.

One drive backup

56. All GL data are to be saved on their corresponding OneDrive folder for each user, each server will have a OneDrive account to sync across their backups to the GL Office 365 platform and also automatically synced to a 3rd party Service provider – SPINBACKUP. Spinbackup allows recovery of the latest Folders in case of ransomware attacks.



Backup media changes

57. Weekly and Monthly backup media must be changed (removed) from the backup drive every Monday morning and new drive media for the scheduled Weekly or Monthly backups must be inserted and labelled.

58. Media for daily backups must be changed when needed and a new media inserted before the next daily backup.

	Backup Selections - AD – (Daily, Weekly, Monthly)			
Job	**Server**	**Folders**	**Sub Folder**	**Location**
GLDRDC Daily, Weekly, Monthly	**GLDRDC**			
		System State	**All**	**Q:\SYSTEM STATE**
GLDRDC1 Daily, Weekly, Monthly	**GLDRC1**	System State	**All**	**Q:\SYSTEM STATE**
GLHQDC2 Daily, Weekly, Monthly	**GLHQDC2**	System State	**All**	**Q:\SYSTEM STATE**
GLHQDC1 Daily, Weekly, Monthly	**GLHQDC1**	System State	**All**	**Q:\SYSTEM STATE**

	Backup Selections - Users Data & SQL (Daily, Weekly, Monthly)			
Job	**Server**	**Folders**	**Sub Folders**	**Location**
GLSQL Daily, Weekly, Monthly	**GLSQL**	Entire VHD		**Q:\SQL**
GLAPP2 Daily, Weekly, Monthly	**GLAPP2**	C:\DATA\	**ALL**	**Q:\APP2**
		Entire VHD		

	Backup Selections – Pastel and Payroll– (Daily, Weekly, Monthly)			
Job	**Server**	**Folders**	**Sub Folders**	**Location**
GLTS - Daily, Weekly, Monthly	**GLTS**	C:\EvoData	**ALL**	**Q:\GLTS**
		Entire VHD		**Q:\**
GLAPP1 – Daily, Weekly, Monthly	**GLAPP1**	Entire VHD		**Q:\GLAPP1**

	Backup Selections – Applications– (Daily, Weekly, Monthly)			
Job	**Server**	**Folders**	**Sub Folders**	**Location**
GLHQAPPSRV1- Daily, Weekly, Monthly	**GLHQAPPSRV1**			
		Entire VHD		**Q:\GLHQAPPSRV1**
	GLHQHST1	System State		**Q:\GLHQHST1**

Backup Selections – Pastel – Firewall (Daily, Weekly, Monthly)				
Job	**Server**	**Folders**	**Sub Folders**	**Location**
GLFW-DC - Daily, Weekly, Monthly	**GLFW-DC**	XML Backup	**ALL**	**Q:\GLFW-DC**
		Entire VHD		
GLSA – Daily, Weekly, Monthly	**GLSA**	XML Backup	**Entire**	**Q:\GLSA**

Backup media storage

59. All Media must be

- Stored offsite
- Sent to external backup site every week on Tuesday.
- Labelled properly and comprehensively.
- Recorded in a log book of all backup media must be completed for any media that is sent to backup site

Controls to ensure procedure is carried out consistently

60. Ad-hoc testing procedure:

- User logs a call to request for a file restoration specifying relevant details.
- The backup administrator obtains an appropriate backup Media.
- The file get restored as per user's specification
- The user is contacted to verify the status of restoration.
- In case of an unsuccessful data restoration, the problem must immediately be investigated and correctional action taken.
- The Media must be taken back to its original location.

61. Monthly testing procedure:

- ○ Backup / Restore tests should be done on the first Tuesdays of every month.

- Two restore tests must be done:
- User or Departmental Data to "OFFLINE" Storage i.e. Disaster Recovery Server
- Exchange Mailbox Store to "OFFLINE" Storage i.e. Disaster Recovery Server
- In case of an unsuccessful data restoration, the problem must immediately be investigated and correctional action taken.
- The Medias must be taken back to their original location.

Corrective action

62. A failed full backup (Monthly or Weekly backup) must be rescheduled to run the same day on which it is discovered to have failed.

63. Daily Medias should not fail for more than 2 days in succession otherwise the cause of the failure must be investigated immediately and corrective action must be taken and documented.

64. If a backup is not successful due to a Media hardware component failure, it will be investigated, restored to operational use, and tested. (A data recovery of at least 1 GB in size must be done).

65. Assigned drive may change on the External Hard drive backups due to drive replacement.

IV. EQUIPMENT AND SOFTWARE

66. All equipment must be recorded in the equipment register kept by the Finance Officer under the guidance of the Director of Operations.
67. Staff must communicate with the Finance Officer when they need equipment at least a day in advance so that it can be made ready e.g. one may need to use the camera but maybe the memory card is full so Finance Officer needs to test and prepare the gadget for use.
68. Staff must sign for the equipment upon collection and upon return.
69. If one is traveling over the weekend, equipment must be collected on Friday so that Finance Officer does not share the cupboard keys with anyone.
70. All equipment must be returned after immediately after use.
71. Any staff with laptops must sign for these and abide by the rules in GL policies and rules.

Copier and Scanner

72. Copier only for light copying. No books and bulk workshops or meetings material shall be photocopied but service outsourced.

Computers

73. No personal videos, photos, music stored on Gender Links computers or laptops.

74. Each staff responsible for computer care and ensuring that weekly virus check is performed.

Internet

75. Usage monitored and GL reserves right to block websites that bears no relation to our work.

- Monitoring internet usage

Call Logging Process / Request for IT Service Provider Assistance

76. All calls must be logged via the helpdesk on the email IT@sinebhongo.com. In all requests, please copy the Director of Operations (finmanager@genderlinks.org.) This will assist with HQ intervention and facilitation by phone call if required and will keep the DOO informed of the progress on the matter and when its resolved.

77. Where email facility is no longer available, use of another officer email or other available email facility or by phone to Helpdesk hotline: +27 10 100 3880

78. When sending support request, please provide the following information to enable IT Service Provider to service your call more effectively:

- On the subject, include a brief and precise description of the problem
- Company Name
- Your name
- Your phone number
- Brief description and impact of issue.

Equipment Use

79. GL may issue equipment to members of staff requiring these for their work.

80. All GL office equipment shall be used for GL business only.

81. All staff in possession of GL equipment must sign a form taking responsibility for the equipment **(See Form IT1: GL equipment form).** Damage to and loss of equipment due to negligence of a staff member shall require the staff member to replace or pay GL the value of the equipment.

82. Staff are responsible for taking due care of GL equipment including:

- Ensuring that these are ALWAYS carried as hand luggage on aeroplanes.
- Stored safely.
- Have valid anti-virus software that is regularly updated and runs regular
- Never left unattended.
- GL reserves the right to recover any costs or losses that may result from negligence in the care and security of office equipment.

- Equipment owned by GL shall under no circumstances be taken away from the office at any time for use other than for GL designated work and events.

83. Office equipment and software shall be signed out by the Finance Officer under the guidance of the Director of Operations and returned accordingly.

84. Office equipment and software shall be locked up at all times. It is the responsibility of the Finance Officer under the guidance of the Director of Operations to ensure that this is done and to keep the key in a safe place.

Ownership and insurance

85. Gender Links shall maintain in the asset register all IT equipment that the company has ownership of or title enabling the organisation to enjoy full use of.

86. All GL offices shall ensure that all IT equipment is comprehensively insured with reputable insurance provider companies.

87. The following conditions apply to personal laptops not owned by GL:

- GL is not in a position to insure self-owned lap tops because the premium on such is extremely high and may exceed the replacement value.
- Staff using their personal or company owned laptops on GL premises are expected to exercise maximum caution including using the security cord; never leaving laptops on their desks at the end of the day or at weekends when they are away from the office; and locking their laptops away in cupboards to which they keep the keys when they are out of the office for extended periods.
- In the event that a self-owned laptop is stolen from the GL premises or on GL business even after all the above have been observed and in the assessment of the CEO the loss is not the fault of the staff member concerned GL will replace the laptop to a maximum amount of the market value of the laptop at the time of its being stolen.
- GL bears no responsibility for a self-owned laptop that is stolen away from the office premises.
- As important, if not more important than the laptop itself, is the data contained that often represents an invaluable amount of time and work paid for by GL. Therefore a critical condition of any laptop use (and part of the loan agreement) shall be that the staff member concerned backs up their data weekly to One Drive. Managers responsible for sections of the Intranet

Care and maintenance

88. Copying of large personal files (especially audio visual files) onto GL computers is prohibited.

89. Routine maintenance on laptops and computers should be conducted by IT Service Provider. It is the responsibility of every staff member to notify the IT Service Provider when computers or printers are not working properly. Individuals shall take equal care of their laptops.

90. Eating and drinking in close proximity to computers is not allowed at any time.

91. Connection of personal equipment to the GL network without permission from the Director of Operations is prohibited.

92. Copying or removing software from GL equipment is prohibited.

93. Computers must be switched off after use. In the case of the GMDC lab, the station must be left ready for the next patron. Leave the monitor on the login screen, pick up all your papers and push in your chair.

94. It is the responsibility of all staff to ensure that their computers and laptops have the latest anti- virus installed.

95. It is the responsibility of the IT Service Provider to ensure that the anti virus is programmed to run a full system scan every week.

96. The IT Service Provider shall be responsible for ensuring routine maintenance of equipment including virus checks.

Protection of Intellectual Property

97. GL has the responsibility to uphold software license provisions and copyright laws for the software that is officially installed and the publications officially posted on the Organization network.

98. The organisation cannot accept responsibility for unofficial software installations, publication postings, and messages that are the acts of private individuals acting in a private capacity. The organisation will, however, remove software or publications from its network and computing facilities whenever it discovers their installation constitutes copyright violation, piracy, or other form of malfeasance.

V. DISASTER RECOVERY

99. In the event of a complete network failure, power cut, server breakdown, fire or any other eventuality where the network is unavailable, a disaster plan needs to be in place to ensure the continued running of the organisation.

100. The following emergency procedures need to be in place: To ensure that operations and other critical management systems can still run, the member of staff responsible for these areas should ensure that they have their own disaster recovery plan. This will enable them to continue working at the individual level. The person responsible should adhere to the following guidelines in formulating their own disaster recovery plan:

- Identify essential management functions that must take place in order to support an acceptable level of continuity for the organisation.
- Document procedures to implement this disaster recovery plan.
- Make sure the plan can work effectively in the event of a disaster.
- Make sure staff who work within these critical management areas are aware of the plan and are able to carry it out.
- Plan for the alternate processing of data to use during a disaster. This would include keeping hard copies of certain data and documents and documentation of any disaster plan.

101. When the server and network have been restored any new information can then be transferred or entered back into the network system. If a user on the administration network needs to load up an important document, this should be possible since extra backups are made independently of the network servers. A user could then work locally (not attached to the network) on their desktop PC or laptop with that document.

102. To provide the maximum protection against the possibility of server failure, Gender Links policy states that all network servers purchased, have built in fault tolerance mechanism.

Server backup and restoration:

103. Each server is backed up every weeknight. This backup includes the server operating system, configuration files, and in the case of the Primary Domain Controller, this would include network data such as usernames, policy and profile data and security information.

104. In the event of complete server operating system failure, the system would initially need to be re-installed and then the server backup restored. In the event of server hardware failure, the server would first need to be repaired, then the server backup restored.

Data restoration

105. Only the Systems Administrator, and authorised personnel will have access to means to restore network data. The Systems Administrator will determine if a successful restoration is possible.

106. Any requests for restoration of user data will be made to the System Administrator. In the event of complete server failure where a full restoration of organisation management software and data files is necessary, the CEO or a member of the Board will need to give approval.

Alternative accommodation

107. GL will keep an up to date register of all locally available office premises. This register will be kept off-site and can be used to find available office space for the continuation of the organisation, in the event that the Disaster Recovery Plan has to be implemented.

Policy Compliance

108. DOO, with the assistance of the IT Service Provider will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, network monitoring, internal and external audits. GL CEO must approve any exception to the policy in advance.

VI. ANNEXURES

ANNEX A. PASSWORD CONSTRUCTION GUIDELINES

1. Purpose

The purpose of this guide is to provide best practice for the creation of strong passwords.

2. Scope

This guideline applies to employees, contractors, consultants and temporary workers at GL, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

3. Statement of guidelines

All passwords should meet or exceed the following guidelines:

Strong passwords have the following alphanumeric characteristics:

- At least 8 characters.
- Both upper and lower case letters.
- At least one number
- At least one special character or symbol (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor or weak passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation. ***(NOTE: Do not use either of these examples as passwords!)***