Garib Unnayan Sangstha (GUS)
Humanitarian Cooperation- according to need

Garib Unnayan Sangstha (GUS) IT Policy and Guideline

1. Equipment Policy

a. All IT Equipment and resources owned by GUS are under IT Section custody.
b. All employees must use the laptops/others given by the GUS for the official purpose.
c. Acceptable use and code of conduct.

2. Software Usage Policy

a. All software must be purchased or acquired through the IT section, including authorization and obtaining the necessary licenses for such software.
b. GUS laptop/desktop is installed with a licensed Microsoft Windows Operating system, MS Office, antivirus and some standard system software regardless user's designation.
c. The installation of software without the approval and assistance by the IT Section is prohibited.
d' User is also prohibited from installing any games, utilities, and personal software on GUS Laptop Computers.
e. User is not encouraged to download any of the following file format (ending with extension) *.dat *.mov *.pif *.bat *.exe *.wma *.mp3 *.avi *.xvid *.wav *.Inl

3. Antivirus Policy

a) ICT section will provide antivirus software installed to protect GUS information assets from malicious software.
b) Antivirus system will automatically scan and update all laptop/computers that connected to internet based on schedule configure.
c) All laptop/computers should run the latest antivirus software as approved ICT section.
d) E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail that may contain virus.
e) User must exercise caution when coping files. Only download from reputable sites.
f) User must exercise caution when opening / copy file from removable media such as USB drive, memory stick, CD-ROM or portable hard drive. All removable media should be scanned for viruses before being used.

4. Email Usage Policy

a. Email eligibility will be assessed based on requestor's functional dependency; HR section is responsible for verifying staff eligibility consistent. Exception approval must be endorsed jointly by AD- HRM, and Director
b. Email is must be GUS own domain like; latifgus@gmail.com and also Gmail ID selected format by latifgus@gmail.com
c. Email should be used for official work related communication only.

d. Email should be checked on daily basis.
e. Users shall not send attachment larger than approved as per approval email limit which is l5 MB to external and internal recipient.
f. Proper security measures must be taken when sending confidential information.
g. All Users that provided with GUS official email accounts is not allowed to use web mail applications such as Outlook, Hotmail and group mail.
h. Do not use Organization's email when posting to public newsgroup, blogs and forum unless authorized and acknowledge by the communications.
i. User must exercise extreme caution when opening attachments and scan for virus.
j. User should use Inbox as a temporary store for mails. Delete any unwanted emails.
k. Regularly clean out Deleted items/ Trash folder and sent items folder"
l. Must not open email file attachments received from unsolicited or entrusted sources.

5. Internet Usage Policy

a) Access to the Internet is made available only to authorized user and registered visitors, All visitors need to access internet must register to IT section and subject to approval by the Head of ICT
b) Access to Internet services is permitted for official purposes and limited personal use subject to management discretion and acceptable and proper use.
c) User is strictly prohibited from using GUS internet facility for the reasons mentioned Below but not limited to:
i. Downloading of video or music files
ii. Downloading software not relevant to official work
iii. Downloading and execute non-licensed software at official work
iv. Downloading of any copyrighted materials belonging to third parties
v. Visiting Internet sites that contain obscene, racist, hateful, or pornographic material
vi. Visiting Internet that contain violence, weapons, terrorism or militant material
vii. Using the Internet to send offensive, defamatory or harassing material to other USETS
viii. Using the laptop/computer to perpetrate any form of fraud, or software or music piracy
ix. Hacking into unauthorized areas
x. Online gaming
xi. Online gambling
xii. Online auctions
xiii. Undertaking deliberate activities that waste staff effort or networked resources
xiv. The deliberate or negligent introduction of any form of computer virus into any GUS IT System or network
d) No user is allowed to use GUS IT resources to access 'blogs' discussion groups, home pages etc.
e) No user is allowed to install and utilize any instant messaging, with VoIP (voice over Internet Protocol) program such as program such as Google Talk (GTalk;, Live Messenger etc. through GUS IT Internet facilities. Any need for such installation Must approve. By Director and IT personnel only.
f) All Internet access within GUS Internet facility is subject to monitoring as set out by the IT section and monitoring procedures. User should therefore have no expectation of Confidentiality in the use of the GUS Internet facilities.

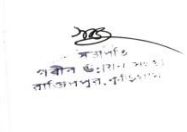
g) Any official purchasing requirement or procurement exercise can only be taken forward by the procurement unit in line with business procedures.
h) IT Section have right to physically or remotely access user's laptop/computer at any time, without notifying user for monitoring purposes.

6. Network Access Policy:

a) All authorized users are eligible to access the corporate LAN with an assigned Ip address as long as the usage is in accordance to GUS policy.
b) IT section reserve the right to withdraw any connection without prior notices to user when there is a breach of policy.
c) WiFi access must be setup/configure by IJ section only.
d) Connections to the corporate network from are limited to end-point devices such as Laptops, printers, scanner or other terminating devices us pre-approved by Head of ICT.
e) No user is allowed to modify or extend the network in anyway by installing devices such as personal switches, hubs, routers. Gateway or wireless access points. These additional unmanaged connections strictly prohibited.

7. Data Access and Usage Policy

a) Privilege to access server host applications such as email and others centrally managed and administered by IT section.
b) User access is controlled by unique user ID and password.
c) Each laptop user is automatically authorized to access his/her functional departments shared file folder. Exception to view other department's folder must be endorsed by the data owner and Head of IT.
d) Only authorized lT personnel/IJead of IT have the right to ask for user password in the Case of investigation.
e) Password should be reset at least once in every 3 months.
f) Do not use function such "remember password", "Always signed in,, on any the Or animation' s app I i cation/systems.
g) User should not read, copy, change or delete other user's file or software without explicit agreement by the owner.
h) User should not have expectation of personal privacy in any use of IT facilities, Messages or other data created, transmitted, stored on the organization's IT resources.



Md. Abdul Latif
Executive Director
Garib Unnayan Sangstha (GUS)

Md. Sajedul Islam
Chair person- Board of Trustee
Garib Unnayan Sangstha (GUS)