IT POLICY

a) Internet Usage

- All applications for Internet account must be done by submitting the Internet Access Request Form with proper approval obtained from department head and factory manager for tracking and recording purposes.
- Internet access restricted to Managers and Exempt Staff authorization upon factory manager approval.
- Internet account is strictly for the applicant own use only, no sharing of account is allowed.
- The account owners are fully responsible for all the files and software downloaded and all others transactions made via their account.
- The account owners will be responsible for all legal proceedings brought against them by themselves should it arises and company will not be responsible for any legal proceedings that may be brought against them.
- All the activities and transactions of the account will be logged.
- Company's management reserves the rights to approve and reject any Internet access applications.
- Surfing on the Internet is restricted to company's business purposes only. Illegal sites e.g. pornographic, terrorist-related, gambling, games etc. are strictly prohibited.
- Using instant messaging software & media streams for non work-related or personal are not allowed.
- File downloading from Internet is prohibited unless prior approval is obtained from the management.
- Company's management reserve the rights to review employees' Internet usage and to disclose the information without any notification to or permission from the employees sending or receiving the files. Company's management reserves the rights to deny users' access to external Internet sites that serve no legitimate business purpose.
- Company's management will perform investigation of suspicious or unusual Internet activities and report findings.

b) Email Usage

- Email users with authorized accounts and permission from department head and factory manager are only allowed to use email system for official company business.
- Email account restricted to supervisor level and above only.
- Users are not allowed to discloses sensitive and confidential information through e-mail.
- Users should not allow any person to use their password or to share account except for those meant to be shared. It is users' responsibility to protect their account from unauthorized use.
- Users are liable/responsible for all actions related to their account by changing password periodically and using password that is not easily guessed are highly recommended.

- Any attempt to circumvent system security, guess other passwords, or in any way gain unauthorized access to other's email account is forbidden.
- Transferring copyrighted materials to or from any system or via the email system without express consent of the owner may be a violation of Federal Law and is a felony under State Law.
- Email users are expected to maintain a high standard of ethical conduct while using the system. This means users are not to bring embarrassment, or harm that would distract from the good reputation of any affiliated group.
- Chain letters are clearly an annoyance to most users in addition to being a waste of technical resources and potentially illegal.
- Users who receive unsolicited chain mail should report the incident to email administrator.
- Users who forward chain email should be aware that their user names will be appeared in the forwarding path.
- The maximum file size (including attachments) sent to any user, may be internal or external, will be limited to 2MB at all time.
- All subscriber/enrolment to any Internet news group/discussion group/listserver are highly prohibited. The control is required to enable smooth email traffic transmission & allow solely for email, which respect to company related business only.
- Users are reminded to use the email as and when is necessary only. Any misuse of company time is highly prohibited.
- Public folder is for departmental information sharing purposes, personal email are prohibited.
- All users' mailbox are allocated 30MB of size.
- Sending and receiving of email will be discontinues if user's mailbox is oversize.
- Notification will be send by system to alert user when user's mailbox is near to limit.
- Personal folder should keep below 2GB of size, and the folder's housekeeping is the own user's responsibility.
- Out Of Office:
    - Turn ON "Out of Office Assistant" feature. (This should apply for IMAP protocol only exclude GKL users POP3 protocol)
    - Trigger MIS folk increase mailbox size. (This should apply for managers & officers level only)

c) Software Control

- MIS has predetermined the software to be installed in each of the computer. For any additional software to be installed to the pc/notebook, approval from MIS needs to be obtained.
- Employees are strictly prohibited from installing any pirated or illegal software. Should one be found doing so, the company will take appropriate disciplinary action against the employee including employment termination or legal actions.
- Any installed software that is use solely for the user's self benefit will be removed without prior notice.

- No games related programs should be installed at all time.

d) File Transfer Protocol (FTP) server.

- FTP server is for files/documents transfer purposes only.
- All transferred files/documents should remove after copy to own storage.
- MIS has authorities to remove files/documents more than 7 days.
- MIS will not responsible for any files/documents lost that stored in FTP server.
- Housekeeping will carryout from time to time to make sure the availability of server's space.

e) Diskettes, CD-ROM, Laptop, Computers & other IT Properties (Applicable to employees, in-house customers, frequent visit customers & frequent visit vendors)

- Personal storage media for example diskettes, CD-RW, portable hard-disk, laptop or USB drive are not allowed to bring into company.
- All company's storage media use on any PC belongs to customer or GSB/ISO MUST ensure of virus free by pre-scanning and remove off the virus. Any detection of virus by customer IT or MIS, the external drive will be confiscated by either customer PIC or GSB IT.
- Installation any type of media from employees or vendors to be used in company must obtained approval.
- All employees are fully responsible on the company's IT equipment that have been assigned to him/her
- Laptop with "Company Asset Tag" or any IT devices with "Company Authorized Sticker" are only allow to use in the company premise. Those without "Company Authorized Sticker" or if the company believes that the IT Devices have been used within company premises, the HR/Security/MIS/Management may retain the IT Devices or take any step to delete any information which the company reasonably believes has been copied/obtained at the company premises without approval.
- To get the "Company Authorized Sticker", employees, customers or vendors are required to apply through MIS by filling up the "Company IT Device Justification" form.
- All in-house customers, frequent visit customers & frequent visit vendors must follow the Globetronics IT Policy.
- All customers/vendors shall be liable for any company loss or damage resulting from violation of the procedures. Customers/Vendors shall not hold the company liable for any losses or damages, whatsoever, including loss of use of the IT Devices or loss of any data in the IT Devices.
- All employees are well informed that any company's information taken out without proper authorization will be confiscated of investigation, which might call for disciplinary action on employee involved.

f) External or personal IT equipment – Item Declaration procedure

- All vendors, customers or visitors are not allowed to bring in any IT devices into the company or connect to company's IT network unless with prior declaration at the main guard house.
- Example of IT devices:-
    1. Notebook / Laptop / Computer
    2. Memory stick media / Pen-drive / External hard disk
    3. Wireless broadband USB drive
    4. CD writer / CD-RW / DVD-RW
    5. Tape drive
    6. Magnetic optical disk
    7. ZIP drive
    8. Modem
    9. MP3/MP4 Device
- All vendors, customers or visitors bringing in the devices must register with security personnel before entering company premises & MUST ensure the devices are "virus free" by pre-scanning and remove off the virus. Any detection of virus, the external drive may be retained by HR/Security/MIS/Management.
- The "Declaration Form" needs to be signed by the requestor, vendors/customers/visitors and security personnel.
- Once registered, security personnel will place the "Company Authorized Sticker" on the IT Devices or seal the sticker over the LAN(RJ45) with a date written on sticker.
- If seal is broken or without "Company Authorized Sticker" or "Date of Expired Sticker" or if the company believes that the IT Devices have been used within company premises, the company may retain the IT Devices or take any step to delete any information which the company reasonably believes has been copied/obtained at the company premises without approval.
- Requestor are responsible to ensure that their vendors, customers or visitors follow the procedures mentioned above.
- Employee who requires to bring their personal IT devices are required to follow the "Item Declaration" Procedure. Failing to, HR/Security/MIS/Management has the right to confiscate said devices. The employee will then be referred to HR Dept for disciplinary action to be taken against him/her.
- All vendors, customers & visitors shall be liable for any company loss or damage resulting from violation of the procedures. Vendors/Customers/Visitors shall not hold the company liable for any losses or damages, whatsoever, including loss of use of the IT Devices or loss of any data in the IT Devices
- Employee found violating the policy shall be liable to stern disciplinary action up to termination of service

g) Audit

- All computers/system residing in company premises are subjected to MIS regular audit. MIS will report the cases to the management on those computers failed the audit process.
- MIS has the authority to remove any systems that are suspected cause performance and security threats to company's network.
- MIS will conduct periodic audit to ensure compliance to the policy.

h) Policy

- Company reserves the right to modify this policy when necessary.
- Any other activities require which not stated in the policy, approval from company's management is required.
- All the managers shall be familiar with this policy and educate to their subordinate and take appropriate action in the event of policy violations.
- Disciplinary action will be taken against employees for any misuse or violations to the policy.
- This policy includes rules and regulations and general information.