Contents

OVERVIEW

GeBBS Information security team is committed to protect the organization's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly

Effective security is a team effort involving the participation and support of every employee and affiliate of the organization who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property GeBBS. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Refer to Human Resources policies for further details.

PURPOSE

The purpose of this policy is to outline the acceptable use of GeBBS systems. These rules are designed to protect interest of employees, customers and all the systems at the organization. Inappropriate use exposes GeBBS to risks including virus attacks, compromise of network systems and services, and legal issues.

The objective of this policy is also to educate end users on the acceptable usage and Security role and responsibilities of employees, contractors and third-party users of GeBBS's information and information processing facilities. GeBBS must ensure that all employees & external party workers use organization IT assets as defined by the policies, procedures and guidelines and only for business purposes.

SCOPE

This policy applies to employees, contractors, consultants and other workers at GeBBS including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the organization.

POLICY

GENERAL USE AND OWNERSHIP

While GeBBS' network administration desires to provide a reasonable level of privacy, users should be aware that the data the users create on the corporate systems remains the property of GeBBS. Because of the need to protect the organization's network, management cannot guarantee the confidentiality of information stored on any network device belonging to GeBBS.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. For security and network maintenance purposes, GeBBS may monitor equipment, systems, data files, emails and any traffic sent or received via the company's network (intranet / internet) which is owned or

managed by GeBBS though any individual/ groups/ firms/ clients within or outside the organization authorized by GeBBS at any time, with or without notice to employees.

GeBBS reserves the right to audit any IT Assets owned or managed by the organization on a periodic basis to ensure compliance with this policy.

All users of GeBBS IT assets and working in GeBBS Information processing facility will be responsible to practice information security policies and Acceptable usage guidelines.

USER RESPONSIBILITIES

These guidelines are intended to help users make the best use of the computer resources at your disposal. Users should understand the following.

1. GeBBS Security Policies and Procedures

•Users must act in accordance with the GeBBS' information security policies.

•Users shall understand their roles and responsibilities with respect to information security.

•Users may be subject to sanctions or disciplinary action for violations of the security policies

•Users must be individually responsible for protecting the data and information in their / their hands. "Security is everyone's responsibility".

•Users must be aware of Data classification of IT Assets accessed by them and follow the guidelines. If not aware or are not sure, it is recommended that they read it on the GeBBS Intranet, "BUZZ".

•Users must use the resources at their disposal only for the benefit of GeBBS.

•Users must understand that they are accountable for their system.

•All user actions may be monitored. User consent for such monitoring.

•All IT Assets should be classified and labeled as per Information Classification and labeling procedure.

•All electronic communication should adhere to Electronic Communications Policy.

•Laptops users should adhere to Laptop Security Guidelines.

2. Physical Control

•All users shall ensure they wear visibly identity cards all the time when on GeBBS premises.

•Users must protect IT Assets from unauthorized access, disclosure, modification, destruction or interference.

•Log off or lock screen before you leave your workstation.

•If a user causes any damage to an IT asset, then they will be held accountable for any damages to IT Assets.

•User shall not install any unauthorized software and shall restrict the use of USB.

•Under no circumstance's user may indulge in any activity that is illegal, unauthorized as per local, state, federal laws.

•Employees carrying Personal Electronic Storage Devices/electronic gadgets etc. should declare them and handover the same at the main security gate and collect it while leaving office at the end of the day. Employees are not supposed to carry these gadgets inside GEBBS premises.

3. Reporting security events or potential weaknesses

• User must report security events or potential security weaknesses or other security risks to GeBBS InfoSec team.

•Ensure that on any occasion CD's and other media are brought into the Company only with appropriate authorization and they are checked for viruses by GeBBS Helpdesk before they are used.

• Inform GeBBS Helpdesk immediately if you think that your workstation may have a virus.

•Ensure that you use only the system which is allocated to you Report any SPAM mail received to infosec@gebbs.com

•Any new/change requirement in the service/resources should be done through IT service desk portal.

Please note the following:

•Workstations will be audited periodically.

•Logins and use of the Company's network are monitored and audited.

•Encryption of information should be in compliance to Electronic Communication Policy.

4. Password and Access Management

•Users shall ensure that they choose a password that is hard to guess. Passwords should be secured as per Password Policy.

•Users are assigned unique "User ID" for logging into internal GeBBS systems, users are required to follow GeBBS policies and procedures related to Access Control. Users must access GEBBS resources using their own unique ID‟ s provided to them.

•Protect equipment from theft and keep it away from food and drinks. Ensure that all important projects and functions related data is saved on the server so that it gets backed up regularly. Liaise with GeBBS Helpdesk if you require assistance.

•Ensure that the laptop data card provided is used for business purposes only.

•Ensure the connection to GeBBS Network using laptop card is not used by unauthorized personnel.

•Do not install any Microsoft product without approval from AVP. In case of any deficiency, hardware engineers and system administrator who is having access to systems will be held responsible and warning letter will be issued.

5. CLEAR SCREEN AND CLEAR DESK

•Employees must lock their computer system by using (Ctrl+Alt+Del) keys followed by “Lock Computer” or (Windows Key +L) when moving away from their workstation and they should not wait for the screensaver to lock the workstation.

•Employees must ensure that their PC / Laptop has approved screen saver enabled with password protection and they cannot change the screen saver setting in their workstation.

•Employees should not leave unattended Hard copies of sensitive information or media near the workstation areas or their respective cubes/tables/desks the table.

•Employees must lock all confidential documents and personal items in drawers or lockers before moving away from their workspace.

•Employees must keep a clean desk and remove/shred unnecessary papers if no more required.

•If users do not need some printouts, they must shred them in the nearest available shredder.

•When you have others in the cubicle keep your open documents upside down unless that can be shared.

•Employee must not print sensitive documents in remote printer, and they have to go and personally pick up the printouts once fired instead of waiting for someone to come and hand it over to them.

•Employee must not display sensitive information (passwords, IP addresses, customer sensitive information, and personal data) on dashboard or post it (sticky notes) in their cubicle.

•All GeBBS employees play an important role in managing Information Security and are supposed to visit the Intranet and read the GeBBS Security Policies, strictly adhere to the same.

6. Business Continuity

All users are required to support GeBBS in all the activities related to business continuity and actively participate disaster management programs implemented time to time.

UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., Network staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of GeBBS is authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing GeBBS owned resources.

1. Misuse of GeBBS services

•Open or shift or tamper the hardware and firmware settings on the desktop including headset, mouse or keyboard etc.

•Automate logon process.

•Change time settings on your desktop.

AUP

•Duplicate or copy software other than for backup purpose.

•Users are not allowed to carry their personal Laptop, USB drives.

•Copy data in any format and send outside the company without prior approval from the authorized personnel.

•Download or install unlicensed software / Shareware / Freeware from the Internet or distributed by PC magazine covers on your desktop/laptop.

•Alter the system / software default configuration, this work may only be undertaken by IT staff.

•Disabling of antivirus software on the system.

•Bring any form of magnetic media i.e., CDs, Zip drivers, Pen drive, DVDs etc.

•Share the local hard disk on the network.

•Install of any additional hardware on desktops provided without IT teams authorization.

•Log into more than one system concurrently (Please log out of the system before you log into another system).

•Permit others to use system where you have logged in.

•Imitate any kind of logos relating to the Company or the third party or any client of the Company without prior permission.

•Use a computer account that you are not authorized to use.

•Obtain or use another staff members' password.

•Use the corporate network to gain unauthorized access to any computer systems.

•Knowingly perform an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.

•Knowingly run or install on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.

•Attempt to circumvent data protection schemes or uncover security loopholes.

•Violate terms of applicable software licensing agreements or copyright laws.

•Deliberately waste computing resources.

•Use electronic mail to harass others.

•Mask the identity of an account or machine.

•Post any documents/materials on electronic bulletin boards without proper approvals.

•Attempt to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

•Give others the opportunity to look over your shoulder if you are working on something sensitive.

2. Internet

•Users must not use or access the Internet for non-business purposes and restrict personal use to bare minimal limited to educational and knowledge related to work. Users should strictly avoid visiting nonbusiness, offensive unethical sites which violate GeBBS security policies.

•Users must not subscribe to horoscope, astrology sites or other similar free mailing lists.

•User must not download songs, movies, humor clippings, and advertisements, pornographic &

other non-business or non-productive material.

•Users must not post any GeBBS' proprietary information or GeBBS, customer proprietary information on Internet share drives / briefcase, public forums, newsrooms or bulletin boards. This is strictly prohibited, and any violation will be subjected to disciplinary process that includes legal consequences.

•Access to non-GeBBS free/third party e-mail sites such as Yahoo, Hotmail, rediff mail etc. is strictly prohibited.

•Downloading and usage of Google talk, IP Messenger, Yahoo messenger, and MSN Messenger services in GeBBS Information processing Facilities are strictly prohibited. The only exception would if client has extended their chat facility to us.

•Users must not try to change attempt to use any proxy sites themselves to misuse Internet access facility.

•Users must not upload or mail GeBBS' confidential and sensitive documents to any third external party or even to their own personal ID‟ s created on any free mail sites.

•Mail Traffic and Internet Access are continuously monitored for any security violations.

•Users must not solicit to any activity or purpose which is not expressly approved by GeBBS management and attempt to reveal or publicize GeBBS proprietary or confidential information or any of its customers to any other third party.

•Users must not represent personal opinions on internet as those of the company (GeBBS).

•Users must ensure that they do not send advertisement of sale of personal IT Assets, invitations, wishes, etc. to large groups.

•Users of GeBBS Information systems must be aware that their information systems (computer, PCD, internet, email, Messenger, FAX, and Telephone Conversations), its usage and information exchanged are not private and the company reserves the right to monitor and audit these on ongoing basis and during or after any security incident. Logon Banners are displayed on Servers and Devices warning users about this.

3. social media

Users must not:

•Create or transmit material that might be defamatory or incur liability for the company.

•Post messages, status updates or links to material or content that is inappropriate. E.g., pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling, or illegal drugs. Inappropriate content or material also covers any text, images or other media that could reasonably offend someone based on race, age, sex, religious or political belief, national origin, disability, sexual orientation, or any other characteristic protected by law.

•Use social media for any illegal or criminal activities.

•Send offensive or harassing material to others via social media.

•Broadcast unsolicited views on social, political, religious, or other non-business-related matters.

•Use social media for advertising or endorsement purposes.

•Send or post messages or material that could damage GeBBS's image or reputation.

•Discuss colleagues, customers, or suppliers without their approval.

•Post, upload, forward or link spam, junk email, chain emails and messages.

Users must:

•Be respectful, polite and patient, when engaging in conversations on GeBBS's behalf.

•Not speak on matters outside their field of expertise.

•Not post discriminatory, offensive or libelous content and commentary.

•Remove offensive content as quickly as possible.

•Correct any misleading or false content as quickly as possible

4. Unacceptable use of GeBBS Assets

GeBBS network and IT infrastructure users must not-

•Damage computer systems.

•Obtain extra resources which are not authorized to an individual.

•Deprive another user of authorized resources.

•Gain unauthorized access to systems.

•Use unlicensed or pirated software.

•Download and/or Run any hacking utility or tools including password crackers, environment/network scanners, and sniffers on GeBBS network/systems/devices.

•Try breaking into other‟ s systems/applications through unethical means and cracking codes of illegally downloaded applications.

•Users must not use any common account unless it's operational necessity and appropriate approvals are in place.

•Users must not scribble passwords on paper or desk boards.

•Users must ensure that Corporate Hardware is not used for Personal purpose.

•Use of any Personal Hardware, PC or laptop in GeBBS is prohibited.

•Use of External Storage devices (CD‟ s/Zip Drives/USB Hard disk/Pen drives) must not be permitted on corporate network/Hardware unless authorized by the InfoSec team& IT Head.

•If privileged access is given to Users, they should use those access rights only for the business purpose for which they are given access.

•Users must be familiar with the GeBBS' security requirements for mobile devices.

•Any breach of GeBBS policy must warrant necessary disciplinary action up to termination of employment.

5. Email

•Use of GeBBS email systems must be treated by GeBBS employees as a privilege and not as a right.

•GeBBS maintains the right to review, audit, intercept, access, monitor, delete and disclose all messages created, received, sent, or stored on the email server, client or in any other form.

•The email system and all copies of messages created, sent, received or stored on the system are (and remain) the property of GeBBS.

•GeBBS Email Systems should be mainly used for business purposes and users must restrict personal use of mails to bare minimum level.

•The language used should be in consistent with other forms of business communication.

•Employees should treat E-mail messages with sensitive or confidential information, files as "GeBBS confidential" and take due care as per the information handling guidelines. All PHI shall be transmitted outside GeBBS via encrypted means only.

•The email system must not be used to create, send, receive or store any offensive or disruptive messages, or materials that infringe the copyright or other intellectual property right of any third parties or illegal activities.

•Unauthorized use of email systems is not permitted which includes, but is not limited to, transmitting or storing offensive material; sexual implications, gender specific comments, defamatory statements, or any other comment that offensively addresses someone‟ s religious or political beliefs, national origin, or disability; compromising the security of information contained in Company computers; conducting or soliciting for political, personal, religious or charitable causes or other commercial ventures outside the scope of the users' employment and users' responsibilities to the GeBBS.

•Users must avoid opening any mail from unknown users / sources and also avoid downloading or opening suspicious attachments or clicking on suspicious links.

•GeBBS must restrict attachments size on the company mail system. Refer to electronic communication policy for details.

•GeBBS reserves the right to audit, retrieve and read any email messages without prior notice.

•Employees must only disclose information or messages obtained from the email system to recipients authorized to have such information on need basis.

•Employees and external parties are not authorized to retrieve or read any email messages that are not addressed to them. Employees should not attempt to gain access to other employee's messages without his / her permission.

•In order to guard against dissemination of confidential corporate information, employees should take due care while reading confidential mails. Email windows should not be left open on the screen when the computer is unattended; at such times the screen should be cleared, and the computer should be locked so that for re-access the user‟s password would be needed.

•must not try to automatically forward their emails to any address. Outside the GeBBS networks.

•Auto forwarding of emails within GeBBS for business purposes, may be allowed for a limited period with the prior approval of the concerned manager.

•Users must not send „confidential‟ or „restricted‟ information via email outside GeBBS, unless it is compliant to the document classification and information handling procedures. GeBBS email serv

•GeBBS email service must be used only for official purpose. Users must not indulge in sending chain letters, mass mailing or religious emails from a GeBBS email account. It is strictly prohibited and considered as a security incident.

6. Software

•Users must not download software on their own from the network/internet. Any business requirements that necessitate download must log ticket with helpdesk with business case and senior's approval.

•Users should not distribute software (e.g., setting up ftp server) as they do not have the right to do so.

•Users must not download any software or electronic files without prior approval from the IT team and without reasonable virus protection measures in place.

7. Personal Electronic storage Devices

It has significant threat to security. The use of Personal Electronic Storage Devices within GeBBS Premises is strictly prohibited in order to prevent information leaks, IPR violations, unauthorized disclosure of confidential information etc.

Personal Electronic Storage Devices which fall into these prohibited categories include but not limited to the following.

Computer systems: Computer systems can be used to store sensitive data and may introduce viruses into the network. Handheld computer systems are of particular concern. They lack the security of their larger counterparts and their small size makes them easy to lose or steal. Anything that synchronizes to a workstation fits into this category. Examples include but are not limited to PCs, laptops, I pad, Tablets PC, electronic organizers and data watches.

Recording devices: Audiovisual recording devices represent a threat for obvious reasons. Examples include digital cameras, PC cameras, video recorders that are restricted in GeBBS and smart phones/cell phone camera combos.

Data Storage devices: Small storage devices and backup media can be used to transport large quantities of sensitive information.

Examples of specific prohibited Data Storage Devices which are capable of transferring and copying data using zip drives, CDRW drives, USB storage devices, iPods, USB hard drives through LAN, wireless medium etc.

Alter the system / software default configuration, this work may only be undertaken by IT Services staff: Employee must not use unapproved methods to remotely access company systems. Use of Personal Modems and wireless network devices including Data Cards are restricted in GEBBS.

Consultants and visitors must be advised of these restrictions and monitored for Security Compliance by the GeBBS escort.

ENFORCEMENT

Any misconduct pertaining to or in violation to the abovementioned policy will be adequately governed by HR disciplinary procedures.

DEFINITIONS

Term Definition

Spam: Unauthorized and/or unsolicited electronic mass mailings.