Policy - Acceptable Use

Introduction

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct GlobalLogic business or interact with internal networks and business systems, whether owned or leased by GlobalLogic, the employee/consultants, contractor or a third party. All employees, contractors, consultants, temporary, and other workers at GlobalLogic and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with GlobalLogic policies and standards, and local laws and regulation.

This policy applies to all equipment that is owned or leased by GlobalLogic.

Policy

1. General Use and Ownership

GlobalLogic proprietary information stored on electronic and computing devices whether owned or leased by GlobalLogic, the employee/consultant or a third party, remains the sole property of GlobalLogic.

Employee/consultant responsible for promptly reporting the theft, loss or unauthorized disclosure of GlobalLogic proprietary information.

Employees/consultants may access or use GlobalLogic systems, applications or any other resources as well as process GlobalLogic or any of its clients, vendors, partners information to the extent it is to authorized and necessary to fulfill their assigned responsibilities.

2. System and Network Activities

Organizational User IDs, websites and email accounts may only be used for organizationally sanctioned communications.

The distribution of any information through the Internet (including by email, instant messaging systems and any other computer-based systems) may be scrutinized by GlobalLogic and GlobalLogic reserves the right to determine the suitability of the information.

The use of organizational computer resources is subject to law and any abuse will be dealt with appropriately.

It’s prohibited to visit Internet sites that contain obscene, hateful or other objectionable material, attempt to bypass organizational surf control technology and/or post indecent remarks, proposals or materials on the Internet.

Users shall not solicit emails that are unrelated to business activity or which are for personal gain, shall not send or receive any material which is obscene or defamatory or which is intended to annoy, harass, or intimidate another person, and shall not present personal opinions as those of the company, and the use of organizational email facilities is subject to further detailed rules set out in Email and Communication Activities Section of this document.

Users may not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to the company or any third parties, may not reveal or publicize confidential information, and will not

send confidential emails without the level of protection required in **Policy - Information Classification, Labeling and Handling.**

It's prohibited to download or execute any software from untrustworthy resources unless it's required by GlobalLogic policies and procedures

Users shall not seek to avoid and will uphold GlobalLogic's anti-malware policy and procedure, will not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network, and will not examine, change or use another person's files or any other information asset for which they don't have the owner's explicit permission.

Users shall not carry out any other inappropriate activities and shall not waste time or resources for non-business-related activities.

It's prohibited to use p2p or Tor connections (including but not limited to: BitTorrent, uTorrent, Transmission, Kazza, Morpheus, eDonkey).

3. Email and Communication Activities

Organizational email addresses shall not be utilized for personal use, including personal purchases, personal registrations at the external resources, or any other personal transactions and/or activities.

It is strictly prohibited to use personal emails as well as other means of personal communication for processing of GlobalLogic or its Clients information. This also includes any testing activities during the project execution.

Organizational email facilities may not be used for sending defamatory emails, or using email for harassment, unauthorized purchases, or for publishing views and opinions (defamatory or otherwise) about employees/consultants, workers, suppliers, partners or customers of GlobalLogic.

Emails should have a footer that contains the legal disclaimer.

Organizational email may only be used for the communication of confidential information in line with the requirements of **Policy- Information Classification, Labeling and Handling.**

Users must not open incoming email attachments that originate with unknown third parties or that, even if they appear to have been sent by a known party, were not expected. These attachments may contain viruses, worms or trojans and any such emails must be reported to the Information Security Officer immediately, by creating a respective ticket in the HelpDesk or by other means of communication. Suspicious emails cannot be forwarded, copied with active links to anyone, whether inside or outside the network. Exception may be if the Information Security Officer asks you directly about it.

Viruses and hoax virus messages: users are required to report any third party email messages they receive about viruses to the Information Security Officer or IT Help Desk immediately by telephone or in person.

Do not click on any link that came through an email from an unknown source. It may contain malicious code or could be a 'Phishing Attack'. Do not share emails with active malicious links with your colleagues, but immediately report it to the Information Security Officer by any means of communication.

Users are prohibited from using organizational email facilities for forwarding chain letters or impersonating other people, nor may organizational email addresses be left on any websites other than for legitimate and necessary business purposes.

Users are required to limit the use of group email addresses, to limit copying to unnecessary recipients, to restrict use of the 'reply to all' function, and restrict the use of the blind copying feature.

Users are required to comply with the **Policy - Information Security Incident Management.**

Organizational email may not be used to purchase anything on behalf of GlobalLogic without specific prior authorization, and then only in accordance with GlobalLogic's current policy on purchasing.

Employees/consultants are prohibited from setting up automatic forwarding of emails to addresses external to GlobalLogic or of copying emails to addresses outside GlobalLogic unless there is a legitimate business purpose for doing so.

Transfer of executable files via email is prohibited even if they are archived. Blocked file's extensions are: 7z, asp, bat, class, cmd, com, cpl, exe, fon, hta, ini, ins, iw, js, jse, pif, rar, scr, shs, vb, vbe, vbs, ws, wsc, wsf, wsh, zip.

Only GlobalLogic IT is authorized to create GL Google Apps accounts or mail groups.

Only GlobalLogic email addresses can be included in the GlobalLogic mail groups. External addresses can't be added to GL mail groups Owner of each mail group is responsible for maintaining actuality of the members. Mail groups which are no longer relevant or not used for more than 1 year are deleted by IT.

An email archiving feature is enabled to archive and retain all the inbound and outbound emails for the users. Email accounts are backed up on a daily basis, forwarding is set by request from the user's manager. Google Docs owner is changed according to the user's manager decision. Backups are stored for indefinite periods and are subject for change at any time.

Google docs and Site owner is responsible for access management to his/her Google docs/Sites. Write access must be limited and disable as soon as no longer required. Google docs/Sites must be deleted if no longer required or at least access should be revoked.

It is allowed to configure and use GL Google Apps account on mobile devices on condition that device access is password protected.

Users are provided with internal SMTP service relaying to Google Apps servers as following:
- SMTP service is used to send mail messages for testing purposes and notifications
- SMTP service is allowed only for IT infrastructure and project computers for which access was requested through IT HelpDesk.

Email and related services availability is ensured by Google as per SLAs: Google Apps Service Level Agreement (http://www.google.com/apps/intl/en/terms/sla.html)
Health status of Google Apps services can be checked at http://www.google.com/appsstatus#hl=en&v=status&ts=1382090797832

The following communication/collaboration channels, provided only by GlobalLogic or Client, are allowed to be used (depends on licence availability):
- GlobalLogic email (Gmail)
- Google Chat
- Google Meet
- GlobalLogic Helpdesk tickets
- WebEx
- Slack
- Zoom
- MS Teams.

Users shall be careful while using messengers and do not trust links and files sent from unknown resources. Even for known resources it is suggested to make sure that a sender has no malicious intent.

People should avoid transferring confidential data via messengers. It is suggested to use email communication for such cases.

GL IT provides Voice and Video communication services which include telephony, audio and video conferencing systems.

It is not allowed to relocate IP-phones without notifying IT.

Outbound video-conferencing calls are allowed to any destination by default. Inbound calls are possible for approved sources only. To be able to receive a call from new source apply to IT for new remote host authorization.

4. Passwords

All the GlobalLogic employees/consultants must follow password requirements, stated in the **Policy - Password Management**.

5. Clear desk policy, screensavers and information reproduction

Users are obliged to ensure that there is no confidential or restricted information (in paper or removable storage media format) left on desk, or left in or near reproduction equipment (photocopiers, scanners, printers etc.) when user is not in attendance and ensure that such information is secured.

Employees/consultants are obliged to ensure that no one is able to access their computer when they are not present and that password protected screensaver that operates within 10 minutes of no activity are used or which are activated when computer is left unattended.

Employees/consultants are obliged to terminate active computer sessions when they have finished them and to logged off (i.e. not simply turn off the computer screen) whenever they have finished working and that the workstation is to be protected by appropriate key locks when they are away from the workplace.

Employees/consultants may only use GlobalLogic's equipment (photocopiers, scanners, printers etc.) for proper organizational purposes and are obliged to use facilities that are appropriate for the classification level of any information with which they are dealing.

6. Software

It is prohibited for the employees/consultants to make any attempts to disable, override or remove any of GlobalLogic's installed software, including anti-malware software, firewalls, automatic updating services and system BIOS.
Re-installing the operating system by the user is strictly prohibited. If such a procedure is necessary, the user should contact IT support.

It's prohibited to install or execute software (applications, scripts, code, etc.) downloaded from untrustworthy resources, for which GlobalLogic does not have a valid license and does not have prior authorization. This prohibition applies to freeware, shareware, subscription-based software, screensavers, toolbars and/or any other programs that might be available.

GlobalLogic's approved software is listed on Standards - Software

Infrastructure administrators maintain a configuration control schedule for software.

More detailed information is described in the **Policy - Software Management.**

It is prohibited to use any unauthorized software - applications, SaaS, AI-based tools, etc. Software shall be authorized either by GlobalLogic or the client. Software must be authorized by GlobalLogic, client or both. If

authorization is done by the client - documented approval shall be obtained from the client for the use of any particular software, and if possible, added to respective project specifications in SoW.

For any such authorization, the request should be created to the Information Security Team via HelpDesk.

7. Cloud Services

Use of cloud services for work purposes must be formally authorized by GlobalLogic IT.
Customer information may not be processed with the use of such services without formal authorization by Customer and Project management approval.

8. Data control and legislation

Employees/consultants are to ensure to abide by any legal requirements in respect of their computers use, including privacy and data protection regulations.

9. Backup and information classification

Employees/consultants are responsible for ensuring that all information on their workstations/laptops/corporate networks and cloud storages is correctly classified and labelled in line with the requirements declared in the **Policy - Information Classification, Labeling and Handling.**

Backup and archive are processed in line with **Procedure - Backup and Archive**.

10. Hardware

- Usage of personal devices for work purposes is strictly prohibited, except the devices with no storage and/or record capabilities (headsets, monitors, keyboards, etc).
- Users are allowed to work on equipment (workstation, laptop, tablet etc.) provided by GlobalLogic IT or Client only.
- Usage of personal removable media devices is strictly prohibited.
- Usage of personal devices in all GlobalLogic networks except guest one is strictly prohibited.
- Detailed information about hardware usage is described in **Policy – Hardware Asset Management**.

11. Maintenance

Employees/consultants are responsible for the physical security of their workstations/laptops according to the **Policy – Hardware Asset Management**.

12. Audit and security monitoring

Use of the Internet/intranet/email/instant messaging may be subject to monitoring for security reasons and/or network management and users may have their usage of these resources subjected to limitations by GlobalLogic.

13. Revocation and change of access rights

GlobalLogic IT may only process changes to user rights once a request has been created in HelpDesk and approved by the asset/system owner.

14. Physical security

All GlobalLogic employees/consultants are obliged to follow GlobalLogic's country/location specific physical access policies and procedures.

15. Behaviour during phishing attacks

- All GlobalLogic employees/consultants must be diligent when it comes to phishing attacks - never click on links, download files or open attachments in emails received from unknown sources.
- Be wary of emails asking for confidential information – especially if it asks for personal details or credentials.
- All GlobalLogic employees/consultants should always, where possible, use a secure website (indicated by https:// and a security “lock” icon in the browser’s address bar) to browse, and especially when submitting sensitive information online, such as credentials.
- In case the received email looks suspicious - **do not** forward it to your colleagues, but immediately contact the Information Security Officer or submit an incident ticket via HelpDesk (Information Security (DCP) project). Submitted tickets **should not** contain active links - the responsible person will contact you directly and request additional details.

16. Reporting Information Security Events/Incidents

All GlobalLogic employees/consultants must follow **Procedure - Reporting Information Security Events** when it comes to any observable occurrence that is relevant to information security. This can include attempted attacks or lapses that expose security vulnerabilities.

17. Awareness

All employees/consultants must attend/participate in mandatory awareness training provided by GlobalLogic and such attendance should be tracked. Managers are responsible if their subordinates are participating in mandatory IS Awareness campaigns and completing them.

Managers are responsible for ensuring that all employees/consultants (and others within his/her control) who conduct work, are competent to conduct the tasks required. These competences must include awareness of the information security policies and procedures, and how an individual’s work affects the overall information security objectives of the company.

18. Compliance

The Information Security Officer will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CISO in advance.

An employee/consultants found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Breaches of these requirements or any other misuse of email that negatively affected the GlobalLogic may be subject of GlobalLogic’s disciplinary policy.

Change History

Revision	Change Description	Valid Date	Approver
1.0	Initial version. Document is created based on Policy - Internet Acceptable Use, Guideline - Rules of Email Use, Guideline - Control of Software Installation, Policy - Communication and Guideline - Individual User Responsibilities due to documentation restructure project.	01/28/2021	Alok Malik, CISO
1.1	Doc ID was added	5/13/2021	Alok Malik, CISO
1.2	Sections 2, 3, 6 and 17 were updated. Changes in the wording, no additional requirements.	8/11/2021	Alok Malik, CISO
1.3	Typo correction	09/09/2022	Alok Malik, CISO
1.4	Exception is added to point 1 in section 10.	1/20/2023	Denys Kudriavchenko, Head of Security Risk & Compliance
1.5	Section 6 was extended regarding usage of applications, SaaS, AI-based tools, etc.	07/12/2023	Denys Kudriavchenko, Head of Security Risk & Compliance
1.6	Section 3 was updated regarding usage of personal email	08/16/2023	Denys Kudriavchenko, Head of Security Risk & Compliance
1.7	Section 1 was updated regarding of logical access	03/13/2024	Denys Kudriavchenko, Head of Security Risk & Compliance