GUJARAT ALKALIES AND CHEMICALS LTD.

GACL®

Promoting Green Technology

INFORMATION TECHNOLOGY CYBER SECURITY POLICY

TABLE OF CONTENT

REVISIONS

Revision Details

Revision No.	Revision Date	Revision Description
1	31-Jan-2019	Initial Version (Baseline)
2	5-Sept-2020	Added Remote Work Security Policy
3	10-Aug-2021	Added Privacy and Personal Data Protection Policy
4	05-Jan-2023	Added Clean Desk Policy and Physical Access Control Policy

1 OBJECTIVES

The primary objective of this document to use IT resources in a cost-effective manner that safeguards GACL data and promotes accuracy, safety, Information, and efficiency. It also provides Policy to achieve efficient and effective use of Information Technology to improve business processes, to increase productivity while ensuring accuracy, accountability, confidentiality, availability, and integrity of the information.

This document aims to provide Policy on the aspect related with information technology such as Software usage Management and its compliances, Network Management, Desktop Management, Internet usage, Usage and Access control of ERP Applications such as SAP Systems and Intranet Systems, Email usage etc. Proper use and control of computer resources is the responsibility of all employees. Intentional or reckless violation of established policies or improper use of GACL computers or systems will result in corrective action. Employees should also be aware that any work completed on GACL computers is subject to monitoring and review.

Under this policy, the goal is to comply with regulations and to protect the integrity of the business data that resides within GACL's technology infrastructure. GACL IT Team can devise, circulate and/or implement any Procedure or SOP/ Policy relevant to usage of Information Technology in general or specific to particular aspect on need basis with necessary approvals, as required.

2 SCOPE OF INFORMATION TECHNOLOGY(IT) CYBER SECURITY POLICY

This policy applies to all employees and contractors/third party of GACL who are using and managing IT resources includes hardware and software resources. The Policy aim to regulate and control, the access to the information through ERP/SAP system, Intranet and Internet, Users to manage the Computer Hardware / Peripherals for proper usage. The scope aims at safeguarding business interest of GACL by preventing occurrence of inappropriate, unethical, or unlawful behavior by any of the users and preventing external threats to IT system.

GACL recognizes the importance of IT security in relation to both its obligations and the effect on business continuity. This guideline is intended to create an accountable, secure, and extensible framework around all Information Technology resources and activities under the control or care of GACL.

The scope can be reviewed time to time to incorporate changes in policy due to changes in technology, company policy, statutory requirement, business requirements, and operational requirement. Such changes, amendments, deletions are to be affected after proper approval of the Management, in case if required. The amendments, changes, alterations, deletions, etc. required will have to be done through insertions, additions, deletions of clauses in appropriate Revision section. The objective of the change, whenever changed

or amended, should always address the need to regulate, control and monitor proper use of Information Technology in the overall interests of the organization. The amendments, changes, alterations, deletions, etc. will be communicated to the employees and contractors/third party of GACL who are using and managing IT resources. Records of such communication will also be maintained.

3 APPLICABLE RULES & REGULATIONS

GACL will adhere to the following rules & regulations to ensure information security and data privacy to the all its stakeholders:

- Information Technology Act, 2000
- Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

4 ACCEPTABLE USE OF IT ASSETS

4.1 Objectives

The purpose of this policy is to outline the acceptable use of IT assets. These rules are in place to protect the authorized user and GACL. Inappropriate use exposes GACL to risks including Virus/Malware attacks, compromise of network systems and services.

4.2 Scope

This policy applies to all employees, users or third party who are using Desktop or IT resources/infrastructure issued by GACL. All are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with GACL policies and standards, local laws, and regulations.

4.3 Policy

4.3.1 All electronic files created, sent, received, or stored on GACL owned, leased, or administered equipment or otherwise under the custody and control of GACL are the property of GACL.

4.3.2 Access requests must be authorized and submitted from departmental HoD for employees to gain access to IT systems.

4.3.3 Authorized users are accountable for all activity that takes place under their Username or User-id.

4.3.4 Authorized users should be aware that the data and files they create on the IT systems immediately become the property of GACL. Because of the need to protect GACL network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to GACL.

4.3.5 GACL IT Department routinely monitors usage patterns for its e-mail/Internet communications and other IT services and systems. All messages created, stored, sent, or retrieved over the GACL Information Systems are the property of the GACL and shall not be considered private information. GACL reserves the right to access and monitor all electronic messages, and soft or hard copy files of the user's communications at all times in accordance with the relevant laws of the country.

4.3.6 IT Department reserves the right to remove any non-business-related software or files from any system.

4.3.7 System level and user level passwords must comply with the Password Policy. Authorized users must not share their GACL login ID(s), account(s), passwords, or similar information or devices used for identification and authentication purposes. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.3.8 Users shall not use GACL Information Systems in a manner that would violate any applicable law, regulation or any GACL policies or procedures.

4.3.9 Use of any communication facilities not provided or authorized by GACL for any official communication is prohibited. Users shall not use any unauthorized / personal e-mail services (e.g. Gmail, outlook.com, yahoo, etc.), instant messengers (e.g. Google chat, WhatsApp, Telegram, Facebook chat, etc), or communication facilities (e.g. cloud storage, Pen Drives, Mobile phone, external Hard disks etc.) for the transmission, storage, or retrieval of GACL Information.

5 SOFTWARE USAGE POLICY

5.1 Objectives

Various IT applications make use of proprietary software on various devices used within the organization. These licenses can be out rightly purchased or taken on license fee basis as per the policies of software vendor.

5.2 Scope

This policy applies to all users or third party who are using Desktop or IT resources/infrastructure issued by GACL. The Software being used for Plant Operations and Controls are excluded under the referred scope.

5.3 Policy

5.3.1 GACL will make use of only legal licenses and opensource licenses through respective software providers. The management will provide budgetary support for fulfilling legal compliances in this respect.

5.3.2 GACL will treat the installation of unlicensed software by users as a serious breach of the IT Cyber Security Policy.

5.3.3 Record of Software license will be maintained by the IT Department.

5.3.4 Employees will refrain from any usage of any Software that are either related to games, videos, music, etc. or which is detrimental to the Employee's productivity are strictly prohibited.

5.3.5 Specialized software license requirements pertaining to Research, Design, Project Management, Process Control Systems, etc. are not covered here under and will be duly taken care by the respective user departments.

5.3.6 Copying or unauthorized use of licenses purchased by the company is strictly prohibited for the employees.

5.3.7 All the Software Programs and Documentations created by Employees, Consultants or Contractors for the benefit of GACL would be intellectual property of GACL unless and otherwise covered by a contractual agreement.

5.3.8 IT Department will consider up-gradation of software on need and utility basis.

5.3.9 Users must not upload any GACL data / information on any free online software, converters or file sharing websites (e.g. PDF converter, WeTransfer, etc). Such act must not be done for any official purpose. Only applications approved / provisioned by IT team shall be used.

6 INTRANET / SAP SYSTEM USAGE AND ACCESS CONTROL POLICY

6.1 Objective

GACL Intranet and SAP System are key Transaction processing systems and employee's facility to interactively assist the GACL's business functions. It allows employees to access information about or in connection with the GACL and its work.

It is important to have policy connected to the usage and access control mechanism for Intranet / SAP System in order to ensure that; the system provides the access to authorized users only to acquire information for business decisions on the need-to-know principals.

6.2 Scope

This policy applied to all employees or third party who are using various modules available under GACL intranet/SAP Systems.

6.3 Policy

6.3.1 All employees or third party of GACL can access the intranet/SAP System through their user id's and password. They will maintain confidentiality of access through his/her password and will take all appropriate care not to leak out password to any unauthorized person.

6.3.2 Shared access on GACL Intranet / SAP system or any other system is not permitted.

6.3.3 For any access to Intranet Module or SAP System, Employee will initiate the request through the concerned Head of the Department. IT Department will review/ revise/ reject/ approve this request application as per the requirement.

6.3.4 There are different levels of access like entry, edit, approving, forward, sanction, reports, view, processing etc. and the user will have to mention specific rights required for his/her function with due concurrence of the concerned Head of the Department.

6.3.5 Access rights required by third party working for GACL will be given as per the approval of the HoD. HoD of that functional department which has hired services of third party will have to initiate request for access rights.

6.3.6 Request for new development or modification in the program, form, report, view etc will be initiated by the user of duly concurred by the concerned Head of the Department and will forward to IT Department. IT Department will review/ revise/ reject/ approve the request after assessing operational, technical or economic feasibility. This request shall be submitted online and status of the same shall be available to users online.

6.3.7 In case of problems with the functioning of software application of intranet / SAP System, users must intimate IT Department.

6.3.8 Even though the system or program development work is carried out with its proper procedure and with proper testing, it is users responsibility to verify the output time to time and inform IT Department in case anything wrong in that.

6.3.9 All accounts must be disabled immediately upon notification of any employee's termination.

7. INTERNET USAGE POLICY

7.1 Objective

The purpose of this Internet Usage policy is to define standards to ensure employees use the Internet to gather information, which are relevant to GACL business activities in a safe and responsible manner, and ensure that employee Internet usage can be monitored or analyzed during an incident.

7.2 Scope

This policy applied to all employees or third party who are using Internet through GACL network.

7.3 Policy

7.3.1 Users are provided access to the Internet to assist them in the performance of their jobs and used for GACL business purpose. At any time, at the request of management, Internet access may be revoked.

7.3.2 Internet and messaging services will be duly protected by firewalls, anti-virus and anti-spamming software solutions. Every year or on need basis, the audit for vulnerability gaps will be carried out.

7.3.3 IT Department will monitor misuse of Internet connectivity and will inform concerned user to desist from such use.

7.3.4 No files or documents may be sent or received that may cause legal liability for, or embarrassment to, the GACL.

7.3.5 Internet user is prohibited to download video files, music files, game and other free software that are detrimental to the performance of desktop machines.

7.3.6 IT Department will block the websites that fall under objectionable category and also those which are being used for purposes other than GACL business activity.

7.3.7 Internet user discipline is of prime importance to the overall IT networks security of the organization.

7.3.8 Any activity, which is detrimental to the interest of the organization and also to the security of business data and network, shall be reported to the concerned authority for taking appropriate action. Internet should not be used for any purposes which are against GACL business and other legal regulations of the country.

7.3.9 User must not use the Internet Services to breach the security of another user, or to attempt to gain access to another person's computer, software or data, without the knowledge and consent of that person or to attempt to circumvent the user authentication or security of any host, network or account, including accessing data not intended for your access, unauthorized logging into or making use of a server or account or probing the security of other networks.

7.3.10 User must not use the Internet Services to interfere with (or encourage others to interfere with) computer networking or telecommunication services to any user, host or network, including denial of service attacks, flooding of a network, overloading a service, or attempting to crash a host.

7.3.11 User will not use any medium to access Internet connectivity which are not approved by the management.

7.3.12 Connections such as VOIP or through Cell Phones are prohibited for all Internet users unless exclusively approved by the management.

7.3.13 Users shall not launch any social media handle, page using company name and logo without written permission of the authorized Corporate Communication Department / HR Department.

8. HARDWARE (DESKTOP / LAPTOP) AND PERIPHERAL MANAGEMENT AND SECURITY POLICY

8.1 Objective

The policy is aimed to provide enhance security and quality operating status for Computer Hardware / Peripherals (Desktop/Laptop/Printers/Scanners etc.) and to ensure proper, efficient, optimum use of machines and peripherals so that overall performance and life of Hardware is maintained, and overall compliances are adhered to. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure the hardware against such attacks.

8.2 Scope

This policy applied to all employees or third party who are using Computer Hardware and other IT related resources of GACL.

8.3 Policy

8.3.1 Desktop/Laptop users are required to take regular backup of their files, data and e-mails.

8.3.2 User will be careful in using external devices such as pend drive or external hard disks etc. to avoid ingress of virus or malware etc into GACL IT infrastructure.

8.3.3 All Desktops/Laptop's issued by GACL are loaded with anti-virus, malware and Data leak protection (DLP) software's and user will ensure that anti-virus, malware and DLP function is active on their desktops/Laptops. IT will obtain alerts of infected workstations and perform certain remediation tasks

8.3.4 All peripherals such as printers, scanners etc. attached to desktop shall be optimally used so as to conserve stationery items.

8.3.5 Desktop/Laptop Users shall not use any unauthorized software, which may lead to legal compliance issues.

8.3.6 Software for videos, games, music files etc. shall not be used. IT Department will deploy a software tool for the asset management monitoring and remote control of desktops to alert against such uses.

8.3.7 Desktop users have to ensure that their local files and folders are not shared on the GACL's network.

8.3.8 Users should ensure their Desktops/Laptops are fully shut down and turned off at end of day.

8.3.9 Users should get in the habit of logging off when their work is done. This is not only to protect their personal account data but also to protect others using the system.

8.3.10 Computers should be locked or shut down when left unattended for any significant period of time

8.3.11 Individual user shall reasonably protect and take care of the desktops and peripherals from dust, spillages and physical damages.

8.3.12 Desktop user shall destroy their used ribbons and cartridges as per the ISO Policy.

8.3.13 Requirements for new hardware should be discussed in advance with the IT department to assess the detailed specification.

8.3.14 The user of a particular department will initiate request form for new hardware requirement duly concurred by concerned Head of the Department. IT Department will review the requirement based on the technical feasibility and shall issue the required hardware based on the availability of hardware and budget.

8.3.15 The deployment of new hardware or re-deployment of existing hardware will be undertaken by the IT Department/Services provider after consultation with concerned Departmental Heads.

8.3.16 The relocation of hardware within or outside GACL premises should not carried out without prior intimation/approval from IT department in advance to ensure good reason for relocation, determine the most appropriate means of relocation and to ensure equipment registers are updated.

8.3.17 Problems with hardware and software installed at user's desktop should be reported to the IT Department in accordance with established IT Help Desk procedures.

8.3.18 The response times for support requests depend on the nature of the request and on available resources. IT department makes every attempt to expeditiously handle incoming support requests. Depending on the nature of the request, IT Department will respond to service requests anywhere from within 1 hour to 48 hours of the receiving the request.

8.3.19 When there is a high volume of requests, requests are addressed based on priority and the order received.

8.3.20 IT department may resort to disabling all communication ports on the desktop if the same is required in the interest of the security of data and information. Such activity shall be duly approved by Management, in case if required.

8.3.21 To monitor, regulate and control use of unauthorized software of files and objectionable data storage for different desktops is under the purview of IT department.

8.3.22 It is the responsibility of each employee of GACL to protect Information technology base resources from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to GACL's public image.

8.3.23 The Laptop Policy in force will be integral part of this policy.

9. EMAIL SECURITY AND USAGE POLICY

9.1 Objective

The purpose of this policy is to ensure the proper use of GACL e-mail system by its employees, or any third party who are operating on behalf of GACL. Electronic Mail is a tool provided by the GACL to complement traditional methods of communications and to improve management and administrative efficiency. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner.

9.2 Scope

This policy applied to all employees or third party who are using email account of GACL domain.

9.3 Policy

9.3.1 E-mail accounts are created by the IT department.

9.3.2 Users shall not use third party email systems (e.g. Google, Yahoo, Hotmail etc.) to store, transmit and/or process official information. Additionally, users shall be prohibited from copying/ forwarding official emails and information to such unauthorized third-party email systems.

9.3.3 GACL email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any GACL employee should report the matter to their supervisor immediately.

9.3.4 Employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. GACL may monitor messages without prior notice.

9.3.5 GACL e-mail services may be used for incidental personal purposes provided that such use does not:

- Directly or indirectly interfere with the GACL performance of work duties, operation of computing facilities or e-mail services.

- Interfere with the e-mail users' employment or other obligations to the GACL.

- Violate this Policy, or any other applicable policy or law, including but not limited to use for personal gain, conflict of interest or commitment, harassment, defamation, copyright violation or illegal activities.

9.3.6 Employees shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the GACL unless expressly authorized to do so.

9.3.7 No files or documents may be sent or received that may cause legal liability for, or embarrassment to, the GACL.

9.3.8 GACL shall retain the right to review, delete, copy and modify the content being generated or transmitted using its resources.

9.3.9 Employees are responsible for safeguarding their identification (ID) codes and passwords, and for using them only as authorized

9.3.10 Access to GACL e-mail services is a privilege that may be wholly or partially restricted by the company without prior notice and without the consent of the e-mail user.

9.3.11 Users should enable spam filters to ensure protection against potential malware and phishing, as applicable.

9.3.12 Employees who have retired, terminated or resigned from the GACL will have email privileges removed effective on their last worked day updated by HR Department.

10. NETWORK ACCESS AND USAGE POLICY

10.1 Objective

The purpose of this policy is to ensure secure and reliable network access and usage by the users. This policy is intended to protect the integrity of the GACL network and to mitigate the risks and losses associated with security threats to the GACL network and information systems.

10.2 Scope

This policy applied to all employees or third party who are using GACL network.

10.3 Policy

10.3.1 Technological changes and other factors may require a reconfiguration of the network resulting in a change to the network addresses assigned to computers. IT department will give prior notice to affected users before making any changes.

10.3.2 Access to GACL network from outside GACL premises can be provided. The user who wishes to access GACL network from outside GACL premises shall take approval from their Head of Department and submit a request to IT Department. IT Department will install Virtual Private Network (VPN) on the desktop or laptop of the user and provide user id and password for the same so that the user can access GACL network from outside GACL premises.

10.3.3 The users can access SAP system and Intranet once they are connected using VPN to GACL network.

10.3.4 GACL employees or departments may not connect, nor contract with an outside vendor to connect, any device or system to the GACL's data networks without the prior review and approval of IT Department.

10.3.5 Departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the GACL must get prior approval from IT Department.

10.3.6 Physical access to GACL networking equipment (routers, switches, hubs, etc.) is not permitted without the prior approval of IT Department.

10.3.7 If security problems are observed, it is the responsibility of all GACL’s network users to report problems to IT Department for investigation.

10.3.8 Establishing unauthorized network devices, including router, gateway or remote dial-in access server; or a computer set up to act like such a device is not permitted.

10.3.9 There will be no monitoring or recording of the data content of packets traversing the Computer Network without the explicit permission of the IT Department.

10.3.10 IT Department may, at its discretion, devolve some responsibility of management, maintenance and monitoring to End User departments to support their activities as efficiently as possible.

10.3.11 Non-GACL IT systems that require network connectivity must be approved by IT Department for accessing GACL networks.

11. OUTSOURCING MANAGEMENT/THIRD PARTY/SERVICE PROVIDER SECURITY POLICY

11.1 Objective

Different maintenance and upkeep services are outsourced to different service providers for proper management of IT infrastructures and it may require service provider/third party contractors to carry out specific tasks. It is essential that proper evaluation of such service providers is done prior to assigning such services and regular monitoring of the services provider is done so that company IT infrastructure is secure and gets maximum benefit and value for money.

11.2 Scope

This policy applied to all employees or department who are outsourcing the IT related work to third party or service provider.

11.3 Policy

11.3.1 Detailed review of the service provider in terms of his capacity, manpower skills, availability of resources, turnover, availability of required licenses, etc. shall be taken up and shall be documented before considering his name for the enquiry.

11.3.2 Service Provider has to follow all Policies and procedures laid down by GACL for securing IT assets.

11.3.3 Non-Disclosure Agreement (NDA) clause to be signed by the service provider, as applicable.

11.3.4 Due approval as per the company's work order procedure shall be sought as per the quantum of work to be awarded.

11.3.5 Feedback from the existing client of a particular service provider shall be sought verbally or in writing from such contact persons of the clients and it will be documented appropriately.

12. CLEAN DESK POLICY

12.1 Objective

The purpose and principle of a "Clean Desk" policy is to ensure that confidential data is not exposed to individuals who may pass through the area such as members, service personnel, and thieves. It encourages methodical management of one's workspace. Because of the risk of being compromised, confidential information should always be treated with care.

12.2 Scope

This policy applied to all employees or third party who are using IT assets

12.3 Policy

12.3.1 All employees should take appropriate actions to prevent unauthorized persons from having access to member information, applications, or data. Employees are also required to make a conscientious check of their surrounding work environment to ensure that there will be no loss of confidentiality to data media or documents.

12.3.2 Users shall ensure that their desk is kept clear of unnecessary paper documents during and after office hours. While leaving, users must ensure that all paper documents and files are locked away in cabinets.

12.3.3 Users shall ensure that all prints are immediately collected from the printer tray and fax machines.

12.3.4 Users shall make sure that their computer screen is locked while they are away from their computer

12.3.5 Sensitive information on paper that is to be shredded must not be left unattended to be handled later. They must be shredded immediately, or securely stored until the time that they can be shredded.

13. PASSWORD POLICY

13.1 Objective

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of GACL's entire corporate security. As such, all GACL employees (including contractors and vendors with access to GACL systems) are responsible for taking the appropriate steps to secure their passwords.

13.2 Scope

This policy applied to all employees or third party who have account or id to access the GACL intranet or any IT Systems.

13.3 Policy

13.3.1 It is recommended to change the password time to time to maintain confidentiality and passwords must be changed every 90 days.

13.3.2 Users will be fully accountable for their passwords and any access related to these passwords

13.3.3 Do not share your passwords with anyone, including assistants, supervisors or co-workers.

13.3.4 Do not reveal a password over the phone line, in email messages, in any questionnaires or in any security forms.

13.3.5 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system without encryption.

13.3.6 Passwords should be at least of 8 alpha-numeric characters and contain special characters such as #, @, ! etc.

13.3.7 PCs must not be left unattended without enabling a password-protected screensaver or logging off the device

13.3.8 The same password must not be used for multiple accounts.

14. DISPOSAL OF OLD HARDWARE/EXTERNAL MEDIA/ SCRAP OF E-WASTE

14.1 Objective

All hardware has a useful life. Once the useful life of the hardware if over, the hardware can be disposed off in form of a scrap or e-waste. It has to be ensured that no sensitive information is passed on while scrapping of IT assets.

Scrap or E-Waste is generated in the form of consumables like Printer Cartridges, Old Magnetic Media and Obsolete Computer Hardware viz. Desktops, Laptops, Printers, Scanners etc.

14.2 Scope

The scope of hardware disposal is applicable to all GACL employees and third party working for GACL and using GACL hardware.

14.3 Policy

14.3.1 The old desktops and laptops which are not working and are unusable are replaced with the new ones as per the need. Useful parts of the old machines are used and the old machines are stores in a specified location for disposal as scrap or e-waste.

14.3.2 All the equipment's such desktop, laptops or external media which is to be disposed off will be wiped of all data before disposal.

14.3.3 It is the responsibility of the users to take proper backup of the data before asking for a new machine. IT Department can help transfer the data from the old machine to the new machine but will not be responsible for the loss of data.

14.3.4 E-Waste of empty consumables are being sent to designated bins in the Scrap Yard of Stores Department under intimation to Stores Department and further

disposal activities of the consumable Waste is being taken care by Stores Department.

14.3.5 E-Waste of Obsolete Computer Hardware viz. Desktop, Laptop, Printers, Scanners etc. are scrapped through Stores in line with the Scrap Procedure defined as per Purchase Policy.

15. PRIVACY AND PERSONAL DATA PROTECTION POLICY

15.1 Objective

Privacy and confidentiality of personal data are important values for GACL. Normally, users can expect that their communications and the contents of their accounts will be treated as private and confidential and that their files will not be accessed without their permission. However, individuals have no right to absolute privacy when using information technology at GACL. GACL owns the information technology infrastructure and is responsible for its use. Company reserves the right to take action to see that its information technology is used lawfully, appropriately, and efficiently in pursuit of the primary purposes of the company.

15.2 Scope

This policy applied to all employees or third party who or using GACL's IT resources.

15.3 Policy

15.3.1 IT department may deploy monitoring tools, as need may be, to access any file, data, program, or e-mail in order to gather sufficient information to diagnose and correct network, hardware, and software problems or maintaining legal compliances. This work will be carried out in judicious manner.

15.3.2 For routine system administration, IT department can monitor levels of network traffic, use software that logs network activity, make copies of files, and maintain archives of these copies.

15.3.3 IT Department will gather and release information that is normally confidential when specifically requested by management of the company.

15.3.4 Employees shall treat the personal data of the other employees, customers and business partners fairly and lawfully. Employees entrusted with the task of collecting personal data shall do so only for specific, lawful, explicit, and legitimate purposes in furtherance of the GACL's business. Further employees shall process such data consistent with those purposes.

15.3.5 Employees must not use GACL data or system for any illegal or unauthorized uses.

15.3.6 Employees shall protect personal data that is in his/her custody from unauthorized access

15.3.7 Employees shall ensure that said data is appropriately destroyed after the business purpose is served.

15.3.8 Employees shall disclose and divulge data only with authorized personnel and in line with the procedures laid out by the organization

15.3.9 Employees shall obtain and process only the data that is necessary and directly related to his/her duties; and will not collect excessive personal data than required

16. REMOTE WORKING SECURITY POLICY

16.1 Objective

Remote working allows employees to work at home. It is a voluntary work alternative that may be appropriate for some employees and some jobs which need to be carried out in other than office hours.

16.2 Scope

This policy applied to all employees or third party who or using GACL's IT resources.

16.3 Policy

16.3.1 Employees must be connected to GACL's VPN at all times while accessing GACL's Systems remotely.

16.3.2 Employees must not use unsecured public WiFI for accessing GACL systems.

16.3.3 Users must ensure that they create a strong, unique password to connect to their home router. They should also change the SSID, enable the strongest network encryption protocol available, and limit access to specific MAC addresses.

16.3.4 Employees must enable two-factor or multi-factor authentication where applicable.

16.3.5 Employees must ensure that their devices are up-to-date on patches.

16.3.6 Employees should ensure that the IT assets are not damaged or lost while traveling or using it remotely. Employees should inform the IT department immediately in any of these events.

17. DATA BACKUP

17.1 Objective

Data is important asset of the organization. Hence it is imperative that it has to be secure and backed up in case of any adversity.

17.2 Scope

This policy applied to all employees or third party who is using GACL data.

17.3 Policy

17.3.1 Users shall take regular backups of the business data residing in their Desktop's, Laptop's and any other devices. Additionally, users must prioritize the backup of critical and sensitive data, and if deemed necessary, ensure a more frequent backup interval. The backup shall be taken only on assets which are owned by the organization.

17.3.2 Users shall not share/store any business information on their personal devices such as pen drive, external hard disks etc. or on email id's such as Gmail, outlook.com, Hotmail, yahoo etc)

17.3.3 The HoD of the respective department has to ensure that the data is backed up of the employees of their department and all necessary data is taken from the employee, when employee is leaving the company.

18. PHYSICAL ACCESS CONTROL

18.1 Objective

Physical access controls define who is allowed physical access to GACL facilities that house information systems, to the information systems within those facilities, and/or the display mechanisms associated with those information systems. Without physical access controls, the potential exists that information systems could be illegitimately, physically accessed and the security of the information they house could be compromised.

This policy applies to all facilities of GACL, within which information systems or information system components are housed.

18.2 Scope

This policy applied to Data centers, Data rooms, Switch and wiring closets or other facilities for which the primary purpose is the housing of IT infrastructure.

18.3 Policy

18.3.1 Employees must escort visitors within the company premises.

18.3.2 Access to IT facilities, information systems, and information system display mechanisms will be limited to authorized personnel only.

19. UNACCEPTABLE USE OF INFORMATION TECHNOLOGY

19.1 Objective

Following categories of uses, but not limited to, are summarized as unacceptable uses of information technology services provided by the company.

19.1.1 The retention or propagation of material that is offensive, obscene or indecent on the desktops.

19.1.2 Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights.

19.1.3 Data theft by any means or mode and of any document/information pertaining to GACL.

19.1.4 Unsolicited advertising often referred to as "spamming".

19.1.5 Sending e-mails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address.

19.1.6 Attempts to break into or damage computer systems or data held thereon.

19.1.7 Actions or inactions, which intentionally or unintentionally, aid the distribution of computer viruses or other malicious software.

19.1.8 Attempts to access, read, use, transfer or tamper with accounts or files that you are not authorized to use.

19.1.9 Using the Company network for unauthenticated access.

19.1.10 The downloading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid license, or other valid permission from the copyright holder.

19.1.11 The distribution or storage by any means of pirated software.

19.1.12 Connecting an unauthorized device to the Company network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and Policy relating to security.

19.1.13 Circumvention of Network Access Control.

19.1.14 Monitoring or interception of network traffic without permission.

19.1.15 Probing for the security weaknesses of systems by methods such as port scanning, without permission.

19.1.16 Associating any device to network Access Points, including wireless, to which you are not authorized.

19.1.17 Non-business activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs.

19.1.18 The deliberate viewing and/or printing of pornographic images.

19.1.19 The passing on of electronic chain mail.

19.1.20 Physical damage of any Information Technology system

19.1.21 The use of Company business mailing lists for non-business purposes.

19.1.22 The use of CDs, DVDs, and other storage devices for the purpose of copying unlicensed copyright software, music, etc.

20. PENAL PROVISION

Any breach to the Information Technology Security Policy may be liable for disciplinary action in consultation with the HR department and the HoD of the concern user.

21. TRAINING & COMMUNICATION

The policy will be communicated to all the existing employees through an appropriate channel. New joiners and third-party users will be communicated at the time of on-boarding.

Annual training sessions on the policy will be organized for the employees and third-party users. All the records related to the training imparted will be duly maintained.

22. GRIEVANCE REDRESSAL

Employees and third-party users are encouraged to reach out on email msbrd@gacl.co.in in case of any grievance and concern with respect to the information security and data privacy.

23. REVIEW AND GOVERNANCE

Any subsequent amendment / modification including in the laws related to Information Technology Cyber Security Policy shall automatically apply to this Policy. The same shall be added / amended / modified from time to time as authorized by the Board of Directors with due procedure.

The Managing Director is authorized to amend or modify the Information Technology Cyber Security Policy, in whole or in part, from time to time.