G R INFRAPROJECTS LIMITED

GRIL POLICIES & PROCEDURES			
Policy Name	IT End User Policy	**Number**	GRIL/IT/2022-10

Table of Contents

Introduction 1

Policy Objectives 2

Scope 3

IT Acceptable Usage Policy 3

Policy Statement 3

Policy Maintenance 3

Policy Requirements 3

Access, Identification & Authentication to IT Systems 3

Service Desk 4

Control of Personal Computers 5

Email Usage 5

Internet Usage 6

Data protection and Privacy of Company Private and Confidential information 8

Security standards for incident reporting 8

Software Usage 9

Cyber Security Awareness 10

Asset management 11

Responsibility of assets 11

Media Handling 12

Clear Desk 12

Clear Screen 13

Physical Security 13

Employee Exit 13

Introduction

End Users are the weakest link in information security as many of the cases leakage can be avoided if the person involved can have better knowledge in data protection. Users are recommended to develop information security mindset, build, and reinforce good practice through regular updates of information security awareness.

Policy Objectives

The purpose of this policy is to ensure that employees are aware of their responsibilities when using equipment and information systems provided by G R Infraprojects Limited ("GRIL").

- To provide guidelines to end users to ensure computer facilities are used in a professional manner and in a way that does not compromise GRIL's business, reputation, or its employees in any way.
- Minimize the threat of accidental, unauthorized, inappropriate (Oral, Written, Technical) access to either electronic or paper-based information owned by GRIL or temporarily entrusted to it
- To ensure implementation and compliance with GRIL IT security policy across all operations.
- To familiarize users with appropriate etiquette (Authenticate Use) for workstation, Internet, email, and general usage of IT facilities.

Scope

The scope of this policy applies to all users of GRIL including employees, third party vendors, contractors, temporary staff etc. to follow the Acceptable Usage Policy.

IT Acceptable Usage Policy

Policy Statement

Information Technology (IT) equipment and systems are an integral feature of GRIL's business operations. The aim of this policy and guidance is to ensure that employees are aware of their responsibilities when using the equipment and information systems provided by GRIL for them to carry out their work; to clarify the bounds of personal use; and to underline the seriousness with which the GRIL views the inappropriate, unlawful, or malicious use of the IT equipment Vs systems provided.

Policy Maintenance

End users will be informed of any subsequent changes or updated versions of such standards, guidelines, and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from GRIL Intranet or other relevant communication media on an on-going basis and accept the terms and conditions contained therein.

Policy Requirements

Access, Identification & Authentication to IT Systems

- Users will be issued with a user identity and granted access to IT systems post HR and IT Head approval.
- The IT department will issue an initial ID and password to be used to access the system. This password must be changed immediately upon IT Asset issued, by the user or when prompted by the system. Users should use passwords which are:
  - ✓ At least 9 characters long.
  - ✓ Does not contain your username, real name, or company name.

- ✓ Check if significantly different from previous passwords. Previous 3 passwords shall not be used. Passwords that increment e.g., Password1, Password2, Password3 ... are not strong.
- ✓ Contains characters from each of Upper Case, Lower Case, Numbers and Special Characters i.e., complexity requirements are met.

- A password protected screensaver is automatically activated following a period of inactivity and can be activated manually.
- To support GRIL sustainability objectives, users are expected to shut down their PCs, monitors and other devices i.e., Printers Etc. at the end of the working day.

Note: 1. Maximum Password Age of 90 days
2. Minimum Password Age of O days

Service Desk

- GRIL Help Desk service provides with a single point of contact that is geographic and platform- independent.
- Through this Help Desk, the issues reported will be registered, acknowledged, validated, investigated, and resolved. End-users can track their requests and are informed of associated status.
- It helps reduce service disruptions and improve user satisfaction.
- The support request methods are available at GRIL.
  - ✓ Through the online Helpdesk system
  - ✓ By calling to Helpdesk number (Service Desk)
  - ✓ By sending Email to service desk.
- The IT service desk should be the first point of contact for end users for below activities.
  - ➢ Access Rights Management
  - ➢ IT Asset allocation
  - ➢ Return of the IT asset
  - ➢ Problem and disruption of IT services
  - ➢ Network Connectivity, access to printers and shared folders etc.
  - ➢ Software installation
  - ➢ Access to new internet website
  - ➢ Reporting of suspicious or untrustworthy activities like virus detection

- Account lockout or password reset related queries.
- Others

Control of Personal Computers

- Individuals should contact the IT Service Desk when experiencing problems with their computer and hardware and must not attempt to fix any problems themselves.
- Individuals must take care to ensure that laptop computers or other devices are kept securely, particularly when travelling to or from the workplace.
- Any losses must be reported immediately to the Service Desk.
- Individuals shall be liable to replace or pay an equivalent amount to the organization in case of theft, loss, or physical damage to the property.
- The organization retains the right to deduct the same from the salary in case of such an event.

Email Usage

Employees using GRIL email system must adhere to following guidelines:

- GRIL's email system, network and Internet access is intended for business use only.
- Email Accounts shall not be synchronized with unauthorized mobile devices.
- All information created, sent, or received via GRIL's email system, network, internet including all e-mails and electronic files, is the property of GRIL.
- Employees should have no privacy regarding this information. GRIL reserves the right to access, read, review, and monitor and copy all files on its computer system at any time and without notice.
- Before sending mail, the sender must ensure the correct email address is used for the intended recipient(s).
- Any message or file sent via email must have the employee's signature consisting of employees.name and designation.
- Alternate internet service provider's connection to GRIL's internal network is not permitted unless explicitly authorized by Domain Head and properly protected by a firewall or by implementing other appropriate security controls.
- Restricted/Confidential information should not be sent via email unless encrypted or password protected at the time of transmittal.

- Employees should exercise sound judgement when distributing messages. Employees must also abide by copyright laws, ethics rules, and other applicable laws.
- Email messages must always contain professional and appropriate language. Employees are prohibited from sending abusive, harassing, intimidating, threatening, discriminatory or otherwise offensive messages via email.
- Chain messages and exe, graphics and/or programs should be deleted and not forwarded.
- Email messages must contain the following disclaimer.

"This message (including any attachments) may contain confidential, proprietary, privileged and/or private information. The information is intended to be for the use of the individual or entity designated above. If you are not the intended recipient of this message, please notify the sender immediately, and delete the message and any attachments. Any disclosure, reproduction, distribution or other use of this message or any attachments by an individual or entity other than the intended recipient is prohibited."

Internet Usage

To prevent any appearance of inappropriate conduct on the Internet and to reduce risk to the organization, GRIL shall not be liable for any user activities on the internet. Users shall access the internet only for business purposes and should not perform the following activities:

- Enter into contractual agreements via the Internet, e.g., enter binding contracts on behalf of the organization over the Internet.
- Use the organization's logos or the organization's materials in any web page or Internet posting unless it has been approved, in advance, by the Organization Management.
- Solicitations for any purpose which are not expressly approved by Organization Management.
- Represent individual opinions as those of the Organization.
- Use software files, images, or other information downloaded from the Internet that has not been released for free public use.
- If a business need exists, then protective methods and software should be installed on the user's workstation to prevent hackers getting access to the data on the user's workstation.
- Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on the organization network or systems.
- Attempt to gain illegal access to remote systems on the Internet.

- Attempt to inappropriately telnet to or port scan remote systems on the Internet.
- Use or possess Internet scanning or security vulnerability assessment tools without the permission of the IT-Head.
- Post material in violation of copyright law.
- Reveal or publicize proprietary or confidential information.
- Establish Internet or other external network connections that could allow other organization users to gain access into GRIL systems and information assets.
- Use or download tools such as games, clip art, etc. These applications pose a potential virus and security threat to system functionality and compatibility concerns, in addition to professional integrity and legal implications.
- Connect the organization's system to the internet through PDA's, mobile phone.
- Conduct or participate in illegal activities, including gambling.
- Access or download pornographic material.
- Make or post indecent remarks.
- Upload or download commercial software in violation of its copyright.
- Upload or mail an organization's confidential documents without the permission/authorization of the concerned parties.
- Download any software or .exe, Audio, video, Apk's etc. files. In case somebody needs an excess to the same a prior approval from the IT Head is required after submitting business justification.
- Intentionally interfere with the normal operation of Internet gateway.
- Use Instant Messaging software like Google Talk, Yahoo, and MSN etc.
- Only below listed categories of allow-listed domains can be accessed:
  - ✓ Business and Economy
  - ✓ Education
  - ✓ Online Banking
  - ✓ Government
  - ✓ Health
  - ✓ Information Technology/Computers
  - ✓ Search Engines/ Portals
  - ✓ Web Communications
  - ✓ News and Media
  - ✓ Reference

- ✓ Shopping
- ✓ Real Estate
- ✓ Restaurants & Dining
- ✓ Travel
- ✓ Vehicles

- For accessing any domains other than those listed above, approval from the Department Head and IT Head shall be required.

Data protection and Privacy of Company Private and Confidential information

- Sensitive personal data, Company Private and Confidential information or information of a person means such personal information collected, received, stored, transmitted, or processed by corporate body or intermediary or any person, consisting of: -
  - ➢ Password
  - ➢ User details as provided at the time of registration or thereafter.
  - ➢ Financial information such as Bank account or credit card or debit card or other payment instrument details
  - ➢ Call data records
  - ➢ Biometric information
  - ➢ Personal Details i.e. Aadhar Card, PAN Card etc.
  - ➢ Company Documents, Data, Presentations MIS or any other important information.
- Any detail relating to the above clauses as provided to GRIL for providing service shall be protected from unauthorized access, modification, and disclosure in line with IT Act 2000 and IT Act (Amendment) 2008 and other applicable legislation and statutory/regulatory requirements.

Security standards for incident reporting

- Anyone within GRIL becoming aware of a security weakness or incident must report it to the IT Department as soon as possible. A security incident is any incident that may affect or has affected:
  - o The confidentiality of the GRIL's information.
  - o The integrity of the GRIL's data.

- The availability of the firm's IT systems.

- Here are some examples of security incidents that require a report to the IT department:
  - A virus found or suspected.
  - An operational incident like software or data corruption, hardware failure.
  - IT equipment lost, damaged or stolen.
  - Unauthorized people entering GRIL premises and utilizing GRIL network.

Software Usage

Employees should use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyright software (except for backup and archival purposes by designated managerial personnel) is a violation of copyright law. To ensure compliance with software license agreements **employees must adhere** to the following:

- Employees must use software in accordance with the manufacturer's license agreements.
- Employees should acknowledge they do not own any software or related documentation.
- Unauthorized duplication of software is **prohibited.**
- Employees are not permitted to install their personal software onto computer systems at GRIL network. Employees are not permitted to copy software from GRIL's computer system for installation on home or other computers without prior authorization.
- Employees are prohibited from giving computer owned software data to other persons not employed by GRIL. Under no circumstances will GRIL use software from unauthorized source, including, but not limited to, Internet, home, friends and/or colleagues on GRIL's computer system.
- Use of any software or tools to examine /test the network or workstations without authority is prohibited.
- Request for the software installation must followed through service desk team.
- Installing software without prior written approval of IT Head is prohibited.
- The following software's shall be installed onto computer systems at GRIL network:
  - Microsoft Windows 10 Pro (Licensed)
  - Adobe Acrobat reader
  - McAfee
  - Win Rar
  - Google Chrome

  - Printer Drivers
  - WPS office

- Below mentioned software's can only be installed post approval from IT Head:
  - Microsoft O365 office (Licensed)
  - Adobe Photoshop (If required)
  - Auto CAD (If required)
  - Corel Draw (If required)
  - SAP Client (If required)
- For installing software other than the above-mentioned list of software, prior approval from the HOD and IT Head shall be required.
- Using software that is not licensed by the manufacturer or approved by GRIL is prohibited.

Cyber Security Awareness

- Users should not open any files attached to an e-mail from an unknown, suspicious or untrustworthy source.
- Users should not open attachments that are from an unknown or non-trusted source.
- Users should not open any files attached to an e-mail whose subject line is questionable or unexpected. If there is a need to do so, they should always save the file to the hard drive before doing so.
- Users should delete chain/junk e-mails and not forward or reply to any of the chain/junk mails. These types of e-mail are considered as Spam, which is unsolicited and intrusive that clogs up the network.
- Users should exercise caution when downloading files from the Internet and should download. only from a legitimate and reputable source. Verify that an anti-virus program checks the files on the download site.
- Users should store all critical data on the GRIL fileserver or provided Cloud **Microsoft One Drive** to enable regular back up of the data. If a virus destroys the data files on the users' desktop, they can be replaced with the back-up copy. The backup files should be stored in an off-site location.
- Both inbound and outbound email messages should be scanned for viruses.
- Always scan CDs, USB pen drives etc. from an unknown/unsecured source for viruses before using it, if you are entitled to access those media.

Asset management

Responsibility of assets

- **Inventory of assets:** The Information Security Management System (ISMS) applies to the IT assets (including asset types - Physical, Software, Paper, People, Information, Service and Site) of GRIL, for the business functions and office location. All GRIL IT assets are listed in the information asset register. The asset type comprises of physical assets, software assets, paper assets, people assets, and site as an asset, information asset and service as an asset. The information asset inventory shall contain the following information as minimum:
    1. The type and location of asset.
    2. The Asset owner and Custodian.
    3. The classification of the asset (i.e., restricted, confidential, internal only, public).
- **Stewardship of asset:** The asset owner (GRIL IT Team) shall be responsible for the appropriate classification, maintenance of Asset. The asset owner may delegate the responsibility of the maintenance and protection of the information asset to an individual/function referred to as "Asset Custodian".
- **Acceptable use of assets:** GRIL (IT) shall ensure that there are rules defined for the acceptable level of use for all the assets of GRIL. Also, GRIL (IT) shall educate the employees, contractors and third parties to follow the below guidelines for the acceptable level of use of all the assets.
    - Assets such as data, systems, software, or an account shall only be used for business and operational purposes of GRIL.
    - Assets shall be protected from unauthorized usage and formal procedures shall be followed.
    - developed for handling and storage of information assets based on their classification to protect the information asset from unauthorized disclosure or misuse.
    - Individuals are required to handover the assets back to IT, when they are either transferred across locations, separating from project or separating from the organization.
    - Changes in function or roles may also warrant return of the assets, otherwise IT function will not provide, or role change the clearance.

- Individuals should maintain assets in working conditions and avoid any physical damage to hardware assets. In case of any damage or loss of functionality, the IT function should be informed immediately.

- **Replacement of Assets:** The replacement of Asset, we will be in sole discretion of IT Departments evaluation. The replacement of assets is applicable for the below cases, after approval from IT head.
  - If the Laptop/Desktop is damaged physically and not repairable.
  - If the asset is more than 5 years old and has performance issues.

- **Usage of Data Cards:** Data cards shall be issued on a temporary basis for individuals travelling remotely. For the permanent issue of data cards, approval from IT Head and Function Head shall be required.

Media Handling

- **Management of removable media**: Removable media shall be managed in accordance with the classification of the same. Records shall be maintained for all the media removed from GRIL. Approval shall be taken from Domain head for the use of removable media for business purposes. Employees shall get proper authorization from the Domain Head if removable media are required to be taken out of office premises. Removable media shall be sanitized before being issued to the employees. The contents of any re-usable media shall be made unrecoverable before putting it to re-use.
- **Disposal of media:** Media containing critical and sensitive information shall be disposed of in a secure manner as per approved procedures. The technique used for the disposal of media shall depend on the type of media and the classification of information present in the media. Authorized persons shall do the disposal of the media. The organization can select a suitable external party for collection or disposal of media.
- **Physical media transfer:** Removable media carrying information of Restricted or Confidential classification shall be transported using only the services of authorized vendors and all employees and third-party staff carrying media are required to ensure its appropriate employees and third-party staff carrying media are required to ensure its appropriate protection during transit.

Clear Desk

All employees shall ensure that:

- Sensitive information is kept in a secure location e.g., storage in a locked drawer, file cabinets etc.
- All non-public documents when printed or scanned are cleared from printers or scanners. Immediately.
- Unauthorized use of photocopiers and other reproduction technologies (e.g., scanners, digital cameras etc.) is prohibited.

Clear Screen

- Users shall log off or lock their computers (by using Windows key + L) when leaving it unattended for any period.
- A password, token or similar user authentication mechanism shall control computer terminals when unattended. Password protected screen saver will be activated within 1O minutes of user inactivity.
- Users should turn off computers or log off all network resources at the end of each day.

Physical Security

- Users should not allow any unauthorized person to enter the GRIL's data center.
- Users should not take in or out any equipment from the Company without authorization.
- For visitors, mobile phones with cameras are not allowed inside the Company's Data Centre or Server/Network Rooms.
- Users should adhere to all physical security standards to be followed in the Company.

Employee Exit

- Any asset assigned to user shall be returned by him/her to the IT Department in working condition.
- Individuals shall be liable to pay an equivalent amount to the organization in case of any physical damage, theft, or non-working of asset.
- The organization retains the right to deduct the same from the salary in case of such an event.
- The IT Team shall be responsible for disabling all access/authorization given to the user.