Reviving Green Revolution Cell

End User IT Policy

REVIVING GREEN REVOLUTION

An Initiative of TATA TRUSTS

Table of Contents

1.0 Introduction

1.1 Purpose

The purpose of this policy is to outline the necessary rules to ensure the usage of laptop/PC's and installed application is not violating the cyber safety as well as to ensure the safety of organizations hardware's also, and recovery of IT services in the event of a disaster or any form of service disruption.

The purpose of IT policy is to provide users with rules and guidelines about the appropriate use of RGR's' equipment, network and the Internet facility.

1.2 Coverage

This policy applies to employees, contractors, consultants, interns, and other workers, including all Third parties (collectively called Users) having access to the RGR's equipment, information and systems, Internet facility and electronic communication (E-Mail) services.

This policy applies to all Systems owned, Leased or used by RGR as well as any non-RGR owned system or devices that connect to RGR's' resources.

This policy will cover the following component related to IT infra and supports.

1. Acceptable usage of Work laptops,
2. Acceptable usage of office internet
3. Backup and redundancy mechanisms

1.3 Responsibilities

The Executive Director, RGR is responsible for ensuring that all stakeholders in critical RGR' Applications are aware of RGR's IT Policy. The Users are responsible for not compromising RGR in any way through the use of organizational equipment's, Internet / e-mail facilities

2 Definitions

'*Users*' includes all employees, associates, temporary staff, and other vendors with a RGR-owned or personal computer connected to RGR' network.

'*Vulnerable and Malicious domains*' are sites that will respond differently depending on the User Agent or Referrer and might lead to infections with harmful viruses and malwares if the user's machine is infected.

'*Backup*' describes the process of creating and storing copies of data to protect the organizationagainst data loss.

3 Policy Guidelines

The organization shall adopt appropriate practice and mechanism within the organization toensure the following:

- Acceptable usage of Work laptops,
- Acceptable usage of office internet
- Backup and redundancy mechanisms to ensure the security for organization's equipment'sand data.

The following controls shall be enabled for the same.

3.1 Acceptable usage of Work Laptop

This document serves to outline the organization's policy on the use and storage of your laptop. This is intended to minimize the organization's exposure to information security risk as well as to increase the user's personal safety and safeguard the organization's hardware investment.

3.1.1 Physical security controls for laptops

- The physical security of laptop is user's personal responsibility is required to take all reasonable precautions.
- ▪ Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel.
- ▪ Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock itout of sight in the trunk or glove box but it is generally much safer to take it with you.
- ▪ Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage.
- If it is lost or stolen, user must notify the Police immediately and inform the IT Help/Service Desk as soon as practicable (within hours not days, please).

3.1.2 Virus protection of laptops

- Viruses are a major threat and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software must be updated at least monthly. The easiest way of doing this is simply to log on to the network for the automatic update process to run. If you cannot log on for some reason, contact the IT Help/Service Desk for advice on obtaining and installing anti-virus updates.

3.1.3 Controls against unauthorized access to laptop

- Users are personally accountable for all network and systems access under their user ID, and must keep their password secret.
  - Users' laptops are for official use and should not loan it or allow it to be used by otherssuch as family and friends.
  - Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine. Other controls for laptops

3.1.4 Unauthorized software

- Users must not download, install or use unauthorized software programs. Software packages that permit the computer to be ‘remote controlled’ (e.g. PC anywhere) and ‘hacking tools’ (e.g. network sniffers and password crackers) are explicitly forbidden on equipment unless they have been explicitly pre-authorized by management for legitimate business purposes.

3.1.5 Unlicensed software

- Users must be careful about software licenses and unless they are specifically identified as “freeware” or “public domain software”, may only be installed and/or usedif the appropriate license fee has been paid.
- Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period.
- Some software is limited to free use by private individuals whereas commercial use requires a license payment, hence users are restricted from installing such software

3.1.6 Laptop Backups

- Users must take backups of their own data on the designated cloud storage as deemedby the organization.
- Backup to cloud can be automated or manually synched but it is users responsibility to contact IT helpdesk to remedy any issues in their system related to the Cloud backup utility.

3.1.7 Laws, regulations and policies

- Users must comply with relevant laws, regulations, and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example.

3.1.8 Inappropriate materials

- RGR will not tolerate inappropriate materials such as pornographic, racist, defamatory, or harassing files, pictures, videos, or email messages that are deemed offensive or cause for embarrassment to organizations reputation. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites.

3.2 Acceptable usage of Internet Use

All Users are expected to adhere to the following guidelines while using internet facility provided bythe office

- User’s access to Internet use is provided as long as it helps in increasing productivity and it is used responsibly.
- Users can be banned and blocked by the RGR if considered harmful to the productivity and RGR’s operations as a whole.

- Users must not visit internet sites that contain obscene, hateful or other objectionable material, shall not attempt to bypass the RGR web content filtering controls and shall not make or post indecent remarks, proposals or materials on the internet
- The RGR' Systems shall not be used as a forum to promote religious or political causes, or any illegal activity. Likewise, offensive or improper messages or opinions, transmission of sexually explicit images, messages, objectionable cartoons, or other such items, or messages that may be construed as harassment or disparagement of others based on race, color, age, national origin, religion, sex, veteran status, disability, or any other status protected under applicable international, federal, state, and/or local law are also prohibited on the RGR's Systems.
- Users shall not download illegal software from the internet, execute, or accept any illegal software programs or other code on the internet.
- Users will not carry out any other inappropriate activity as identified from time to time by RGR and will not waste time or resources on non-RGR activities
- Users shall not share any sensitive, objectionable or confidential information on social media.

- The equipment available for users at the working place belongs to the RGR & any data transmitted, created and received or any website visited and content downloaded canbe monitored by the RGR.
- Users must never share their personal passwords to any RGR System, and shall not attempt to gain access to another User's systems and messages. The RGR, however, reserves the right to access RGR's any systems including but not limited to, email and voice mail messages at any time, without notice to the Users.

3.3 Backup

The organization shall adopt appropriate backup and redundancy mechanisms to ensure the availability of IT systems and services. The following controls shall be enabled for critical systems and services:

3.3.1 Regular backup and restoration

- Establish and operate a process for regular backup and restoration depending on thebusiness criticality and sensitivity of data.
- Daily incremental back-ups of essential information and software.
- The application owners should ensure that the one-time backup of key data like sourcecode, executable, etc. are shared by the technology partner post go-live.
- In addition to the scheduled backups, backups shall be taken in case any of thefollowing events occur:
- Change including operational or configuration changes
- Change or upgrade of an operational system

- Prior to installation of software or operating system patches or security updates
- Backup retrieval and restoration shall be tested regularly (at a minimum on an annual basis) and the results documented.
- In case of managed systems e.g., public cloud, IT Infrastructure team shall verify the readability of backups shared by the application developer, periodic restoration tests shall be carried out on the test systems by new or existing third-party vendor.

3.3.2 Provision infrastructure for user backups.

- Users shall ensure regular back up of critical data and ensure it's uploaded to designated cloud storage as deemed by the organization. e.g., MS OneDrive
- Users must take backups of their own data on the Backup to cloud can be automated or manually synched but it is users responsibility to contact IT helpdesk to remedy anyissues in their system related to the Cloud backup utility

4 Monitoring and review

The IT Infrastructure team shall verify compliance to this policy through various methods including but not limited to monitoring, reports, internal and external audits, and feedback of the policy owner.

- Any deviations in the plan shall be monitored and recorded appropriately and be recorded in the tracker.

4.1 Policy exception

The Executive Director must approve any exceptions of policy on recommendation of respective ReportingManager and Function Head.

5 Policy ownership and review

The owner of this document is the Executive Director. The owner is responsible to ensure the informationin this document is current and aligned with other related policies and guidelines.

- The document shall be reviewed on a yearly basis at a minimum or on a need basis toensure it remains relevant.