Rogers

Rogers Group Information Security and Technology Policy Manual

TABLE OF CONTENTS

INFORMATION SECURITY AND TECHNOLOGY POLICY

Introduction

Information management is an essential part of Information Technology (IT) governance, which in turn is a key aspect in corporate governance. An integral part of establishing an IT governance framework is Information Security and Information Technology controls. This framework sets out the policies and standards pertaining to the use of IT within the Rogers Group (the "Group").

Information Security relates to the following basic principles:

- **Confidentiality:** Information is not made available or disclosed to unauthorized individuals and/or entities.
- **Integrity:** Safeguarding the accuracy and completeness of information.
- **Availability:** Where accessible and usable upon demand by an authorized party.

Information Technology relates to business technology and its ever-increasing reliance on handling and optimizing the Group's business processes.

The Group is committed to safeguarding the confidentiality, integrity and availability of all its Information Technology Systems and Information Assets, to comply with regulatory, operational and contractual requirements.

This Information Security and Technology Policy (IST Policy) provides parameters and guidance to all Group employees in respect to the protection of all Information Systems and Information Assets.

The IST Policy is also available on the Rogers Website (www.rogers.mu).

Objectives

The objectives of this IST Policy are as follows:

- **Compliance:** Ensure compliance with the current laws, regulations and employee guidelines.
- **Security:** Establish an acceptable level of security for accessing Information systems and safekeeping Information data.
- **Control:** Maintain controls for protecting the Group's Information Systems and Information Assets against theft, abuse and other forms of harm or loss.
- **Responsibility & Ownership:** Motivate Group employees to be responsible for ownership of and knowledge about information security, in order to minimize the risk of security incidents.
- **Business Continuity:** Ensure that companies within the Group are capable of continuing their services and operations even if major security incidents occur.
- **3rd party Confidentiality:** Ensure that external service providers comply with the Group's Information Security requirements.
- **Accessibility:** Certify that this policy is accessible to all Group employees, business consultants and **3rd party** contractors.

Roles and Areas of Responsibility

This section defines the roles and responsibilities for users who have IT security or related governance responsibility for protecting the information and systems they operate, manage and support.

Role	Responsibilities
Guardian of the IST Policy	The Guardian oversees the compliance and controls set out in this IST Policy.
Author of the IST Policy	The Rogers Corporate Manager Information Systems is the overall author of this IST Policy. In collaboration with the Sector's Technology Managers, they shall ensure that this Policy is utilized and adhered to.
Chief Executive Officers	The ultimate responsibility for the effective implementation of the IST Policy and compliance thereto lies with the Group Chief Executive Officer in collaboration with each Sector Chief Executive Officer.
Sectors Technology Managers	Each Sector Technology Manager, in consultation with his respective IT Staff, is responsible for the development, management and maintenance of the Sector's Information and related Information systems in compliance with the IST Policy.
IT Staff	Sectorial IT Staff are personnel administrating the Company's Information Systems in compliance with the IST Policy.
Users	Employees, otherwise known as users are responsible for complying with this IST Policy.
Consultants and Contractual Partners	Contractual Partners and Consultants work in partnership with the Company. A signed confidentiality agreement is required, prior to accessing the Company's Information and Information systems.
Guests	One time or recurring guests must be restricted to limited or no access to Company data.

Compliance with the IST Policy

All users within the Group shall comply with the IST Policy herein contained.

All Contractual Partners and Consultants must conform to all guidelines set out in this IST Policy and this obligation should normally be found in the Confidentiality Agreement they sign.

Guests/visitors attending the Group's premises must be reminded not to misuse the Company's internet connection, disclose information and/or take photographs of restricted areas.

Policy Derogation or Exemption

A request for a derogation from or exemption to the IST Policy, would need to be documented as follows:

"*The following (Sector Name) are explicitly exempted from or can derogate from complying with the requirements set out in the Information Security and Technology Policy".*

The request must be addressed to the Author of the IST policy, copied to the Rogers Legal and Compliance Manager.

Policy Review

A request for an amendment to the IST Policy shall be channeled through the Rogers Legal and Compliance Manager in consultation with the Rogers Corporate Manager Information Systems.

Principles for Information Security

Integrated Risk Management Framework

The Group's approach to Information Security will be based on continuous risk assessments. These assessments will identify, quantify and prioritize the risks according to relevant criteria.

The Sectors Technology Managers will be responsible for ensuring that risk assessments within their area of responsibility are reported through internal control plans and when required with the assistance of an external IT Auditor.

Classification of Information Assets

Information Assets should be classified according to their security level and respective access control. Users administrating Information on behalf of the Group should treat the said Information according to its classification.

Classification	Description	Example
Sensitive	The highest level of sensitive Information that when disclosed to an unauthorized party, could lead to major theft and fraud, compromise the reputation of the Group, lead to regulatory fines or cause a confidentiality breach.	Examples include but are not limited to Sensitive Financial Information, Strategic Plans, Board Papers or documents relating to the Groups financing arrangements and/or Customer data records.
Confidential	Information that is Proprietary. Unauthorized disclosure could have a significant business impact for the Group.	Examples include but are not limited to Company Data Records, Minutes taken from management meetings and/or Payroll related Information.
Internal	Information intended solely for use within the Group. Provided freely to employees, but not for the public.	Examples include but are not limited to Company policies, standards and procedures and/or internal corporate communication.
Open	Intended for issue to the general public	Examples include but are not limited to Marketing materials, advertisements and/or published press releases.

Data Protection Act

The Group complies with the Data Protection Act 2017 (DPA). It has adopted a Data Protection Compliance Manual, which details how the Group complies with the DPA.

In addition, the Group has published its Data Protection Policy and Data Protection Notice on its website to explain to data subjects how their personal data are processed and maintained and what their rights are with regards to such data.

Human Resources and Information Security

The Group has established the controls set out below to enhance Information Security within the companies of the Group prior to employment, during, and after employment:

Prior to employment

Information Security Regulations should be embodied in the contracts when recruiting permanent employees, contractors and/or temporary staff.

During employment

Information Security refers to the requirements under the IST Policy and the responsibility for complying with the present IST Policy regulations.

These regulations should be:

- Reviewed regularly with all users and with all new hires.
- Made accessible through internal communication channels.

All users should receive adequate training and updating regarding the disclosed policy.

Termination or change of employment

Controls should be put in place to limit user's access to Company information upon resignation, and then user access should be closed upon termination or change of employment. The return of all IT assets should be handed in at the conclusion of the employment.

Information controls regarding Physical and Environmental Security

Physical and Environmental security in relation to Information Assets and computer equipment relates to the following key areas:

- Securing physical access to server rooms.
- Securing physical access to Company workspace.
- Clear desk and screen practice.
- Mobile equipment security.

Server Rooms

Company servers, switches, Uninterruptible Power Supplies (UPS), routers and/or any other relevant equipment must be hosted within a secure server room.

Measures for securing a server room should include the following:

- Adequate ventilation as well as protection against damages caused by water and humidity.
- Fire prevention systems, including alarms at critical points and fire extinguishers.
- Installing a door access control system.
- Video cameras at the entrance is recommended.
- Fireproof server cabinet.
- Flood alarms including if possible a raised floor.
- Suitable controls to ensure that only authorized personnel can access.

The Sectors Technology Managers are responsible for approving physical access to the server room by visitors and third-party contractors. This includes:

- Ensuring that works carried out must be suitably monitored.
- Escorting a visitor by a staff member from the IT Department or a Security Guard.
- Signed access Logbooks for identification purposes to be kept for reference.

Company Workplace

Measures for securing access to a Company office must include the following:

- Forms of identification for those requiring access.
- Visitor screening prior to entry.

Clear Desk and Computer Screen

All sensitive and/or confidential information must be removed from a user's workspace and/or locked away when the items are not in use.

Users must ensure that information in their hardcopy:

- Is secure in their work area.
- Is removed, and locked in a drawer when the desk is left unoccupied.
- When disposal is required, use an official shredder bin.
- Whiteboards and or Flip charts must be removed and/or erased after use.

Users must ensure that all printers, photocopiers and/or fax machines are clear of papers as soon as they are printed.

All computer equipment must be turned off or protected with a screen saver password when the workspace is left unattended.

Company Portable Devices

Information classified as Sensitive and/or Confidential must not be stored on a portable computer device (e.g. laptops, external storage devices, mobile phones and tablets) without the proper authentication (passwords).

If it is necessary to store this information on a portable device, access must:

- Be password protected.
- Be safeguarded using an encryption software.
- Have a screen lock security process using either a pattern password or PIN.

Company portable devices, are very often the target of thieves not, only because they want to resell the device but also because they know the data on those devices can be far more valuable. As such:

- Devices should never be left unattended and/or made visible in a vehicle.
- Never left unattended in public places.
- The device should be kept with the user the whole time.
- During air travel, should be treated as carry-on luggage.

Operational Procedures and Areas of Responsibility

Account Identity & User Access Policy

Definition and Purpose

The Account Identity and User Access Policy addresses how access to the Group's Information and Information Systems is controlled through the identification, authorization and authentication of users:

- Identification through user accounts is the mean used to identify users accessing the Group's Information Systems and/or Information assets.
- Authorization through access rights, addresses how access to Information assets is determined, granted and enforced.
- User Authentication is defined as the creation, usage and lifecycle of effective password management, critical to securing access.

The administration of user accounts and access privileges is to be restricted to suitably trained members of the IT Department, under the supervision of the relevant Sector Technology Manager.

User Account Management

User accounts should be traceable to a specific entity, to detect unauthorized access and/or processing activities.

The Sector Technology Manager in accordance with the Sector IT Staff must ensure that:

- Users attend all appropriate training courses prior to their user account being activated and deployed.
- Only one user is associated with an account. Shared accounts used to access Secure and/or Confidential Information are not permitted.
- Account management settings be set to enable, for lockouts after a set number of failed attempts. Access should then be locked for a minimum of one hour, unless a member of the IT Department intervenes.
- Audit trails and log files are to be kept and recorded for the creation, disabling, deletion and/or changes to user accounts.

The administration of all user accounts must include the following guidelines:

- All accounts must have a password that adheres to the practices outlined in the Password Management Policy document (See below). On first login, the user must change the default password assigned to the account.
- Accounts for contractors and/or consultants not affiliated with the Group, must have the prior approval of the account requestor.
- The naming convention for the creation of new accounts must include the user's name. The system shall use one or more letters of the user's first name and last name to create a unique identity.
- An account will be disabled and/or removed once a user has completed the duration for which the access was granted, (Applicable but not limited to Temporary, Trainee or Contractor accounts).
- An account will be immediately disabled when left idle for more than 25 days, and removed from all security workgroups when a user has terminated or changed his/her employment.
- Default user accounts provided with a purchased software must be disabled or used only for designated maintenance tasks and must not be employed for daily use.

Users must refrain from the practices set out below, which fall under the category of **unacceptable use**:

- The use of any account without a written request and approval notice.
- Accessing any system using another user's account credentials.
- Sharing of accounts between users.

User Access

All access requests must be, formally documented along with the access requirements, and approved by the applicable Head of Department and the Sector Technology Manager.

As such, the Sector Technology Manager together with the IT staff of the sector will be responsible for:

- Granting user access to Information Systems and Information assets.
- Restricting and/or limiting access upon a user's resignation date.
- Disabling access when a user ceases to have a legitimate reason to access the same, including but not limited to a termination or change of employment notice.
- Reviewing access at regular intervals, ensuring appropriate user rights are still allocated.
- Enforcing a dual factor authentication on critical accessible services.
- Allowing access to Information Systems and or information using privileged accounts.

Password Management Policy

Definition and Purpose

The Password Management Policy provides the best practices for the creation of passwords. This applies to all passwords including but not limited to user-level accounts, system-level accounts, server domain admin accounts, web accounts, e-mail accounts and privileged accounts.

The Policy applies also to all users, business consultants and third party contractors, who have or are responsible for an account (or any form of access that requires a password) on any system.

Password Creation Guidelines

Password creation should meet the following complexity characteristics:

- A minimum of 8 alphanumeric characters.
- Contain both upper-and lower-case characters.
- To include at least one special character **(for example !@#$%^:")**.

Users should refrain from the examples given below, which fall under the weak password creation category:

- Easy-to-guess passwords, especially "password".
- Your name, the name of your spouse or partner, or other names.
- A string of numbers or letters like "1234" or "abcd", or simple patterns of letters on the keyboard, like "qwerty".
- A phone number, your license plate number, a birth date, or other information easily obtained about you.
- Words that can be found in the dictionary.
- Identical to a user account.
- Any of the above followed or preceded by a single digit.

Password Protection Guidelines

- Passwords must not be inserted into email messages or stored on any file without proper protection.
- Users must not share password credentials and should take all reasonable efforts to avert accidental disclosure.
- Users may not use password managers or other tools to help store and remember passwords.
- Refrain from using the "Remember Password" feature on applications (for example, web browsers).

Any user suspecting that their password may have been compromised must report the incident to their respective Sector Technology Manager to enforce a password change.

Administrating Privileged Accounts

A Privileged Account provides elevated access to servers, switches, firewalls, routers, database servers, and the many applications they must manage. Privileged Accounts will be protected through isolation, obfuscation and accountability.

The following describes the best practices, which the Sector Technology Manager should follow in securing Privileged Accounts:

- Maintain an inventory of all Privileged Accounts in circulation.
- Refrain from sharing such accounts between IT Staff.
- Minimize the number of Privileged Accounts.

Examples of common Privileged Accounts are Local Admin Accounts, Domain Admin Accounts, Emergency Accounts, Service Accounts and Application Accounts.

Password Construction Practices for Privileged Passwords

- Configure a minimum password length of at least 10 characters for passwords or 15 for passphrases.
- Enforce password history, with at least 10 previous passwords remembered.
- Enable the setting that requires passwords to meet complexity requirements.
- Reset local admin passwords every 90 days.
- Reset service accounts passwords once a year during maintenance.
- For domain admin accounts, use strong passphrases with a minimum of 15 characters.
- Track all password changes by enabling password audit policies.
- Enable notifications for password expiration.

Password Protection Practices for Privileged Passwords

- Change factory default passwords before deploying any system or device.
- Upon resetting a user password, the default password must be changed at the first login.
- Default application, database, and system passwords shall be changed before moving into a production environment.

Email and Communication Policy

Definition and Purpose

The purpose of this Policy is to describe the acceptable use of the Group's email and related communication facilities ensuring integrity and confidentiality. This includes but is not limited to:

- Email platforms.
- Social chat rooms.
- Instant messaging services.
- Social media and blogging solutions.
- Video conferencing systems.

Corporate Email and Usage Guidelines

When using Company resources to access the Group's business email systems, users must realise they represent their Company and the Group.

In line with the standard practices of email etiquette, users shall be courteous, professional and business friendly in all emails related to the Company. This applies to the other forms of corporate communication tools mentioned above.

Users should refrain from the examples given below, which fall under **the category unacceptable use**:

- To upload, post, transmit or otherwise make available any material that may harm the Company's reputation.
- To send, transmit, or otherwise distribute sensitive and/or confidential information, data, trade secrets or other proprietary information belonging to the Company without the proper authorization.
- To send unsolicited messages, including "junk mails" or other advertising materials to individuals who did not specifically request such materials (email spams).
- To indulge in any form of harassment via email, messaging services, video, telephone or faxing, whether through language, frequency, or size of messages.
- To indulge in online defamation where false and/or damaging statements are made about another person through email, message boards, blogs, chatrooms, or any other Internet-based communication medium.
- To sign up for illegal, unreliable, disreputable or suspect websites and services using a Company designated email account.
- To use, or forge, unauthorised email header information.
- To create or forward "chain letters" of any type.
- To post the same or similar non-business-related messages to large numbers of user newsgroups (newsgroup spam).

Email Security

Email is often the medium of phishing attacks, confidentiality breaches, and other malware viruses. These issues can compromise the reputation, legality and security of the Group. Consequently, users should:

- Refrain from opening attachments and clicking on links when the content is not adequately explained.
- Be suspicious of clickbait headline titles.
- Be wary of requests for secrecy or bearing a sense of urgency, or also authority signs allegedly coming from your superiors that compels the user to act rapidly.
- Analyze email addresses and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).
- Be cautious when receiving any form of suspicious email.

- Avoid accessing personal email accounts within their Company's network.

Email Signature & Disclaimer

An email signature conveys professionalism and represents the Company well. Users should ensure that their Company address with contact details, Company logos and any work-related videos and/or links are located within the email signature.

Email Instructions for Money Transfer

Email Instructions for approving and or effecting any monetary transactions via an electronic fund transfer, to an external vendor, must be followed by a phone call from the instructor. This falls in line with the Dual factor authentication procedure.

Social Media & Blogging Guidelines

Social media blogging, using a Company-computer asset, is subject to the terms set forth in this section. Limited and occasional use of Company-computer assets to engage in blogging is acceptable, if done in a professional and responsible manner and does not interfere with an employee's regular work duties.

As such, users will be prohibited from:

- Revealing any sensitive, confidential or proprietary information or any other material covered by this Policy.
- Making any discriminatory, disparaging, defamatory or harassing comments using a Company computer asset or otherwise engaging in any conduct prohibited by the Equals Opportunity Act.

For companies within the Group that engages in social media activities, they will require a content specialist to manage postings and services to online campaigns. Their primary functions shall be to:

- Monitor the Groups social media channels.
- Review and act on all user-created content that may harm or tarnish the image and reputation of the Company and/or any of its employees.

Where a User Created Content is hateful, derogatory or abusive, the comment may be deleted or altered by the content specialist to fix the abuse. However, a response should always be made:

- To identify that the content was modified or deleted.
- To mention why the content was modified or deleted.
- To identify the complaint, criticism, or comment beneath the abuse and respond accordingly.

Internet Usage Policy

Definition and Purpose

Internet use, on Company time, using a Company device, connected to the Company network is authorized to conduct Company business only.

Users have a responsibility to:

- Use the Internet in a professional, lawful and ethical manner.
- Access the Internet through a computer authorized to link to the Company's network.
- Access the Internet through a computer safeguarded with a Company's anti-virus protection software.

Internet bandwidth resources and storage capacity have finite limits, and all users accessing the internet have a responsibility to conserve these resources. As such, users must not deliberately perform acts that will unfairly monopolise resources to the exclusion of others.

Users must refrain from behaviors detailed below, which fall under **the category "unacceptable use"**:

- Spending excessive amount of time engaging in online chat groups or other social media messaging services.
- Downloading large files through an Internet Download Manager software.
- Accessing, downloading and/or streaming audio and video sites.
- The illegal copying of material (software, files, graphics, documents and messages) protected under the copyright law or making that material available to others for copying.
- Otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.
- Any activity that would constitute a criminal offence.
- Visiting sites using Company resources containing inappropriate content such as but not limited to, "Drug Abuse, Hacking, Illegal or Unethical, Discrimination, Violence, Child Abuse, Alternative Beliefs, Adult Material, Gambling, Extremist Groups, Tasteless, Weapons, Internet TV and Radio, War Games, Online Gaming, Freeware and Software Downloads, Streaming Media, Malicious Websites, Web-Based Personal Email".

The Sector Technology Manager has the right to utilise means that makes it possible to identify and block access to Internet sites containing material deemed inappropriate in the workplace.

Downloading files from legitimate internet sites as well as sharing documents across the internet are common every day practices and can come with a set of risks, as mentioned in the EndPoint Protection Policy (refer to the next section).

Internet services allowing for File Sharing, Internet Telephony, Web based Applications and Social Networking Applications are often referred, to as resources. Any user who has a legitimate need to access such sites may contact the Sector Technology Manager for consultation and authorisation.

EndPoint Protection (Anti-Virus) Policy

Definition and Purpose

Security incidents related to computer viruses and malware threats, and the resulting cost of business interruption and service recovery continue to grow.

Implementing preventive malware and/or virus solutions, protective measures for unnecessary access to networks and computers, and cyber security awareness, are best practice measures that should be taken to reduce such incidents.

The purpose of this Policy is to describe the Group's requirements to prevent and address such threats and to identify the mitigating actions to be taken to reduce these risks.

The terms described in this policy refers to the following:

Term	Description	Example
A malware threat	A software developed by cyber attackers with the intention of gaining access and/or causing damage to a computer and/or network.	Includes but is not limited to Ransomware, Spyware, Computer worms, adware and Trojan malware.
A computer virus	A code designed to corrupt a system file, destroy data and replicate itself onto other machines without the user knowing.	Includes but is not limited to browser hijackers, File Infector and Macro Virus.
Antivirus and Anti-malware solutions	A software that identifies and possibly removes computer viruses, as well as Malware threats.	Norton Symantec, McAfee, Kaspersky and Sophos.

As such all Information Systems including but not limited to workstations and servers, whether connected to the Company network or as a standalone, must use an approved Company protection software.

Common sources of threats can be found from the following:

- Downloaded Programs and files (audio & video files, an e-book and images).
- Pirated, cracked or freeware software's (uTorrent, The Pirate Bay, Warez, Computer games).
- Emails containing attachments and/or URL links.
- Unpatched software (Microsoft Office without the latest security updates).
- Bluetooth transfers.
- Unsafe Internet websites.

The Sector Technology Manager should ensure that:

- Antivirus software is installed on all systems and devices connected to the Group's network. This applies to devices owned by Consultants and Contractual partners.
- Regular threat monitoring exercises should be conducted to detect, remove, and protect against known types of malicious software.
- Mechanisms in place to prevent users from disabling or modifying antivirus detection tools should be verified.
- The Anti-virus automatic update frequency should not be altered to reduce the frequency of updates.
- All servers including (on premise mail servers) attached to the Company's network should utilise an approved virus protection software safeguarding the Group's classification of information.
- Anti-virus mail gateways including Spam sentinel (Lotus Notes) and/or Advanced Threat Protection (Office 365) should be fully operational.
- IT Staff should be proficient with the incident response process in case an infection occurs.

Network Security Policy

Definition and Purpose

The purpose of this section is to establish the guidelines, and to communicate the controls necessary for a secure network infrastructure. It provides the practical mechanisms to support the Group's comprehensive set of security policies, which includes the management of:

- Real time detection systems to monitor activities within the internal network that reports any possible intrusion.
- Enforcing the use of a network vulnerability system, which will detect any possible weaknesses and the steps to remediate them.

To protect the integrity and confidentiality of information and mitigate the risk of a security incident, the following key principles must be applied:

Network administration

The Sector Technology Manager has the ultimate responsibility for supervising the Sector's internal network.

Users must refrain from adopting the practices listed below, which fall under **the category "unacceptable use":**

- Intended disruptions of network communication, which include, but is not limited to network sniffing, denial of service and forged routing information, are clearly prohibited.
- Intentional setting up of honey pots, honey nets or similar technology onto the Company network.
- Port scanning is clearly prohibited, unless engaged by an IT Staff.
- Introduction of malicious programs onto the network is forbidden.

Wireless Access

All wireless devices including laptops, smartphones, tablets, or other equipment are subject to the guidelines and procedures set forth in this section.

The following should, be implemented to reduce risks related to wireless security:

- Wireless networks should, be segregated between external guests and internal networks. Non-Company devices should not be connected to an internal wireless network.
- All default settings for wireless devices (e.g. passwords) should be changed prior to installing the equipment in a production environment.
- Strong passwords should be employed for all wireless SSID and changed on a periodic basis.
- All WIFI access points allowing connectivity to the company network should use the strongest available and feasible encryption mechanism to secure transmissions with wireless clients.

Firewall (Perimeter Security Management)

The role of a firewall is to protect the Group's internal systems and restrict unwanted access into the network.

The firewall performs the following security services:

- Manages access between the Group's Internal network and untrusted external networks.
- Blocks unwanted traffic as determined by the firewall administrator.
- Hides information, such as system names, network topologies, and internal user IDs from the Internet.
- Encrypts the transmission of data across the network.
- Logs traffic to and from the internal networks.

- Provides a virtual private network (VPN) connectivity.

Installation and Maintenance of Network Wiring

This section outlines the requirements for the installation, relocation, or removal of network wiring by cabling contractors. "Network wiring" refers to copper or fiber optic cables.

The Group's network cabling architecture, may be damaged if wiring is altered, removed, or relocated without the proper coordination from the Sector Technology Manager, leading to a potential loss of services.

The Sector Technology Manager must ensure that:

- Appointed Contractors are registered with an affiliated body.
- Approval is granted before any network wiring is altered, removed or relocated as part of any construction projects.
- Any installations to critical services and/or restoration works are duly supervised.

Acceptable Use Policy

Computer Usage

Users must refrain from the behaviours listed below which fall under **the category "unacceptable use"**:

- Unauthorized copying and/or using copyrighted material including but not limited to photos from magazines, books or other copyrighted sources, copyrighted music/films and the installation of any copyrighted software for which the Company or user does not have an active license.
- Using a company-computing asset to actively engage, in procuring material that is deemed highly offensive and/or illegal.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet.
- Providing information (including but not limited to Biometric fingerprint data) about, or lists of, employees to parties outside.
- Intentionally damaging or degrading performance on a Company-computing asset.
- The use of the Group's IT infrastructure for personal commercial activities.

Software Usage

The purpose of this section is to outline the acceptable treatment of software use within the Group. The Sector Technology Manager together with Sector IT staff are responsible for the management of software usage across their respective companies. This includes the following:

Authorized Software Use

- Only authorized software may be used on an issued Company-computing asset.
- Personal software that a user has acquired for Non-Company purposes shall not be installed, on any Company-computing assets.
- Obtainable types of freeware, shareware and open source software's shall not be downloaded, or installed without the prior written consent of the Sector Technology Manager.
- The use of cracked or pirated (copied) software is clearly forbidden.
- Software should not be or installed on more than one machine unless it falls under a volume license agreement.

Software Purchases

- Ensure all software purchases are from an authorised distributor.
- Be responsible for the renewal, and disposal of software licenses.
- Be accountable for the registration under the name of the Company and not an individual end-user.

Installation of Software Licenses

- The overall responsibility for installing any software licenses lies with the IT Staff and/or Sector Technology Manager.
- Ensure that software installation rights are disabled for all users.
- After installation, any media, licensing keys, and license agreements must be given to the Sector Technology Manager for secure storage and control.
- No software shall be installed if it is deemed that system security will be adversely affected by the software.
- All acquisitions of hardware that include bundled software shall be documented and identified to the Sector Technology Manager, who will verify that the Company has an appropriate license for the use of such bundled software.

Software Updates

Patch management is essentially a process for managing updates for software applications. Software patches correct bugs or problems within the software thus making it optimal for use and add compatibility with new hardware. The management of updates should, be defined through a centralized system allowing for the appropriate planning, configuration and deployment process.

This section of the policy is not limited to software updates on applications. It also covers the management of system updates including but not limited to firmware updates on physical hardware.

Removable Storage Devices

Removable storage devices typically consist of portable devices that can be used to copy, save, store and/or transfer data from one system to another. Media devices include but are not limited to USB flash drives, back up tapes, read/write CDs, memory cards, external hard drives and storage cards.

Data Security, Malware Infections, Copyright Infringement and Media Failure are the primary risks associated with the use of such devices.

Users shall ensure that USB scanning occur on all corporate computers whenever a drive is connected. This can help ensure no malware or malicious programs are on the drive as per the threat scanning process.

All sensitive and/or confidential information stored on any removable media devices must use an encryption software where possible. This reduces the risk of any compromise through unauthorized access.

Users shall refrain from the following, which fall under **the category "unacceptable use"**:

- The unauthorized storage of sensitive and or confidential information on any form of storage media device, without prior authorization from the Sector Technology Manager.
- Attempt to install applications or programs from storage devices onto a Company computer asset.
- The use of personal storage devices to store confidential and/or secure information.
- A Company storage device connected or used, on a personal computing asset.
- When in transit, all sensitive and/or confidential information stored on a removable media device must not be left unattended and must remain in an authorized user's physical control.

Cloud Usage

Cloud services often highlighted as cloud computer services offers the following:

- **Cloud storage:** Stores and backs up documents for regular access, sharing and synchronizing them across devices (Box, DropBox, One Drive, iCloud, Amazon Cloud).
- **Cloud backup:** Used as a backup source in the event of a potential data loss (iDrive, CloudBerry).
- **Software as a Service (SaaS):** Uses the internet to provide a particular service (Office 365, Google Apps, QuickBooks Online and Maas Mobile Device Management 360).
- **Cloud hosting:** Facilitates all types of information sharing, such as primary or backed up data storage, email services, application hosting, and web-based phone systems and data storage.

The use of cloud computing services for storing sensitive and/or confidential information must be formally authorized by the Sector Technology Manager given the exposure to online threats such as data loss and unauthorized access.

The Sector Technology Manager has the overall responsibility to certify security, privacy and all other IT management requirements with the cloud-computing vendor.

Computer Asset Disposal

The purpose of this section is to ensure that proper guidance, for disposing company computer assets is followed especially in relation to the destruction of, sensitive and/or confidential information, which the computer hardware may have processed and may still contain or have stored.

In this context, the focus shall be on the Asset Disposal and Destruction Procedures for unused Computer Equipment and if agreed by the Sector Technology Manager, the purchase of "end of use" Computer Equipment.

Unused Computer Equipment should be disposed of securely and safely when no longer required, using formal procedures.

These procedures include:

- A clear identification of Company computing assets that requires disposal.
- Implementation of actions for the disposal of Company IT assets.
- Disposal using a certified third-party supplier.
- Provision of certification and audit trail for asset disposal.

Company computing assets that requires disposal

All asset disposal requests must be formally submitted to the Sector Technology Manager through an asset disposal form.

Process for the disposal of Company IT assets

The Sector Technology Manager shall ensure that all:

- Visible files are deleted, and the hard disk formatted.
- Copyrighted software is uninstalled.

Approved Third Party Supplier/Service Provider

Where a licensed third-party service provider is to undertake secure disposal/destruction on behalf of the Company, the Sector Technology Manager must ensure the disposal criteria is met in accordance with this policy. The use of a degaussing service to effectively, remove all data from a computing hard drive, rendering it unusable is required.

Certification and audit trail

This is, submitted by an official degaussing data report, to be securely stored for reference purposes.

Unused computer equipment that is working, that has yet reached the end of its useful life shall be, treated as follows:

- Made available for purchase by employees. All purchases will carry no warranty or support.
- Returned to the Sector Technology Manager who shall assess whether the same can be donated through an affiliated CSR Programme, or alternatively disposed.

The Finance Department will determine an appropriate cost for each item. Additionally, they will ensure that the asset has been removed from the Asset Inventory register.

Remote Access

In the context of this policy, a remote access will be defined as any connection to the group's internal network and resources from an external location (home, hotel or another office). The purpose is to define rules and responsibilities ensuring that users are aware of the potential risks, whilst connecting from an offsite location:

- Requests for granting remote access must follow the Access Controls Policy.
- Authorized users shall protect their login and password, using controls set out in the Password Management Policy.
- All Company Owned Computers that are connected, to internal networks via remote access technologies must comply with the EndPoint Protection Policy.

It is the responsibility of all users and contractors, with remote access privileges to ensure that their remote access connection is given the same consideration as the user's on-site connection.

Secure remote access must be controlled with an encrypted Virtual Private Networks (VPNs) software.

Services such as Web Ex, TeamViewer and Go to Meeting, to name a few, are prime examples of freeware solutions allowing for a remote access from one site to another. The Sector Technology Manager will assist with authorizing temporary access and may be present whilst the remote session is running.

Mobile Phone Policy

Definition and Purpose

The purpose of this policy is to identify what the Group considers to be acceptable and unacceptable use of mobile work phones.

All references to "mobile phones" in this section includes any mobile phone or electronic device capable of remote communication, such as a smart phone or a tablet with a phone function and calling capability.

All forms of communication, including but not limited to, phone (and video) calls, text (or picture) messages, emails and instant messages.

The use of a mobile phone also includes accessing the Internet, for any purpose.

The Company will provide a cell phone corporate plan and device based on its employees function and needs. This will, be referred to as a Company Issued Cell Phone.

The Company may present alternative measures that will allow an employee to purchase a recommended mobile phone then receive a cost reimbursement, for the purchase amount. The Company will include a corporate mobile plan, governed by a security tracking system, used for accessing Company resources. This will, be referred to as a Bring Your Own Device cell phone scheme.

No user is to access the Company network and/or corporate email through a personal mobile device without the approval of the Sector Technology Manager.

Usage

Users enrolled on either a Company Issued Cell Phone plan and/or BYOD scheme will use their devices for:

- Making business calls.
- Using productivity apps.
- Business messaging, emails and Internet browsing.
- Internet tethering for business purposes.

Occasionally limited personal use may be permitted provided that, all call costs be identified.

Access to Company Resources

Access to Company resources including but not limited to email must follow the terms outlined in the Email & Communication Policy.

Security

In order to prevent unauthorized access, devices must be password protected using the features of the device. The device must lock itself with a pattern password or PIN if it is idle for less than five minutes.

Alternatively, the use of a Mobile Device security solution to preserve and secure the integrity of Company data on their mobile phones is highly recommended.

Confidentiality & Privacy

Users must be cautious when using their mobile phones in public places in order to avoid disclosing sensitive or confidential information.

Lost, Stolen or damaged devices

Users are accountable for all devices under their control. The following procedures provide for reporting of lost or stolen property. In case, a device is lost or stolen, the user:

- Must notify the Sector Technology Manager, so that necessary actions are taken to remotely wipe all Company data (where the device is governed by a mobile device security solution).
- Must submit all the required documentation relating to the stolen device, preferably a police report.

When travelling abroad

To ensure costs are controlled when connecting to a local mobile network, the user must refer to the following guidelines:

Data Roaming

- Contact your carrier prior to you travelling to activate a data roaming package.

Turn off Automatic Downloads, Push notifications and Location Services

- Such features must be turned off, as some applications will automatically download data while the phone is on thus generating additional roaming charges.

Pre-paid call/data packs

- We recommend that a local pre-paid sim card be purchased upon arrival. Top up scratch cards can be used with a defined data package that acts as an alternative to Data roaming.
- Alternatively, pre-paid global SIM cards, can be purchased allowing you reduced rates across multiple countries.

Accessing public WI-FI Hotspots

Users must be aware of the security risks when transmitting information over a public wireless network. Wi-Fi hotspots in coffee shops, airports, hotels, and other public places are convenient, but often they are not entirely secure.

Users must refrain from the following, which fall under **the category "unacceptable use"**:

- Excessive personal use and/or for commercial activities, such as running any sort of private business, advertising or performing work for personal gain.
- Any activity that would compromise the privacy of others including but not limited to the transmission of messages that contains any sensitive, confidential and/or personal Information regarding the Company, its employees and clients.
- To download, host or transmit forbidden content disclosed in the Internet usage policy.
- Any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to the Company. This includes but is not limited to Jailbroken or rooted devices.
- Use of mobile phone's camera or microphone to record sensitive and/or confidential Company Information.

Information Technology Continuity Planning

Definition and Purpose

The purpose of an IT Continuity Plan is to provide management with an evaluation of the Group's IT function's preparedness in the event of a process disruption.

The IT Continuity Plan forms part of the global Business Continuity Planning (BCP) programme which supports business continuity, disaster prevention and total business recovery.

Business Assessment Analysis

The Sector Technology Manager in collaboration with the respective management is required to perform a Business Assessment Analysis for each Information System utilized within his area of responsibility.

The assessment should define the Contingency Plan for the Sector. The Plan shall include the following:

- **Applicable Risk:** Analyse the level of risk and its likelihood.
- **Prioritization of Recovery:** Assess what services are critical and non-critical.
- **Recovery Time:** The duration of time within which a process, function and or system must be restored after a disaster or disruption.
- **Recovery Point:** The maximum tolerable period during which data might be lost from a system.

Contingency Plans

Each Information System must have a Contingency Plan documented for when a specific hardware, software or Network becomes defective or cease to function. This Plan should include an explanation of the system unavailability in the event of a disruption and the process that must be implemented to continue operations during the disruption.

Data Backup Plans

Each Sector Technology Manager should implement and manage a Data Backup Strategy Plan for their respective Sector. The Plan should define the following key requirements:

- Responsible parties within the Sector IT staff, to ensure that the backup of Data, particularly Sensitive and Confidential Data is successfully executed.
- A backup schedule including but not limited to daily, weekly, monthly yearly cycles.
- Information from the Business Systems that are to be backed up.
- Place the backup media is to be stored and persons who have access.
- Place the backup media is to be kept secure before it is moved to storage, if applicable.
- Persons who may remove the backup media and transfer it to storage.
- Restoration procedures to restore Business System Data from a backup media to the appropriate system.
- Test restoration procedures and frequency of testing to confirm the effectiveness of the Plan.
- A method for restoring encrypted backup media, including encryption key management.

Information Security Incident Management

Definition and Purpose

The purpose of this incident response plan is to prepare the Group to quickly and effectively contain a security incident whilst continuing normal business operations.

This policy refers to an Information Security incident as a potential threat to Information, a threat to a Computer System or a disruption of services.

The objectives of establishing a successful incident plan include:

- Analyze the impact of the security incident.
- Identify the cause to aid in reducing its likelihood of reoccurrence.
- Make available all information regarding the incident for analysis and notification.
- Ensure that all parties are aware of their responsibilities regarding incident handling.
- Protect the reputation of the Group.

Effective incident response involves every function within the Group, including but not limited to the Technology Manager and the IT team, the Legal and Compliance Department, Human Resources, Corporate Communications, and Business Operations.

Each security incident presents a unique circumstance that will require a case-by-case examination. However, the following guidelines may be implemented to contain an incident whilst continuing normal business operations.

Incident Discovery and Confirmation

- Describe how the security incident was first learned.
- Analyze audit logs to identify unusual behaviour that indicates a likely threat and/or confirm that the threat has occurred.
- Describe the responsible party.
- Identify the source of threat.
- Evaluate the extent of damage upon discovery and its potential risk.
- Inform management regarding the discovery.

Containment and Continuity

- Gather and protect evidence. Back up any compromised systems as soon as possible for forensic review.
- Increase security controls that will safeguard the system and/or infrastructure (Change passwords for all users/applications/network accounts, Remove systems from production or take systems offline, Close firewall ports and network connections, Blacklisting mail addresses and conduct vulnerability analysis).
- Inform management regarding the evidence obtained and the containment plan to avert a potential spread.

Eradication

- Remove all components related to the incident.
- Test devices to be sure any threats have been removed.
- Compare data before and after the incident to ensure systems are reset properly.
- Share with management the eradication results.

Recovery

- Restore all systems in order to return to normal operations and remediate vulnerabilities to prevent similar incidents (Restore from a backup, replace the compromised source and/or rebuild the system or environment).
- Download and apply security patches.
- Return any systems that were taken offline to production.
- Inform management regarding the recovery plan.

Lessons Learned

- A post-incident review.
- Assess incident cost.
- Implement additional training for all employees.

Communication Strategy

- Assess the impact of the incident to determine what should be communicated and to whom
  - Communication with the current Internal Management Team, The Rogers Legal and Compliance Manager and the Rogers Corporate Manager Information Systems.
  - Communication with external stakeholders including but not limited to customers, industry regulators and partners.

Certain insurers offer customized cyber insurance policies that can cover the following:

- Recovery costs in case of loss of data.
- Potential loss of turnover.
- Cost of communication in the event of an incident.

Terms and Abbreviations

Term	Description	Page
IST Policy	Information Security and Technology Policy	3
Company Website	www.rogers.mu	3
Group	Rogers Group	3
User	All Employees of the Rogers Group	4
Sector Technology Manager	Head of IT from each subsidiary within the Group	4
IT Staff	Refers to IT Administrators and or IT Technical support employed by a sector or outsourced through a third party service provider	4
Rogers Legal & Compliance Officer	Any further amendments pertaining to this policy will be channelled through the compliance officer.	5
Information Assets	Refer to as Company Information	6
Dual factor authentication	An additional security process in which the user provides two different authentication factors to verify themselves	11
Privileged accounts	A privileged account is an account that provides increased access and requires additional authorization. Examples include a network, system or security administrator accounts	11
Password Managers	An application that is used to store and manage user passwords such as Keychain, LastPass, and/or dashlane	12
Remember password	Stores the usernames and passwords you use to access websites and then automatically fills them in for you the next time you visit a website	12
Factory default password	Where a system needs a username and/or password to log in, a default password is usually provided that allows the device to be accessed during its initial setup	13
Email Platforms	Microsoft 365 Suite and IBM Lotus notes	14
Social chatrooms	This refers to Yammer, Microsoft teams and/or Google Hang out	14
Instant messaging services	Skype for business on 365 and Sametime using Lotus	14
Social media and blogging solutions	Social Media Company accounts administrating the following sites Twitter, Facebook, Linkedin, Instagram, Pinterest	14
Video conferencing platforms	Refers to Skype for business, Peoplelink and Zoom	14
On line defamation	Otherwise known as Internet defamation, this refers to a false statement of fact that aims to harm somebody's reputation	14
Company designated email account	A users Company mail account (Refer to email platforms)	14
Clickbait titles	Striking subject titles	15
Monetary transfer	Known as the Electronic transfer of money from one bank account to another	15
Social media Content Specialist	Refers to as an administrator managing a Company's social media account	15
User Created Content	Images, videos, text and audio, that have been posted by users on social media platforms	15
Internet bandwidth	Internet bandwidth is about how much data can be downloaded or uploaded from your computer	16
Streaming audio/video sites	Streaming media refers to either a video or audio content sent over the Internet and played immediately	16
Network traffic	Refers to the amount of data moving across a network at a given point of time	16
Peer to peer File sharing	A files transfer process between two or more computers	16

Term	Description	Page
Internet telephony	A Voice over IP telephony system	16
Social networking applications	Examples include Tumbir, Google+, we Chat, Reddit	16
Spyware	Spyware is a software which monitors the actions that are carried out on a device	17
Ransomware	Ransomware is a type of malicious software that takes over an infected computer/network and prevents the user from accessing files until you pay a ransom	17
Computer worms	A worm is designed to spread itself from system to system	17
Adware	Designed to maliciously push adverts onto the user	17
Trojan Malware	A malicious software which often disguises itself as a legitimate tool that tricks the user into installing it so it can carry out its malicious tasks	17
Browser Hijacker	Redirects the browser to other, usually malicious, websites. A browser hijacker enables browser hijacking	17
File Infector	These viruses attach to host files, so this means they usually stick to files you use often. Any time you open or run the file, the virus is running	17
Macro Virus	It attaches itself to files made from programs that support macros	17
utorrent	A platform for downloading files using a distributed file sharing system. Downloaded files can include copyrighted material.	17
The Pirate bay	Download music, movies, games, pirated software and much more using this site	17
Warez	Unlike pirated software, warez are usually unauthorized releases of software	17
Network sniffing	Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty	19
Denial of service	Purposely interrupting a user's access to any network	19
Honey pots	To further improve computer security, traps are set to detect attempts at any unauthorized use of information systems	19
Honey net	Its purpose is to invite attack by setting up intentional weaknesses on any network	19
Port scanning	Determines what areas (ports) with the network are open	19
Wireless SSID	A Wi-Fi name	19
Company computing assets	Purchased and used exclusively for business use	23
Computer Equipment	Refers to Desktops, Laptops, Smart Phones Tablets	23
Freeware	Refers to software that anyone can download from the Internet and use free eg. Google Talk, yahoo messenger, MSN messenger	24
Shareware	Sharewares give users a chance to try the software before buying it. Eg. Winzip, Wondershare youtube downloader	21
Open Source	Open source is software with source code that anyone can inspect, modify, and enhance eg. Script writing software	21
Degaussing service	Part of the data destruction process, degaussing completely erases the data contents within the hard drive	23
Virtual private network (VPN)	VPN is a technology that creates a safe and encrypted connection over the Internet.	24
Internet Tethering or Mobile Hotspot	Sharing of a mobile device's Internet connection with other connected computers	25