Acceptable Use Policy

AUDIENCE: All employees and relevant parties (contractors, subcontractors, freelancers, applicable business partners and vendors).

Overview

This policy addresses the acceptable use of information technology systems of Tinopolis Group and companies ("The Company or Company"). This policy is in place to protect both you and The Company. Inappropriate use of information technology systems could expose both you and The Company to risks including, but not limited to, malicious code attacks, compromise of network systems and services, as well as legal/compliance issues.

This policy applies to any use of the information technology systems owned or leased by The Company, which includes The Company's telephony systems described below. This policy is a subordinate of the Information Security Policy. It is the responsibility of every employee who engages third party-agents, vendors, contractors or other business partners ("Third Parties") to perform services involving access to The Company systems to work with IT and Legal to ensure such Third Parties are contractually obligated to comply with this policy.

All Company systems are intended for business use. Personal use of Company systems may be permitted, provided that it does not interfere with the performance of your job duties and responsibilities, does not interfere with the performance of The Company systems such that it impacts the network ability/capability (e.g., slows down the network), does not fall within expressly excluded use in this policy and does not otherwise breach any other Company policy, procedure or standard.

For business reasons, and in order to carry out legal obligations as an employer, use of the Company's systems including the telephone, email and IT systems, and any personal use of them, may be monitored. This includes, without limitation, content files, internet, emails and voice mail usage. Such monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes, such as to ensure compliance with applicable laws, rules, regulations and Company policies, as well as to prevent, detect and/or investigate unauthorised use of any Company system. Any monitoring information gathered may be disclosed to appropriate Company management and, if required, to law enforcement agencies.

In general, you are responsible for:

- exercising good judgement regarding reasonableness of personal use of The Company systems. If there is any uncertainty, you either should consult your manager, Human Resources or Service Desk;
- the security of your user ID's and passwords. Passwords should never be shared, and must comply with all requirements regarding creation, format and updating of passwords as set forth in the Access Control Policy;
- taking care of all equipment provided by The Company. The Company reserves the right to reclaim any costs incurred it feels led to damage through negligence;
- taking special care to ensure that Company data on mobile devices is maintained in a secure manner because information on mobile devices is especially vulnerable. Please see the Mobile Device Use section below.

Internet Use

Employees and Third Parties are encouraged to use the Internet to further the goals and objectives of The Company. Access to the internet is provided for business use. Personal use of the Internet is permitted provided that it does not interfere with the performance of your job duties and responsibilities, does not fall within the expressly excluded uses below, or otherwise breaches any Company policy, standard, procedure or guideline:

The following activities are prohibited:

- Viewing or downloading any content that violates The Company's Anti-Harassment and Anti-Bullying policy or is inconsistent with what is expected as acceptable in a work place environment.
- Using Company systems to interfere with or disrupt third-party Internet users, services or equipment. For example, streaming videos/music for the purpose of disabling a third-party system.
- Engaging in activities designed to gain unauthorised access to, or to delete, alter or corrupt data in an unauthorised or illegal manner.
- Engaging in activities such as distributing 'spam,' spreading malicious software (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) or causing any other network disruption.
- Using The Company systems to attempt unauthorised access into any third-party network or computer accessible via the Internet.
- Downloading any software for non-work related purposes onto any Company-owned devices and systems. Further, to ensure the security and integrity of The Company systems, downloading of software for work-related purposes should be performed only with Manager and Head of IT approval.
- Engaging in any activities that violate legal protections provided by copyright, trademark, patent or other intellectual property rights.
- Exporting software, technical information, encryption software or technology in violation of International or regional export control laws. Legal and IT should be consulted prior to export of any materials that is questionable.
- Making fraudulent offers of products, items or services.
- Port or security scanning.
- Executing any form of network monitoring or surveillance that will intercept data not intended for the employee's device, unless this activity is a part of the employee's role and responsibilities.
- Circumventing user authentication or security of any device, account or network.
- Using any unapproved encryption software.
- Using any unapproved freeware or shareware.
- Using privileged credentials to access information on Company systems without a legitimate business reason.
- Accessing websites that circumvent Internet controls to access sites that are explicitly blocked. Examples include illegal activity, sexually explicit, intolerance and hate or anything that violates any company policy.
- Engaging in any other form of illegal activity or activity that otherwise violates any Company policy, standard or guideline.

The above list is by no means all-inclusive, but instead attempts to provide a framework to guide users in the proper understanding of those activities that fall into the category of acceptable use and those that do not. As stated, each employee and Third Party is expected to use good judgement when it comes to other types of usage. If you are unsure, you should check with your manager or the Service Desk.

E-mail Use

E-mail is an essential for business communication and must be used in accordance with this policy. The following guidelines should be followed when using The Company's e-mail system:

- E-mail accounts are only to be used by the registered user, except when a specific delegation of access has been granted by your manager.
- Consider whether using email is the best medium for the message you need to deliver. E-mails should be concise and should be sent on a need-to-know basis. General messages to a distribution group should only be used where necessary.
- If you receive an e-mail message containing offensive or inappropriate material, immediately notify Human Resources.
- Do not open e-mails from unknown sources, as they could be spam or phishing messages that may present a security risk to Company systems.
- Remember that an e-mail sent from a Company e-mail account reflects on The Company.

The following e-mail activities are prohibited:

- Creating or forwarding "chain letters".
- Sending emails containing any Company intellectual property to personal e-mail accounts or forwarding Company e-mails to personal e-mail accounts. If you need to work remotely and do not have a Company laptop, you can log onto webmail or use Virtual Desktop Infrastructure (VDI).
- Downloading any Restricted material (as defined by the Data Security Standard) on a personal device is expressly prohibited.
- Storing, sending or forwarding spam.
- Creating or sending unsolicited marketing communications to customers without first obtaining their prior written consent to receive unsolicited marketing material.
- Creating or sending unsolicited marketing communications to customers who are registered with the direct marketing association's mailing preference service.
- Opening e-mail attachments from unknown sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password.
- Spreading malicious software (e.g., viruses, worms, Trojan horses) or causing any network disruption (e.g., denial of service).
- Engaging in illegal activity or any activity that otherwise violates any Company policy, standard or guideline.

The list above is by no means all-inclusive, but instead attempts to provide a framework to guide users in the proper understanding of those activities that fall into the category of acceptable use and those that do not. As stated, each employee is expected to use good judgment when it comes to other types of usage. If you are unsure, you should check with your manager or the Service Desk.

Telephony Use

Telephone communication is essential to the day-to-day operations of The Company. Telephone and voicemail services are provided to employees and Third Parties in order to facilitate communication.

As with all Company resources, use of voice communication devices should be as cost-effective as possible and in keeping with the best interests of The Company. The Company reserves the right, if deemed necessary and appropriate, to request full repayment of any personal calls or data charges made from Company telephony systems.

Desk phones, telephony equipment (e.g., fax machines, modems, mobile devices or any other equipment that communicates via phone), voice mailboxes and messages contained within voice mailboxes are the property of The Company.

- You should take precautions to ensure that telephone conversations cannot be overheard when discussing sensitive information. This includes the use of mobile phones, speakerphones and public phones.
- Avoid sharing sensitive information via voice mail, whether internal or external telephony systems.

The Company telephony services may not be used for the following:

- Transmitting obscene, profane or offensive messages.
- Attempting to access another employee's voice mailbox unless specifically authorized.

The list above is by no means all-inclusive, but instead attempts to provide a framework to guide users in the proper understanding of those activities that fall into the category of acceptable use and those that do not. As stated, each employee is expected to use good judgment when it comes to other types of usage. If you are unsure, you should check with your manager or the Service Desk.

Printer Use

Printers are intended to be used for printing Company documents; a minimal amount of personal use of Company printers may be permitted. Avoid printing large files or large print jobs, as this can impact network resources and interfere with the ability of others to use the same printer. If you encounter a physical problem with the printer (e.g., paper jam, out of toner, etc.) are unable to resolve it on your own, please contact and report the problem to the Office Runners.

Because printers contain hard drives that retain data, printing Restricted material (as defined by the Data Security Standard) should be limited to instances where there is a business necessity to do so.

Removable Media Use

Removable media (e.g., thumb drives, USB/firewire storage devices, DVDs, CDs, tapes) used to process and store Company information must be physically controlled and secured from unauthorised access. Except in the case of Company-approved necessary back-up data, removable media should not be utilised to process, store or transfer Restricted material (as defined by the Data Security Standard). If you have Company information on removable media, it is your responsibility to ensure information is encrypted and password-protected. Examples of acceptable use of removable media include, but are not limited to:

- Backups sent to off-site backup facilities.
- Production content sent/received.
- Inter-company transfer of large files not appropriate for email.

To secure Company information, you are required to enable power-on or password security and encryption features on all removable media. All passwords must comply with the password configuration requirement of the Access Control Policy. Encryption should comply with the Data Security Standard.

If removable media has been lost or stolen, report it immediately to your manager and the Service Desk.

Mobile Device Use

The increased business use of mobile devices (e.g., laptops, smartphones, tablets, etc.) is creating greater risk to The Company. Therefore, any business use of mobile devices is entirely subject to this Acceptable Use Policy, any and all information security and other applicable policies. This requirement applies to, but is not limited to, all devices that fit the following device classifications (whether owned by The Company or individuals subject to this policy):

- Laptops
- Smartphones, tablets or other devices capable of receiving direct push technology providing real-time delivery of e-mail, calendar, contacts and tasks; or cloud-based applications; or
- Handhelds running the Palm OS, Microsoft Windows CE, Pocket PC or Windows Mobile, Symbian, Mobile Linux, Apple iOS, Android OS, Blackberry OS, Google OS etc.; or
- Devices that are stand alone or wearable, whether connectible using wired sync cables and/or integrated wireless (which may include but not limited to: Wi-Fi, Bluetooth and infrared).

In addition:

- If you are authorised to use Company-owned or personally-owned mobile devices that have access to The Company network, you will be subject to and expected to comply with the terms and conditions of all policies, including those addressing data security and computer access and use.
- Every safeguard practicable should be used to protect data in accordance with the Information Security Policy including encryption, password/pin protection and multi-factor authentication, where available.
- Mobile devices used for Company business purposes must be locked any time the device is unattended.
- Mobile devices used to access or store Company information must not be left unattended in any unsecure location.
- Mobile devices that are personally owned should not be set up to sync Company data other than e-mail (e.g., do not sync Company files/folders etc.).
- Mobile devices should not be used to access or store Restricted material (as defined by the Data Security Standard).

The following activities are deemed inappropriate uses of portable/mobile devices and are strictly prohibited:

- Using mobile devices to scan The Company networks.
- Using mobile devices to install malicious software.

The list above is by no means all-inclusive, but instead attempts to provide a framework to guide users in the proper understanding of those activities that fall into the category of acceptable use and those that do not. As stated, each employee is expected to use good judgment when it comes to other types of usage. If you are unsure, you should check with your manager or the Service Desk.

Monitoring

The Company may monitor use of Company Systems for various reasons, including, but not limited to:

- Ensuring employees and Third Parties are using the systems in accordance with acceptable use and information security policy.
- Preventing, investigating and/or detecting unauthorised use of The Company's systems.
- Ensuring compliance with all applicable laws, policies, rules and/or regulations.

Monitoring may include (but is not necessarily limited to) intercepting and reviewing network traffic, e-mails or other message or data sent or received through The Company systems, and inspecting data stored on individual file directories, hard drives or printed or electronic media.

Information relating to employee and Third Party use of The Company's systems may be disclosed to individuals in The Company, IT, Human Resources, Legal, Senior Management, and, if required, to law enforcement officials. The Company may also store copies of such data and communications for a period of time after created and may delete such copies from time to time without notice.

Disciplinary Procedure

Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.