Information Technology System Acceptable Use Policy and Responsibilities Agreement

Introduction

This policy governs your use of the Company's IT System, which includes all technological and automated data processing equipment used at the Company's facility, accessed remotely, or carried with you for use at home or while travelling.

Violations of this policy may result in disciplinary action, and/or civil and criminal liability.

For clarification on this policy's provisions, to report violations, or to receive authorizations for exceptions to this policy, contact your work supervisor, or consult additional policy documents or relevant orientation or training materials, to determine the appropriate individuals to contact.

Allowable Use of Company-Owned IT System Resources

You may only use Company-owned technology equipment, software, and data for the purpose of conducting the business of the Company. However, personal (non-business-related) use may be allowed as determined by your work supervisor, and subject to all other restrictions in this policy. Where personal use is allowed, in all cases, you may not spend excessive amounts of time on personal activities, or consume excessive amounts of system resources (such as network bandwidth), or in any case adversely affect the function of the IT System. You may not store personal files (such as documents, e-mail, photos or videos) on Company equipment.

Your Responsibilities

For any resources for which you may select your own password (such as logon accounts, e-mail boxes, or online accounts established on behalf of the Company), do not use easily guessable or common passwords. Do not write your passwords down and leave them exposed (such as, for example, on a sticky note attached to the side of your computer).

For any resource that requires a password to access, protect against unauthorized use by logging off, closing the software, and/or locking the device when not in use.

Do not share your passwords or network access with anyone, even trusted fellow employees. If you believe someone needs access to any resources only you have, that user must place a request through authorized channels to gain that access.

Do not provide information about the IT System to anyone. If you receive any queries by visitors or callers about the IT System capabilities, or about your logon accounts or passwords, direct them to your supervisor or IT System manager.

Follow all other security procedures required or recommended by your work supervisor, IT System manager, or authorized delegates.

Immediately report any suspected network intrusion, unexplained degradation or interruption of IT System services, improper use of the IT System by others, unauthorized access to data by others, or any apparent attempts to collect information about the IT System by unauthorized individuals.

Manage your stored data in line with Company information systems policies. This means storing data in appropriate locations according to any classifications assigned, deleting or retaining data according to data retention policies, and preventing unnecessary duplication of data.

Do not remove any Company-owned equipment, software, or physical storage media from Company premises without authorization. While in possession of any Company-owned equipment you take offsite, ensure the physical security of the equipment. Do not leave equipment unattended, even for a moment, in a public place. Remember that it takes just seconds for a thief to steal a laptop computer.

If you access Company IT System resources using personal equipment (such as connecting to the Company network via VPN from your home computer), you must ensure your equipment complies with Company security standards. You may not disable, remove, or circumvent any technical measures in place to enforce these standards. You must also protect your personal equipment, which may have saved passwords and links to protected Company resources, from theft or unauthorized access the same as you must for Company-owned equipment. When no longer needed for Company use, you must remove all Company software, saved data, and saved links and passwords from your personal equipment.

Internet Usage

This portion of the policy covers all aspects of external network communication, including, but not limited to, web searching/browsing, e-mail, file transfer, file sharing, chat, VPN connections, and multimedia (such as online radio stations or video broadcasts), whether using Company-owned equipment or your own personal equipment that connects to the Company IT System or stores Company data.

You must exercise good judgment while accessing the Internet. If a website appears shady, such as offering unbelievable bargains, expressing dire warnings, or unexpectedly attempting to install software on or otherwise control your computer, close the website and report it to your work supervisor or IT System manager.

You may not search for or connect to any web site or service on the Internet that purports to offer illegal or illegitimate services, such as pirated software downloads, cracked software license codes, pirated music or movie downloads, espionage tools, etc.

Do not open any e-mail attachment, click the option to download any file from a website, install any add-ons or updates offered by your software, etc., unless you know exactly what it is, and are expecting it. If in doubt, contact your IT System manager or technical support.

You may not download from or post to any Internet site anything that is abusive, harassing, vulgar, obscene, or indecent, except as expressly approved and required as part of the Company's business. You may not download from or post to any Internet site anything which is defamatory, libelous or otherwise unlawful, or which violates the Company's relevant standards of conduct, sexual harassment policy, or equal opportunity policy, in any case.

You may not download from or post to any Internet site any material where such transfer is prohibited by law or contractual or fiduciary relationship (such as copyrighted material, inside information, proprietary or confidential information, anything that infringes on a patent or trademark, etc.).

When communicating via the Internet in any manner, you may not impersonate any person or entity, or falsely state or otherwise misrepresent your affiliation with a person or entity.

You may not use Company equipment or Internet connections to send or convey in any way advertising or marketing or promotional materials not related to Company business, chain letters, or anything that could be perceived as such.

You may not transmit or assist in transmitting any Company data that is not permitted for disclosure under the Company's data classification system, which typically includes employee data, Company trade secrets, research data, and customer lists.

You may not use Company equipment to try to gain unauthorized access to any other computer system or remote network.

The Company may employ technological measures to prevent access to certain prohibited content. However, any failure of such measures to block prohibited material does not change the policy or absolve you of your responsibilities under this policy. If you do access prohibited material despite these measures, accidentally or otherwise, you must close the window immediately, delete any material downloaded, and report the incident to your work supervisor. By using Company's IT System for Internet access, you acknowledge that the Company has no control over the content of Internet websites, inbound e-mails, and other such services. Where your work duties require you to access the Internet and/or use e-mail, you acknowledge that you may be exposed to material that is offensive and possibly even patently obscene, and you will not deem Company liable for any wrongdoing in this regard.

Additional Prohibited Actions

You may not copy any Company data onto any personally-owned removable media or other device, except as expressly authorized. You may only copy Company data onto Company-owned removable media or devices as part of your work duties, and only where such media or devices are properly secured and accounted for by the Company.

You may not download or install any software onto Company equipment without authorization.

You may not reconfigure system settings on any equipment, apart from ordinary user options for day-to-day functionality, without authorization.

You may not perform any actions that may be perceived as hostile towards the IT System and its security configuration, such as (but not limited to) attempts to reduce functionality, interfere with access, deny service to other users, circumvent any security system, conduct port scanning or traffic sniffing, elevate your privileges, access or alter data for which you are not authorized, cause data corruption, or otherwise use or exploit the system or the information it contains in a manner other than the clearly obvious and/or stated purpose of any given resource.

You may not touch equipment not assigned for your use without proper authorization.

You may not move or disassemble equipment. If you have a need to relocate equipment, contact your work supervisor or technical support.

You may not physically install, connect, or attach to the IT System any wireless access points, network switches, thumb drives, disks, computers, IP phones, mobile phones, or any other device, without explicit authorization, and only in the manner directed.

You may not connect your personal network devices (such as a laptop or handheld device) to the IT System's wireless network unless you receive explicit authorization for each device connected (even if you already know the password), and only if you connect in the manner directed.

You may not employ any methods of encryption except with authorized tools and encryption keys provided by the Company.

Privacy

You acknowledge that, except as prohibited by law, all equipment belonging to the Company is subject to monitoring by the Company, without prior notice, which includes storing a record of all your activity, including personal information you may choose to input, and personal communications you send or receive, even if encrypted. You also acknowledge that the Company may use this information in any lawful manner it sees fit.

For Privileged Users

This section applies if you are granted privileged access to any aspect of the IT System.

You may only use administrative accounts, privileges, and permissions for authorized administrative tasks related to the business of the Company. For any administrative tasks you perform that may alter the configuration of a managed device (such as installation of software or reconfiguration of equipment), or which may affect other managed devices, you must coordinate these tasks with the appropriate systems manager to ensure continuity of operations and appropriate update of documentation.

You may not use your administrative account or access for any day-to-day use, such as routine business and personal operations, Internet browsing, or e-mail. You may not create administrative accounts for others, or provide any elevated access for others, without proper authorization.

I have read, understand, and will comply with this policy.

_____

Employee Signature

_____

Employee Printed Name

_____

Date