Computer, E-mail, and Internet Usage Policy

1. Introduction

This Computer, E-mail, and Internet Usage Policy outlines the guidelines and acceptable use of computer systems, e-mail services, and internet access. The purpose of this policy is to ensure the appropriate, ethical, and legal use of these resources by all employees.

2. Scope

This policy applies to all employees, contractors, and temporary staff who have access to company's computer systems, e-mail services, and internet access.

3. General Guidelines

a) All employees are responsible for using the company's computer systems, e-mail services, and internet access in a professional, lawful, and ethical manner.

b) b. Company-owned computer systems, e-mail accounts, and internet access are provided for business purposes only. Limited personal use is permitted, as long as it does not interfere with job performance or violate any other company policies.

c) c. Employees should not expect privacy when using company-owned computer systems, e-mail services, and internet access, as all data and communications may be monitored by the company to ensure compliance with this policy.

4. Computer Systems

a) Employees are responsible for safeguarding their login credentials and must not share them with anyone else.

b) Installation of unauthorized software on company computers is strictly prohibited.

c) Employees should not modify or remove any hardware or software configurations without prior authorization from the IT department.

d) Employees must lock their computer screens when they are away from their workstations, even for a short period. This can be done by pressing the Windows key + L on a Windows computer or Control + Command + Q on a Mac computer.

e) Employees should shut down or restart their computers at the end of the workday or when instructed by the IT department, as this helps to apply security updates, clear temporary files, and improve overall system performance.

f) In case of a prolonged absence from the office (e.g., vacations, business trips, or sick leave), employees should completely shut down their computers to conserve energy and reduce the risk of unauthorized access.

5. E-mail Usage

a) Employees must use their company-provided e-mail account for all work-related communications.

b) All e-mail communications must be professional and adhere company's Code of Conduct.

c) The use of e-mail for harassment, discrimination, or any other inappropriate behavior is strictly prohibited.

d) E-mail should not be used to send confidential or sensitive information without proper authorization and security measures, such as encryption.

6. Internet Usage

a) Employees must not access, download, or distribute any material that is offensive, pornographic, discriminatory, or otherwise inappropriate.

b) Employees must not engage in any activities that could harm the company's reputation or violate any laws or regulations.

c) Employees must not use company resources to engage in any form of online gambling, participate in illegal activities, or visit websites that promote such activities.

d) Employees must not download or install any unauthorized software, applications, or browser extensions from the internet.

7. Messaging System Usage Policy

a) Company provides a messaging system (such as Microsoft Teams, Whatsapp, or any other approved platform) for employees to communicate and collaborate with colleagues for work-related purposes.

b) All employees are required to use their company-provided accounts for messaging and should not use personal accounts for work-related communications.

c) Messages sent through the company's messaging system should be professional, respectful, and in compliance with company's Code of Conduct.

d) The messaging system must not be used to send or share offensive, discriminatory, harassing, or inappropriate content. Any such behavior will be subject to disciplinary action, up to and including termination of employment.

e) Confidential or sensitive information should not be shared through the messaging system without proper authorization and security measures.

f) Employees should follow proper etiquette and be mindful of their tone and language when using the messaging system. This includes avoiding excessive use of capital letters (which can be perceived as shouting), excessive

abbreviations, and informal language that may be inappropriate in a professional setting.

g) Employees are expected to respond to messages in a timely manner during working hours. However, they should not feel obligated to respond immediately to non-urgent messages, especially during non-working hours or when it may interfere with their work tasks.

h) Employees should use appropriate channels, groups, or direct messages for their communication to ensure that the right people receive the information and to avoid unnecessary distractions or clutter for other team members.

i) The company reserves the right to monitor and review messages sent through the messaging system to ensure compliance with this policy and other applicable regulations.

j) Employees should report any misuse of the messaging system, including harassment, discrimination, or any other inappropriate behavior, to their supervisor or the HR department.

8. Security

a) Employees must report any suspected security breaches, malware infections, or other incidents to the IT department immediately.

b) Employees must not attempt to bypass or disable any security measures, such as firewalls, antivirus software, or content filters.

c) Employees must not use any unauthorized remote access tools or services to access the company network or computer systems.

9. Password Protection and Security

a) Employees are responsible for creating strong, unique passwords for their company accounts and ensuring the confidentiality of their login credentials.

b) To create a strong password, employees should:

i. Use a combination of uppercase and lowercase letters, numbers, and special characters.

ii. Make the password at least 12 characters long.

iii. Avoid using easily guessable information, such as birthdates, names of family members, or common dictionary words.

c) Employees should change their passwords periodically, at least every 90 days, or immediately if they suspect that their password has been compromised.

d) Passwords must not be shared with any other individuals, including colleagues, friends, or family members.

e) Employees should avoid using the same password across multiple accounts or services, both within the company and for personal use.

f) Employees should not store their passwords in an easily accessible location, such as on a sticky note attached to their computer or in an unencrypted file on their devices.

g) Employees are encouraged to use a password manager, approved by the IT department, to securely store and manage their passwords.

h) If an employee forgets their password or suspects that their account has been compromised, they should immediately contact the IT department for assistance in resetting their password and securing their account.

10. Personal Device Policy

a) Company recognizes that employees may use their personal devices, such as smartphones and tablets, for work-related purposes. This policy outlines the guidelines and requirements for using personal devices in the workplace.

b) Employees are responsible for ensuring that their personal devices are secure, up-to-date with the latest software updates, and protected by a password or biometric authentication.

c) When using personal devices for work-related purposes, employees must follow the same guidelines and policies that apply to company-owned devices, including the Computer, E-mail, and Internet Usage Policy and the Messaging System Usage Policy.

d) Employees should not store sensitive or confidential company information on their personal devices without proper authorization and security measures, such as encryption and secure storage apps approved by the IT department.

e) If an employee's personal device is lost, stolen, or compromised, they must immediately report the incident to the IT department, who will take appropriate measures to protect company data and resources.

f) Employees must not use their personal devices to take pictures, record videos, or capture any other confidential information within the workplace without prior authorization from a supervisor or manager.

g) The company reserves the right to monitor and review any work-related communications or data stored on personal devices when there is a legitimate business need or legal obligation to do so.

h) Use of personal device during work hours should not interfere with an employee's job performance or productivity. Employees should use discretion and limit personal activities on their devices during work hours, such as personal calls, texting, or browsing social media.

i) Company is not responsible for any costs associated with the use of personal devices for work-related purposes, such as data usage, voice calls, or device repair and maintenance, unless a specific agreement or reimbursement policy is in place.

11. Wi-Fi Usage Policy

a) Company provides a Wi-Fi network for employees to access the internet and company resources using their company-owned devices, personal mobile devices, and other approved devices.

b) Employees must follow the same guidelines and policies that apply to the use of company-owned computer systems, e-mail services, and internet access while connected to the company's Wi-Fi network.

c) Employees must not share the Wi-Fi password with unauthorized individuals, such as visitors, clients, or contractors, without prior approval from the IT department or a supervisor.

d) The company's Wi-Fi network is for business purposes only. Limited personal use is permitted, as long as it does not interfere with job performance, violate any other company policies, or consume excessive bandwidth.

e) Employees must not use the company's Wi-Fi network to access, download, or distribute any material that is offensive, pornographic, discriminatory, or otherwise inappropriate.

f) Employees must not engage in any activities that could harm the company's reputation, violate any laws or regulations, or compromise the security of the Wi-Fi network while connected to it.

g) The IT department may implement security measures, such as firewalls, content filters, and bandwidth

restrictions, to protect the company's Wi-Fi network and ensure compliance with this policy.

h) Employees should report any suspected security breaches, unauthorized access, or other issues related to the Wi-Fi network to the IT department immediately.

i) The company reserves the right to monitor and review network usage and data traffic to ensure compliance with this policy and maintain the security and performance of the Wi-Fi network.

12. Policy Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. The company also reserves the right to report any illegal activities to the appropriate authorities.

13. Acknowledgment

By using company's computer systems, e-mail services, and internet access, employees acknowledge that they have read, understood, and agree to comply with this Computer, E-mail, and Internet Usage Policy.