Aptos IT Acceptable Use Policy

4/10/2017

Table of Contents

About this Policy 2
System Access Control 2
Internet and Email usage 3
Laptop Usage and Security 5
Printer Usage 6
Telephony system usage 6
Monitoring and logging 6
Employee Agreement 7

About this Policy

This Aptos IT Acceptable Use Policy (this "Policy") is designed to protect Aptos, our colleagues, customers and other partners from harm caused by the misuse of IT systems and data.

The result of misuse can result in potential damage including, but not limited to, malware infection or viruses, legal and financial penalties for data leakage, and lost productivity resulting from system downtime.

Aptos colleagues and contractors are responsible for the security of our IT systems and the data on them. Should any colleague or contractor have questions about this Policy or require clarifications they should speak to the Aptos IT department or their manager.

System Access Control

Access to Aptos IT systems is controlled by the use of individual user IDs and passwords. All user IDs and passwords are to be uniquely assigned to each colleague or contractor for their use. Colleagues and contractors are accountable for all actions on Aptos IT systems using those assigned credentials. The following actions would be considered in violation of this Policy:

- Allowing anyone else to use the assigned ID and password on any Aptos IT system.
- Leaving an assigned user account logged in at an unattended and unlocked computer system.
- Using someone else's user ID and password to access Aptos IT systems.

- Leaving the ID and password unprotected (such as writing it down and having it viewable).
- Performing any unauthorized change to Aptos IT systems or information.
- Attempting to access unauthorized data.
- Providing or transferring Aptos data or software to any person or organization outside of Aptos without the authority of Aptos.

Internet and Email usage

The Internet allows Aptos colleagues and contractors to connect to information resources around the world. Every colleague and contractor has a responsibility to maintain and enhance the company's public image and to use the Internet in a productive manner. To ensure that all colleagues and contractors are responsible, productive Internet users and are protecting the company's public image, Aptos has established the following guidelines for using the Internet:

- Colleagues and contractors accessing the Internet are representing the company. Colleagues and contactors are responsible for seeing that the Internet is used in an effective, ethical, and lawful manner.
- Internet Chat channels may be used to conduct official company business or to gain technical or analytical advice. Databases may be accessed for information as needed.
- Use of the Internet must not disrupt the operation of the company network or the networks of other users.
- Use of the Internet must not interfere with productivity. Any Internet access may be restricted at management's discretion.
- Each colleague or contractor is responsible for the content of all text, audio, or images that they place or send over the Internet. Fraudulent, inappropriate, harassing, or obscene messages are prohibited. All messages communicated on the Internet should have the Aptos resource’s name attached. No messages will be transmitted under an assumed name. Users may not attempt to obscure the origin of any message.
- Information published on the Internet should not violate or infringe upon the rights of others. No abusive, profane, or offensive language or pornographic pictures (etc.) are to be transmitted through the system. Colleagues or contractors who receive obscene or inappropriate messages are obligated to report the message immediately to their manager and the People Team.

- Copyrighted materials belonging to entities other than this company may not be transmitted by colleagues or contractors on the Internet. Users are not permitted to copy, transfer, rename, add, or delete information or programs belonging to other users unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action from the company or legal action by the copyright owner.
- The company reserves the right to access and monitor all messages and files on its systems, including information regarding colleague or contactor Internet use, as deemed necessary and appropriate. Internet messages are public communication and are not private. All communications including text and images can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.
- Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race, religion, national origin, physical attributes, or sexual preference are to be transmitted.

Use of Aptos internet and Email is intended for business use. Personal use is permitted where such use does not affect the network performance, is not detrimental to Aptos in any way, and is not considered in breach of any laws. The following actions would be considered in violation of this Policy:

- Using another person's files, systems, software, or data without permission.
- Using computer programs to decode passwords or access control information.
- Attempting to circumvent or subvert system security measures.
- Knowingly engage in any activity that causes harm to systems or any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- Make or use illegal copies of copyrighted software, or store or transmit such copies on company systems.
- Using the Internet in a manner not authorized by the company to gain commercial or personal profit or advantage.
- Downloading any Public Domain, Freeware, or Shareware programs to company equipment without the prior approval of Aptos IT.
- Installing, executing, or opening any downloads before performing a virus check of that software or file.
- Connecting to any website that contains objectionable, obscene, or illegal materials.
- Uploading or downloading of any unlicensed or illegal issued software or content.
- Posting any objectionable or inappropriate remarks or contents on websites or social media.

- Intentionally connecting to any website that could contain malware or virus that could negatively affect Aptos network or systems.
- Using torrent software of any kind to share or download media or content.
- Posting, disclosing or sending any confidential company or customer materials to the public internet or non-Aptos recipients.
- Performing any type of hacking into unauthorized networks.
- Using the internet or email for any illegal activities such as gambling.
- Distributing messages or images that might be considered offensive, discriminatory, or harassing.
- Sending any unsolicited personal views on religious, political, or social related matters.

Laptop Usage and Security

Colleagues and some Aptos contractors will be provided an Aptos issued laptop or desktop PC device. This device is to be used for Aptos business related work and should be kept safe and secure at all times. The following controls must be applied:

- Aptos anti-virus software and security software must be running and not disabled or removed.
- Aptos laptop devices should not be shared or used by anyone besides the person that is assigned to that laptop.
- Laptop security settings should not be altered without the approval of Aptos IT.
- Laptops should not be left unattended when in public locations, such as airports or coffee shops.
- Laptops should be logged off / locked or protected with a screen locking mechanism controlled by password when unattended.
- Laptops must not contain any illegally licensed or unauthorized software that violates any software supplier's license agreement.
- Aptos is not responsible for any personal files such as music, photos, or videos stored on Aptos laptop devices.
- Lost or stolen laptop devices should be reported to Aptos IT within 24 hours. Where applicable a police report should be filed and shared with Aptos IT.

Printer Usage

Some Aptos offices are outfitted with printer devices intended for the printing of business related materials when necessary. The following usage controls should be followed:

- Take care to not leave confidential materials unattended on printers or copiers.
- All business-related print outs must be securely stored or destroyed using shredders or alternate methods to ensure material cannot be read by anyone not authorized.
- Printing of personal items such as invitations, mailing labels, or other non-business related materials is not allowed on Aptos printer devices.

Telephony system usage

Use of Aptos voice system is intended for business use. Use of Aptos voice systems for personal communications should be limited and only used when necessary. When available, personal communications should be made using personal or alternate means of communications. The following would be in violation of this Policy:

- Except as otherwise provided above, using Aptos telephony system for personal communications or other non-Aptos business.
- Making threatening, hoax, or prank calls to internal or external destinations.
- Calling any toll charging numbers with Aptos telephony systems.

Monitoring and logging

All data that is created and stored on Aptos computers and systems is the property of Aptos. IT system logging and monitoring will take place where is it decided to be appropriate, and investigations will take place where reasonable suspicion exists of a breach of this Policy. Aptos has the right, under certain conditions, to monitor activity on its systems including internet and email use, in order to ensure system security and effective operation, and to protect against any misuse.

Employee Agreement

The company considers any violation of this Policy to be improper conduct and reserves the right to copy and/or examine any files or information residing on the network. Violators are subject to disciplinary action up to and including termination.

I have read and understand this Policy and agree to abide by all the terms and conditions, including using the Internet for business purposes only. I also understand that I can make no assumptions about privacy regarding my Internet usage on Aptos' network.

Employee Name: Raghul Muthu AC

Signature: Raghul Muthu AC
Raghul Muthu AC (Jan 19, 2022 22:00 GMT+5.5)

Date: Jan 19, 2022