Sacramento Transportation Authority

801 12th Street, 5th Floor
Sacramento, CA 95814
(916) 323-0080 Phone
(916) 323-0850 Fax
Email: info@sacta.org
Web: SacTA.org

Information Technology Policy

1. Introduction

This Acceptable Use Policy (AUP) for IT Systems is designed to protect Sacramento Transportation Authority (STA), its employees, and partners from harm caused by the misuse of its IT systems and data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of its systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works at STA is responsible for the security of its IT systems and the data on them. As such, all employees must ensure they always adhere to the guidelines in this policy. Should any employee be unclear on the policy or how it impacts their role they should speak to the Executive Director or IT security officer.

2. Definitions

“Users” are everyone who has access to any of STA’s IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers and business partners.

“Systems” means all IT equipment that connects to the agency network or access agency applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

3. Scope

This is a universal policy that applies to all Users and all Systems. This policy covers only internal use of STA’s systems and does not cover use of its products or services by third parties.

Some aspects of this policy affect areas governed by local legislation (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction.

Staff members at STA who monitor and enforce compliance with this policy are responsible for ensuring that they always remain compliant with relevant local legislation.

4. Use of IT Systems

All data stored on STA’s systems is the property of STA. Users should be aware that the agency cannot guarantee the confidentiality of information stored on any STA system except where required to do so by local laws.

801 12th Street, 5th Floor
Sacramento, CA 95814
(916) 323-0080 Phone
(916) 323-0850 Fax
Email: info@sacta.org
Web: SacTA.org

STA's systems exist to support and enable the business of the agency. A small amount of personal use is, in most cases, allowed. However, it must not be in any way detrimental to users' own or their colleagues' productivity, nor should it result in any direct costs being borne by STA other than for trivial amounts (e.g., an occasional short telephone call).
STA trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the agency's IT systems. If employees are uncertain, they should consult the Executive Director or IT security officer.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorized access is prevented (or at least made extremely difficult). However, this must be done in a way that does not prevent–or risk preventing–legitimate access by all properly-authorized parties.

STA can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.

STA reserves the right to regularly audit networks and systems to ensure compliance with this policy.

5. Data Security

If data on STA's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-STA system any information that is designated as confidential, or that they should reasonably regard as being confidential to STA, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with STA's safe password policy (attachment A). Passwords will be kept in a secure place for reference by a designated employee in case a User is unavailable and/or becomes incapacitated.

Users who are supplied with computer equipment by STA are responsible for the safety and care of that equipment, and the security of software and data stored on it and on other STA systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

801 12th Street, 5th Floor
Sacramento, CA 95814
(916) 323-0080 Phone
(916) 323-0850 Fax
Email: info@sacta.org
Web: SacTA.org

Users who have been charged with the management of those systems are responsible for ensuring that they are always properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into STA's systems by whatever means and must report any actual or suspected malware infection immediately.
With hacking and exploitation on the rise, it is extremely crucial to keep the IT infrastructure protected as much as possible against any potential attacks. These attacks can be very detrimental and although we have several layers and/or platforms implemented as part of our IT security posture at STA, no amount of protection is sufficient without your awareness and/or collaboration.

With that said, here are a few very critical security tips to keep in mind as you work and navigate your technology throughout the day:

1) Always be extra careful when using technology and AVOID clicking any suspicious links, downloading files, providing information, visiting certain sites, granting access, etc. Hackers keep getting more and more sophisticated and their hacks keep getting more and more detrimental so be smart and NEVER panic especially when asked to click something or enter information because "your account got compromised." Sometimes you may have to just call the person communicating with you. If there is ANY suspicion, do NOT take action and/or click.

2) Never leave your computer unlocked when walking away. Unless you are working on your computer, always make sure that its locked. Even if you are in a "safe" place such as work or home, always get into the habit of locking your computer regardless of how long you are leaving it.

3) Create complex passwords. Always make sure you are creating complex and long passwords or passphrases for that matter because those are harder to crack. Moreover, never share your passwords or leave them in an unsafe place.

    a. Length: Longer passwords are generally more secure. Aim for a minimum of 8 characters, but longer is better.
    b. Character Variety: Include a mix of character types such as uppercase letters, lowercase letters, numbers, and special characters (e.g. !, @, #, $).
    c. Avoid Common Patterns: Avoid easily guessable patterns like "123456" or "password" or words that can be find in an English dictionary.
    d. Avoid Personal Information: Don't use easily accessible personal information such as your name, birthdate, or common words associated with you.
    e. Unique Passwords: Use a unique password for each account or service to prevent a breach in one account from compromising others.
    f. Passphrase: Consider using a passphrase, which is a longer sequence of words or a sentence. Passphrases are easier to remember and can be more secure than complex passwords.

4) Use Multi-Factor Authentication (MFA). We highly recommend for you to use MFA whenever possible. What this does is it adds an extra layer of security/authentication by requiring you to enter a one-time code that they text to your phone or by using one of the authenticator apps so that if someone gets a hold of your password, they will need another authentication method to get access.

801 12th Street, 5th Floor
Sacramento, CA 95814
(916) 323-0080 Phone
(916) 323-0850 Fax
Email: info@sacta.org
Web: SacTA.org

5) Avoid using company equipment for personal use as much as possible. Try to keep them separate. Social media is a big topic when it comes to this. Please try to keep that away from company issues equipment/devices.

6) Try to stay away from public WiFi connections especially on your work devices as those networks are usually insecure.

7) If you ever need to access your local office network from outside, contact Evercrest Technologies who can provide Virtual Private Network (VPN) access, which is a secure and encrypted connection to the internal office network.

8) The VPN will allow access to QuickBooks files and server folders at the office.

9) The VPN should not be used on personal computers to access the local work network. Employees should only use company issued equipment and computers.

6. Unacceptable Use

All employees should use their own judgment regarding what is unacceptable use of STA's systems. The activities below are provided as examples of unacceptable use; however, it is not exhaustive. Should an employee need to contravene these guidelines in order to perform his/her role, he/she should consult with and obtain approval from the Executive Director or IT security officer before proceeding.

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.

- All activities detrimental to the success of STA. These include sharing sensitive information outside the agency, such as research and development information and customer lists, as well as defamation of the agency.

- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business.

- All activities that are inappropriate for STA to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.

- Circumventing the IT security systems and protocols which STA has put in place.

7. Enforcement

STA will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include termination of employment.

801 12th Street, 5th Floor
Sacramento, CA 95814
(916) 323-0080 Phone
(916) 323-0850 Fax
Email: info@sacta.org
Web: SacTA.org

Use of any of STA's resources for any illegal activity will usually be grounds for summary dismissal, and STA will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

_____
Employee Name

_____ _____
Employee Signature Date