MCAA ELI Technology Policy

Sponsored By the Mechanical Contractors Association of America

Editor: Aaron Hall

Revision 3, February 2019

MCAA ELI Technology Policy

February 2019

Using this policy

One of the challenges facing associations today is enabling employees to work productively while also ensuring the security of the IT network and, crucially, the data on it. Given that technology is continually changing, employees play a significant role in IT security. This policy provides a framework for users to follow when accessing IT systems and the data on them. It is intended to act as a guideline for organizations looking to implement or update their own Technology Policy.

Feel free to adapt this policy to suit your association. Where required, adjust, remove or add information per your needs and your attitude to risk. This is not a comprehensive policy but rather a template intended to serve as the basis for your own policy.

Your use of this policy is entirely at your own risk and MCAA therefore makes no conditions, warranties, or representations of any kind.

1. Introduction

This Acceptable Use for Technology is designed to protect the Association, employees, members, and other partners from harm caused by the misuse of the IT systems and data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of the 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, lost productivity, and the possible loss of Association information.

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

2. Definitions

“Users”: anyone who has access to any of the Association’s systems. This includes employees and members, outside contractors, agencies, consultants, and suppliers.

“Systems”: all IT equipment that connects to the network or can access association applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, copy machines, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, cloud storage, 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.

Some aspects of this policy affect areas governed by local legislation in certain states (e.g., employee privacy laws): in such cases the Association should develop and issue users with a clarification of how the policy applies locally.

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

4. Use of Technology

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

The Association's systems exist to support and enable the Association. A small amount of personal use is, in most cases, is allowed. However, it must not be in any way detrimental to users own or their colleague's productivity and nor should it result in any direct costs being borne by the Association.

The Association trusts users to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's Technology Systems. If users are uncertain they should consult the Executive Director.

Any information that is particularly sensitive or vulnerable must be securely stored so that unauthorised 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.

The Association may monitor the use of its 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 may access the history of any users.

The Association reserves the right to regularly audit networks and any systems (as defined) to ensure compliance with this policy.

5. Data Security

If data on the Association's systems is 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, or as defined by the Executive Director.

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

Users who are supplied with "systems" by the Association are responsible for the safety and care of that equipment, and the security of software and data stored it and on other 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: setting a secure password on the device will help limit access to the Association's data.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 15 minutes of inactivity. In addition, the screen should be manually locked by the user whenever leaving the machine unattended during the day.

The Association and/or the Executive Director shall work with a technology or IT consultant to make sure all systems are secure and have the updated software and necessary protection.

Users must always guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the Association's systems via email, web downloads, etc.… if a file looks suspicious, do not open/download it, alert the Executive Director or the Technology/IT Consultant.

6. Cyber Liability Insurance

Cyber Liability Insurance can help protect your association from an attack on your server or theft of data from your association. It is strongly suggested that you speak with your insurance carrier to make sure you are covered. Below are a few items to consider and discuss with your insurance broker.

- Retroactive coverage? Data breaches sometimes are not discovered for months, even years. You want to make sure the coverage goes back to the date when the breach occurred.
- Breach continuation? Many times a breach can happen in different areas, or repeat and look very similar, this will help keep them from making them different claims and raising your rates.
- Defense/Settlement Provisions: Make sure you have language allowing the association to pick their own legal team, many insurance carriers pick the legal team for cyber-attacks.
- First Party Restrictions: Many policies have exclusions on liability costs, legal costs associated with the claims. These policies could be costly to the association.
- Third Party Acts: Many associations use third parties to handle some of their technology functions/operations (cloud storage, accounting, etc…). It is important to have coverage for anything being handled by a third party.

- Business Email Compromise: New cyber attacks trick associations into giving them money instead of stealing it. It is basically a trick by someone falsely acting as a vendor, employee, or member which could result in the association giving money away. This is normally not covered by your "crime coverage" because it was done electronically.

- Regulatory Fines and Claims: This area covers data base breach or point of sales terminals. Make sure your carrier knows if you collect credit card information, where the information is stored and how it is used.

7. Passwords

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with this safe password policy.

- Any user with access to the server will be required to change their password every (we suggest 120days).
- The password shall be 8 or more characters and must include a lower case letter, an uppercase letter and a number or a special character (i.e. $%!@).
- Users will not be permitted to use any of the last 5 passwords they have previously used.
- If any user has 10 consecutive failed login attempts, the system will be locked out, the Executive Director and/or the Technology/IT Consultant will be required to unlock the user's account.
- No passwords will be emailed, for any reason.
- The Executive Director and/or IT Consultant can change the user's password.

8. Mobile Devices

Mobile devices, such as smartphones and tablets are important tools for the Association and their use is supported for Association business. However, mobile devices may also present a risk to the Association's data security and can allow unauthorized access to the Association's network.

- All mobile devices, whether owned by the Association or owned by the employees, that have access to Association networks, data, systems or email, shall include laptops, smartphones and tablets.

- Devices must use the most current operating systems and have the most current updates or patches installed.

- Users who wish to store their passwords on the device shall use an encrypted password application.

- Mobile devices must be configured with a secure password as defined in Section 6, the password may be the same as used on other systems/devices.

- User's must report all lost or stolen devices to the Association immediately, including personal devices that were used to access Association data.

- If a user suspects that unauthorized access to company data has taken place on their mobile device, the user must report the incident to the Association immediately.

- Mobile devices must not be "jailbroken" or have any illegal software/applications installed that could circumvent the security protocols. (Jailbroken is to remove the limitations/security designed by the manufacturer to allow for installation of unauthorized software/apps).

- Mobile devices must not be connected to a PC which does not have up-to date anti-virus protection or that does not comply with the Association's data security policy, including a public PC (i.e. local library pc).

9. Unacceptable Use

All users should use their own judgment regarding what is unacceptable use of the Association's systems. The activities below are provided as examples of unacceptable use; however, it is not a complete list. Should a user need to disregard these guidelines to perform their role, they shall consult with and obtain approval from the Executive Director before proceeding.

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

- All activities detrimental to the success of the Association include sharing sensitive information outside the company, such as financial data, and member lists.

- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the Association. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).

- All activities that are inappropriate and/or are detrimental to the Association's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.

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

10. Enforcement

The Association will not tolerate any misuse of its systems and will discipline anyone found to have disobeyed this 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 the termination of employment.

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