McCorvey Companies Technology Acceptable Use Policy

Updated: 7/23/2021

1. Introduction

1.1 - This Acceptable Use Policy (AUP) for IT Systems is designed to protect McCorvey Companies, our employees, customers, and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

1.2 - The repercussions of misuse of our 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.

1.3 - Everyone who works at McCorvey Companies is responsible for the security of our 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 their manager or IT.

2. Definitions

2.1 - Users are everyone who has access to any of McCorvey Companies' IT systems. This includes permanent employees and temporary employees, contractors, agencies, consultants, suppliers, customers, and business partners.

2.2 - Systems means all IT equipment that connects to the corporate network, accesses corporate applications, or is owned by McCorvey Companies. 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

3.1 - This is a universal policy that applies to all Users and all Systems. For some Users and/or some Systems a more specific policy exists in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.

3.2 - This policy covers only internal use of McCorvey Companies’ systems and does not cover use of our products or services by customers or other third parties.

4. Use of IT Systems

4.1 - Users have no expectation of privacy when using a McCorvey Companies System or Software as a Service (SaaS) application. All activity can be actively monitored, reviewed, or audited at any time without users consent or notification.

4.2 - McCorvey Companies' systems exist to support and enable the business. 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 and nor should it result in any direct costs being borne by McCorvey Companies other than for trivial amounts (e.g., an occasional short telephone call).

4.3 - McCorvey Companies trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's IT systems. If employees are uncertain, they should consult their manager.

4.4 - 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.

4.5 - Controlling the security, availability, and financial impact of all IT systems is solely the responsibility of the IT manager. Any new software or system must be evaluated, approved, and purchased by an IT manager.

4.6 - McCorvey Companies can monitor the use of its IT systems and the data on it at any time. This may include examination of the content stored within the email and data files of any user, and examination of the access history of any users.

5. Data Security

5.1 - Users must take all necessary steps to prevent unauthorized access to confidential information.

5.2 - Users are expected to assume all data on company systems is confidential.

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

5.4 – Users may have access to information that they are not authorized to view, use, or transmit. All users must seek explicit written permission to view, use, or transmit any information stored on any computer systems.

- Example: A user has been tasked to update a file named "material costs" in a folder on the network. In that same folder there is another file named "employee pay rates". The user has access to the folder, and authorization to open the "material costs" file, but the user does not have authorization to open the "employee pay rates" file, even though they have the access to do so. Opening the "employee pay rates" file would be a data access violation.

5.5 - Data on local devices, this includes, but is not limited to, desktop computers, laptops, smartphones, and tablets, is not backed up. McCorvey Companies only provides backup mechanisms for their servers. Users must save all company related information to the appropriate location on the provided company servers. Any data saved anywhere other than on the appropriate server location will be lost in the event of a failure, software or hardware, of the local device.

5.6 - Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with McCorvey Companies' safe password policy.

5.7 - Users must not allow any third-party access to any McCorvey system or Software as a Service application using their credentials.

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

5.9 - Because information on portable devices, such as laptops, tablets, and smartphones, is especially vulnerable, special care should be exercised with these devices. 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.

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

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

5.12 - Users must always guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into McCorvey Companies' systems by whatever means and must report any actual or suspected malware infection immediately.

6. Unacceptable Use

6.1 - All employees should use their own judgment regarding what is unacceptable use of McCorvey Companies' systems. The activities below are provided as examples of unacceptable use; however, it is not exhaustive. Should an employee need to contravene these guidelines to perform their role, they should consult with and obtain approval from an IT manager 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 McCorvey Companies. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.
- Registration of any software or service to be used by yourself or department for any company business activity without consent of an IT Manager.
- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network.
- All activities that are inappropriate for McCorvey Companies 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 McCorvey Companies has put in place.
- Data access violations: viewing, using, or transmitting any files the user does not have explicit authorization to view.

7. Enforcement

7.1 - McCorvey Companies 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 the termination of their employment.

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

McCorvey Companies Safe Password Policy

1. Policy Statement

1.1 - All individuals are responsible for safeguarding their login(s) and password(s) to any company related system and must comply with the password standards identified in this policy. Passwords must meet the complexity requirements outlined and must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

2. Entities Affected by this Policy

2.1 - Any individual, system, or company that has access to any McCorvey Companies internal system or Software as a Service (SaaS) applications.

3. Contacts

3.1 - Direct any questions about this policy to support@mccorvey.com

4. Individual Responsibilities

4.1 - Individuals are responsible for keeping passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:

4.1a

- Passwords must never be shared with another individual for any reason or in any manner not consistent with this policy. A shared or compromised password can generate a written infraction.
- All users must never ask anyone else for their password. If you are asked to provide your password to an individual or sign into a system and provide access to someone else under your login, you are obligated to report this to IT immediately.
- Passwords must never be written down or left in a location easily accessible or visible to others. This includes both paper and digital formats. Company passwords should not be stored in a web browser's password manager on a non McCorvey issued Device.
- Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.
- IT will never ask for a password, instead IT will ask you to enter your password for them. In certain support scenarios where an administrative account cannot be used, an individual may allow a technician to utilize his/her computer under the individual's account even if the individual is unable to be present during the entire support session.
- In the event of a hardware malfunction and the device needs to be repaired by a third-party, the device hard drive should be backed up to a secure storage device and wiped securely prior to being handed over to an external technician
- In the event that a password needs to be issued to a remote user or service provider, the password must never be sent without the use of proper safeguards (e.g., do not send passwords through email without encryption).

- Passwords for McCorvey Systems must be unique and different from passwords used for other personal services (e.g., banking).
- Passwords must meet the complexity requirements outlined in this policy.
- Passwords must be changed regularly, as outlined in this policy, at the regularly scheduled time interval or sooner if there is suspicion of a compromise.
- In the event a breach or compromise is suspected, the incident must be reported to IT immediately.

5. Password Requirements

5.1 User Level Accounts

5.1a - The following parameters indicate the minimum requirements for passwords for all user level accounts. User level accounts consist of McCorvey Companies staff (including temps and consultants) that are not Systems Administrators.

- At least sixteen (16) characters;
- Not based on anything somebody else could easily guess or obtain using personal related information (e.g., names, telephone numbers, dates of birth, etc.);
- Not vulnerable to a dictionary attack (see Recommendations for Creating Compliant Passwords section);
- A combination of at least one character from each of the following four listed character types:
  - English uppercase letters (A-Z),
  - English lowercase letters (a-z)
  - Base 10 digits (0-9)
  - Non-alphanumeric (such as ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . / and space)

5.2 System/Administrative Accounts

5.2a - The following parameters indicate the minimum requirements for passwords for all system/administrative level accounts. System/administrative users consist of users with elevated access to administer information systems and applications, most often in the Information Technology Department. Such users have administrator access and these accounts are at a higher risk for compromise.

- At least thirty-two (32) characters;
- A randomly generated combination of at least one character from each of the following four listed character types:
  - English uppercase letters (A-Z),
  - English lowercase letters (a-z)
  - Base 10 digits (0-9)
  - Non-alphanumeric (such as ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . / and space)

6. Recommendations for Creating Compliant Passwords

6.1 - To create a password that is compliant with the parameters specified in this policy, use one of the three methods below.

6.1a - Use a Passphrase

A passphrase is like a password, but it is generally longer and contains a sequence of words or other text to make the passphrase more memorable. A longer passphrase that is combined with a variety of character types is exponentially harder to breach than a shorter password. However, it is important to note that passphrases that are based on commonly referenced quotes, lyrics, or other sayings are easily guessable. Passphrases should be unique to you.

- Use at least twenty (20) characters
- Incorporate the four-character types (a space or special character can be used to separate words or phrases to add complexity)
- Use a phrase that is easy to remember
- Abbreviate most of the words in the phrase to increase complexity

Examples:

Phrase: “When I was five, I learned how to ride a bike.”

Password: When I was 5, I learned to ride a bike.

Phrase: “When I was five, I learned how to ride a bike.”

Password: WheIwas5,Ilear2ridabik.

6.1b - Use an Acronym

An acronym can be used to constitute a strong and compliant password by taking the first letter of each word in a phrase (including punctuation) to form the password.

- Incorporate the four-character types (forming your phrase in sentence case with punctuation can be used to meet the requirements)
- Use a phrase that is easy to remember

Example:

Phrase: “When I was five, I learned how to ride a bike.”

Password: WIw5,Ilhwrab.

6.1c - Use a Secret Code

A secret code can be used in conjunction with the previous methods simply by substituting letters for other numbers or symbols. Combining these methods will make it easy to incorporate the four-character types to meet the password complexity requirements.

- Use a phrase that is easy to remember
- Capitalize the first letter of every word

- Substitute letters for numbers or symbols
- Incorporate spaces or substitute with a different character

Example:

Phrase: “When I was five, I learned how to ride a bike.”

Password: WhenIwa$5,Ilh0wt0rab1k3.