MCUL and CU Solutions Group
Technology and Security Use Policies

Revision Date: December 2024

Table of Contents

Technology and Security Policies

Purpose of these policies is to protect the organization, its staff and its customers/members
The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate use and protection of data and technologies used by the Michigan Credit Union League (MCUL) and CU Solutions Group (CUSG)—collectively known as the organization.

Scope of policy applies to anyone attaching to or using the organization's technology
This policy applies to all team members, contractors, consultants, temporaries, other workers, and guests at the organization, including those team members affiliated with third parties who access theorganization's computer networks. Throughout this policy, "team member" and "user" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by MCUL or CUSG.

General Policy

- All information traveling over the organization's computer networks that has not been specifically identified as the property of other parties will be treated as though it is a corporate asset.
- The organization prohibits unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.
- It is our policy to protect information belonging to third parties that has been entrusted to the organization in confidence in the same manner as MCUL or CUSG trade secrets as well as in accordance with applicable contracts.
- Technologies provided by the organization are intended for business use only.

Team members are responsible for complying with this and all other MCUL or CUSG policiesdefining computer and network security measures.

Security is every team member's duty

- Team members are responsible for adhering to the policies in this document.
- Departmental managers are responsible for ensuring that appropriate computer and communication system security measures are observed in their area.
- The Security Team is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information technology security policies, standards, guidelines, and procedures.
- Information Technology staff are responsible for acting as information technology security coordinators and will take appropriate measures to monitor and protect the organization from technology and security issues.

Technology Usage and Monitoring

Technology is for business use only
MCUL and CUSG technology should be used for business purposes only. Incidental personal use is permissible if the use: (a) does not consume more than a trivial amount of resources that could otherwise be used for business purposes, (b) does not interfere with worker productivity, and (c) does not preempt any business activity.

Monitoring systems are used
It is the policy of the organization to NOT regularly monitor specific team member technology usage. However, the team member technology usage may be monitored to support operational, maintenance, auditing, security, investigative and other similar activities.

Automated filtering and blocking systems are used
The organization may use filtering technologies that limit or block access to programs, files, Web sites, email messages, etc. that are not appropriate or needed for the work environment. If access is blocked to anything needed for business purposes, a request should be made to the Internal Technology Department via the Helpdesk ticketing system, to unblock it.

Copyright protection laws are fully supported
Using and/or making unauthorized copies of licensed and copyrighted software is strictly forbidden.

Use of non-company technologies is not allowed
Team members must not bring non-company supplied computers, computer peripherals, or computersoftware into the organization's facilities without prior authorization from the IT Department.
Likewise, non-company supplied systems may not remotely connect organization's network unless the Security Team has first approved the systems for use. Acceptable remote access includes access to email and other services made available via general Internet connectivity.

Company equipment is not to leave facility without prior approval
Technology equipment must not leave the offices without prior permission of the IT Department. In most instances check-out procedures must be followed to remove this equipment fromthe building. Exceptions are laptops, iPads/tablets, cell phones/smart phones and other portable equipment that has been assigned to a specific individual (policies regarding these equipment types are outlined below in "Portable Equipment and Information" section).

Team members are primary custodians of equipment
The primary user of a computer is considered a custodian of the equipment. If the equipmenthas been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a custodian must promptly inform the involved department manager and/or the IT Department. In most cases, the organization will assume all risks of loss or damage to these items.

Computer Relocation, Hardware Modifications of Software Installation
The department manager is responsible for requesting computer relocation, hardware modifications, or software installation outside of the standard configuration.

Non-approved connections to company technology is not allowed
Users may not enable or knowingly allow non-approved connections to company technologies.

Email and file storage should be managed appropriately
Email and files no longer needed for business purposes should be periodically purged by users to assist Information Technology in managing system resources.

Privacy and Security

Strong passwords must be used and changed regularly by staff
The computer and communications system privileges of anyone or anything must be restricted based on the need to know. This means that privileges must not be extended unless there is a legitimate business need for them.

- Team members must use strong passwords that are difficult to guess.
- Users should not construct passwords that are identical or substantially similar to passwords they have previously employed (e.g. michigan01, michigan02, etc.).
- Passwords should be changed as required on all systems.
- Passwords should not be stored electronically in readable form or written down and left in a place where unauthorized persons might discover them.
- All passwords must be immediately changed if they are suspected of being disclosed or known to have been disclosed to anyone besides the authorized user.

Disclosure of system information is prohibited
Unless approved by the Security Team, disclosure to outside parties or other unauthorized individuals of information regarding any technology-related system, procedure, configuration or measure employed by MCUL and CUSG is strictly prohibited.

Organization owns all information and reserves rights to review it anytime
Unless contractual agreements dictate otherwise, management reserves the right to examine all data, documents, messages and related files processed in any way on the organization's network or equipment. In all situations, permission from management or HR must be gained prior to such access being granted.

Transfer of sensitive information is restricted
It is highly recommended that email or other electronic means not be used for transferring or receiving proprietary or sensitive information. If it is necessary, proper security safeguards (e.g. encryption) should be taken. Under no circumstances should proprietary or sensitive information be accessed remotely via email or any other method on equipment not supplied by the company.

Client and proprietary information is protected and release of it is restricted
Deliberate misuse, unauthorized disclosure, or gross negligence in protecting of client and proprietary information is cause for disciplinary action up to and including dismissal.

Technology staff may review files/email to resolve technology issues
It may be necessary for technical support personnel to review the content of an individual team member's files and communications during the course of problem resolution. Technical support personnel may only perform such reviews with the explicit knowledge of the impacted team member, manager or HR.

All systems should have virus protection
PCs and laptops must have, and servers should have virus protection running at all times with current signature files installed. Updates to signature files should be disseminated automatically via a central AV provider service. Expectations to this policy should be very limited, and only approved by IT team members.

Disabling of security mechanisms are prohibited
Certain security mechanisms and applications (i.e. firewalls, virus protection software, etc.) will be employed to help protect the organization, its staff and customers from security-related issues. As a result, users may not bypass such mechanisms unless express permission is given by IT team members.

Privacy and information delivery cannot be guaranteed
The organization cannot guarantee that electronic communications will be private or delivered. In addition, general Internet activities, transactions and transactions are not automatically protected from viewing by third parties. Unless encryption is used or otherwise secured in some manner, team members should not send information over the Internet if they consider it to be confidential or private.

Security problems are to be reported immediately
If any unauthorized use, disclosure, access or loss of MCUL, or CUSG 's information technology has taken place, or is suspected of having taken place, Helpdesk must likewise be notified immediately. The specifics of security problems should not be discussed widely but should instead be shared on a need to know basis. Additionally, the specifics of any security issues regarding client accounts should also be kept confidential.

Hacking is prohibited
Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the head of the IT Department, including developing or using malicious programs (e.g. viruses, etc.). Any team member performing such activities will be subject to disciplinary action up to and including dismissal.

Public presentations of company is restricted
Team members may not establish Web pages or publicly post information dealing with MCUL or CUSG business without express business authority and approval to do so.

Passwords should not be saved in browser or similar applications
Users should not save fixed passwords in their Web browsers or electronic mail clients.

Management should regularly review system privileges assigned to their staff
Management should annually reevaluate the system privileges granted to users. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

Information Technology should be promptly notified when system privileges need to be changed
Managers or Human Resources must promptly report all significant changes in duties, security requirements or employment status, including separations, (for team members, contract team members and guests) to the system administrators responsible for user IDs associated with the involved persons. Any involved manager and the IT Department should reevaluate all system privilegesfor that user and determine if access that should be added or revoked.

Acquisition of and Changes to Technology

Unapproved acquisition and use of technology is not allowed
The acquisition and use of any technology used within or connecting to the organization's systems must be approved by the IT Department or CEO. This includes all hardware, software, communication lines, networking equipment, Internet-related services or applications, peripherals and other devices and technologies that are purchased or acquired in any other manner.

Unapproved changes to software are not allowed
Team members must not alter or install software on their computers without obtaining advancedpermission from the IT Department.

Unapproved changes to hardware are not allowed
Computer equipment supplied by the organization must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without the prior knowledge of and authorization from the IT Department.

Unapproved downloading software is not allowed
Without prior authorization, team members must not download software from any system outside theorganization onto computers used to handle MCUL or CUSG data.

Portable Equipment and Information

Portable equipment and information should remain in staff possession
Team members in possession of a company issued laptop, iPad/tablet, Smartphone or other transportable equipmentor company information/data must take due care to protect these assets. This includes keeping these items in possession or always locked securely when out in public, including at other offices, in hotels, airports, etc. Team members should not check these computers in airline luggage systems, with hotel porters, etc. These computers should remain in the possession of the traveleras hand luggage.

Portable equipment should be disconnected and turned off when not in use
Team members must not leave their computers unattended when remotely connected to the MCUL and CUSG network.

Hardware is required to be enrolled in Intune
Any hardware used to access company data will be enrolled in MCUL/CUSG Intune. This includes personal hardware equipment including cell phones, personal laptops, or other mobile devices.

Any team member with company issued hardware is required to utilize that equipment
Full time/regular team members issued a laptop upon employment are required to utilize that hardware and are not permitted to utilize their personal computers for company data access or storage.

Personal Mobile Device Use for Security Access
To ensure the security and integrity of company systems, certain security protocols, including multi-factor authentication (MFA) or other forms of verification, may require team members to use their personal mobile devices. By accessing company systems, team members acknowledge and consent to using their personal devices for these security purposes. This may include physical office security or company system security. The company will take all reasonable measures to ensure data privacy and will not access or interfere with personal information on these devices.

Policy Compliance
Failure to comply with policies may result in disciplinary action, up to and including termination of employment.

Company owned items must be returned when team member leaves the organization
If the organization has supplied a staff member with software, hardware, furniture, information, or other materials to perform organization business remotely, the title to, and all rights and interests to these items will remain with the organization. In such instances, staff member possession does not convey ownership or any implication of ownership. Accordingly, all such items must be promptly returned to the organization when a staff member separates from MCUL or CUSG, or when so requested by the team member's manager, COO or HR. Organization information should be protected in a manner commensurate with its sensitivity, value, and criticality. As a result, any security systems put in place by the organization must not be disabled.

Loss of Equipment or Team member Termination

Protection of information in the event of equipment loss or team member termination
If equipment that has been used to access organization information is lost or stolen, or an team member that has used equipment to access MCUL or CUSG information is terminated, the organization has the responsibility to protect the information. If organization management determines that it is necessary, the Director of IT or Tech Support Specialist will 'wipe' the device used to access the information, **even if the device is the personal property of the affected team member or former team member**. The term 'wipe' can refer to the process where the device is reset to an 'as new' state and any existing information on the device is deleted, however it will be general practice to only remove company owned data from any personal equipment.