Acceptable Use Policy, version 1.0.0

Status: ☐ Working Draft ☒ Approved ☒ Adopted
Document Owner: Information Security Committee
Last Review Date: March 14, 2022

Acceptable Use Policy

Purpose

The purpose of the Western Iowa Tech Community College Acceptable Use Policy is to establish acceptable practices regarding the use of Western Iowa Tech Community College **Information Resources** in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

Audience

The Western Iowa Tech Community College Acceptable Use Policy applies to any individual, entity, or process that interacts with any Western Iowa Tech Community College **Information Resource**.

Contents

Policy

Acceptable Use

- Personnel are responsible for complying with Western Iowa Tech Community College policies when using Western Iowa Tech Community College information resources and/or on Western Iowa Tech Community College time. If requirements or responsibilities are unclear, please seek assistance from your manager.
- Personnel must promptly report harmful events or policy violations involving Western Iowa Tech Community College assets or information to their manager or a member of the Incident Handling Team (defined in the incident response policy). Events include, but are not limited to, the following:
    - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to Western Iowa Tech Community College **Information Resources**.
    - Data incident: any potential loss, theft, or compromise of Western Iowa Tech Community College information.
    - Unauthorized access incident: any potential unauthorized access to a Western Iowa Tech Community College **Information Resource**.
    - Facility security incident: any damage or potentially unauthorized access to a Western Iowa Tech Community College owned, leased, or managed facility.
    - Policy violation: any potential violation to this or other Western Iowa Tech Community College policies, standards, or procedures.
- Personnel are prohibited from purposely engaging in activity that may
    - harass, threaten, impersonate, or abuse others;
    - degrade the performance of Western Iowa Tech Community College **Information Resources**;
    - deprive authorized Western Iowa Tech Community College personnel access to a Western Iowa Tech Community College **Information Resource;**
    - obtain additional resources beyond those allocated;
    - or circumvent Western Iowa Tech Community College computer security measures.
- Personnel are not allowed to download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, Western Iowa Tech Community College personnel may not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any Western Iowa Tech Community College **Information Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on Western Iowa Tech Community College time and/or using Western Iowa Tech Community College **Information Resources** are the property of Western Iowa Tech Community College.
- Use of encryption must be managed in a manner that allows designated Western Iowa Tech Community College personnel to promptly access all data.
- Western Iowa Tech Community College **Information Resources** are provided to facilitate College business. Employees are prohibited from using these resources for personal financial gain.
- Personnel are expected to cooperate with incident investigations, including any federal or state investigations.

- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using Western Iowa Tech Community College **Information Resources**.
- Personnel should not intentionally access, create, store or transmit material which Western Iowa Tech Community College may deem to be offensive, indecent, or obscene.

Access Management

- Access to information is based on a "**need to know**".
- Personnel are permitted to use only those network and host addresses issued to them by Western Iowa Tech Community College Information Technology department and are not allowed to access any data or programs contained on Western Iowa Tech Community College systems for which they do not have authorization or explicit consent. Attempts to circumvent Information Resources security will result in disciplinary actions.
- All requests for access to any data or programs must be submitted by the employee's supervisor using the Access Request Form. This request must be approved by the Executive Council member they report through and the Dean of Information Technology.
- All remote access connections made to internal Western Iowa Tech Community College networks and/or environments must be made through approved, Western Iowa Tech Community College-provided, virtual private networks (VPNs) on college owned computers.
- Personnel must not divulge any access information to anyone not specifically authorized to receive such information, including IT support personnel.
- Personnel must not share their personal authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Multi-factor authentication information
    - Access cards and/or keys,
    - Digital certificates,
    - Similar information or devices used for identification and authentication purposes.
- Access cards and/or keys that are no longer required must be returned to physical security personnel.
- Lost or stolen access cards, security tokens, and/or keys must be reported to physical security personnel as soon as possible.

Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following Western Iowa Tech Community College rules:
    - Must meet all requirements including minimum length, complexity, and reuse history.
    - Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
    - Must not be the same passwords used for non-business purposes.
- User account passwords must not be divulged to anyone.

- If the security of a password is in doubt, the password should be changed immediately.
- Security fobs, and keys must be returned on demand or upon termination of the relationship with Western Iowa Tech Community College, if issued.

Clear Desk/Clear Screen

- Personnel are required to log off or lock their workstations and laptops when their workspace is unattended.
- Confidential or internal information is to be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
- Personal items, such as phones, wallets, and keys, should be removed or placed in a locked drawer or file cabinet when the workstation is unattended.
- File cabinets containing **confidential information** are to be locked when not in use or when unattended.
- Physical and/or electronic keys used to access **confidential information** should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Passwords must not be posted on or under a computer or in any other physically accessible location. This will be periodically audited.
- Copies of documents containing **confidential information** should be immediately removed from printers and fax machines.

Data Security

- Personnel must use approved encrypted communication methods whenever sending **confidential information** over public computer networks (Internet).
- **Confidential information** transmitted via USPS or other mail service must be secured in compliance with the Information Classification and Management Policy.
- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential information**.
- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
- Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
- **Confidential information** must be transported either by an Western Iowa Tech Community College employee or a courier approved by the College.
- All electronic media containing confidential information must be securely disposed. Please contact IT for guidance or assistance.

Email and Electronic Communication

- Auto-forwarding electronic messages outside the Western Iowa Tech Community College internal systems are prohibited unless approved by the CIO and the Cyber Security Incident Response Team (CSIRT).
- Electronic communications should not mis-represent the originator or Western Iowa Tech Community College.
- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.

- Accounts must not be shared without prior authorization from Western Iowa Tech Community College IT, with the exception of calendars and related calendaring functions.
- Employees are not to use personal email accounts to send or receive Western Iowa Tech Community College **confidential information**.
- Any personal use of Western Iowa Tech Community College provided email should not:
    - Involve solicitation.
    - Have the potential to harm the reputation of Western Iowa Tech Community College.
    - Contain or promote anti-social or unethical behavior.
    - Violate local, state, federal, or international laws or regulations.
    - Result in unauthorized disclosure of Western Iowa Tech Community College **confidential information**.
    - Or otherwise violate any other Western Iowa Tech Community College policies.
- **Confidential information** must use approved secure electronic messaging solutions to be sent to an approved external recipient.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should use discretion in disclosing **confidential information** in Out of Office or other automated responses, such as employment data, personal telephone numbers, location information or other sensitive data.

Hardware and Software

- All hardware must be formally approved by IT Management before being connected to Western Iowa Tech Community College network servers that contain confidential information.
- Software installed on Western Iowa Tech Community College equipment must be approved by IT Management and installed by Western Iowa Tech Community College IT personnel.
- All Western Iowa Tech Community College assets taken off-site must be physically secured at all times.
- Allowing family members or other non-employees to access Western Iowa Tech Community College issued laptop, tablet, MiFi or any other College device as well as **Information Resources** is prohibited.

Internet

- The Internet must not be used to communicate Western Iowa Tech Community College **confidential information**, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with Western Iowa Tech Community College networking or computing resources must only be used for business-related activities and may not violate any other Western Iowa Tech Community College policies.
- Access to the Internet from outside the Western Iowa Tech Community College network using a Western Iowa Tech Community College owned computer must adhere to all of the same policies that apply to use from within Western Iowa Tech Community College facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- Mobile devices that access Western Iowa Tech Community College email must have Multi-Factor Authentication enabled.
- **Confidential information** is never to be stored on mobile or removable devices.

- Theft or loss of any **mobile device** that has been used to create, store, or access **confidential** or **internal information** must be reported to the Western Iowa Tech Community College Security Team immediately by calling 712-274-8733 ext 1461.
- All **mobile devices** should maintain up-to-date versions of all software and applications.
- All personnel are expected to use **mobile devices** in an ethical manner.
- **Jail-broken** or rooted devices should not be used to connect to Western Iowa Tech Community College **Information Resources**.
- Western Iowa Tech Community College IT Management may choose to execute **"remote wipe"** capabilities for WITCC provided **mobile devices** without warning (see Mobile Device Email Acknowledgement).
- In the event that there is a suspected **incident** or breach associated with a WITCC provided **mobile device**, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- Western Iowa Tech Community College IT support for **personally owned mobile devices** is limited to assistance in complying with this policy. Western Iowa Tech Community College IT support may not assist in troubleshooting device usability issues.
- Use of **personally owned** devices must be in compliance with all other Western Iowa Tech Community College policies.
- Texting or emailing while driving is not permitted while on company time or using Western Iowa Tech Community College resources. Only hands-free talking while driving is permitted, while on company time or when using Western Iowa Tech Community College resources.

Physical Security

- Non-IT Personnel must badge in and out of access-controlled areas. Piggy-backing, tailgating, door propping and any other activity to circumvent door access controls are prohibited.
- Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel at all times or be approved by Security and sign in and out of secured area.
- Eating or drinking are not allowed in data centers.
- Caution must be used when eating or drinking near workstations or information processing facilities.

Privacy

- Information created, sent, received, or stored on Western Iowa Tech Community College **Information Resources** are not private and may be accessed by Western Iowa Tech Community College IT employees at any time, under the direction of Western Iowa Tech Community College executive management and/or Human Resources, without knowledge of the user or resource owner.
- Western Iowa Tech Community College may log, review, and otherwise utilize any information stored on or passing through its **Information Resource** systems.
- Systems Administrators, Western Iowa Tech Community College IT, and other authorized Western Iowa Tech Community College personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges are not allowed to access files and/or other information that is not specifically required to carry out an employment related task. All personnel with extended privileges will be required to agree to and sign the Network/System Administrator Ethics policy.

Removable Media

- The use of **removable media** for storage of Western Iowa Tech Community College information must be supported by a reasonable business case.
- All **removable media** use must be approved by Western Iowa Tech Community College IT prior to use.
- **Personally owned removable media** use is not permitted for storage of Western Iowa Tech Community College information.
- Personnel are not permitted to connect **removable media** from an unknown origin without prior approval from the Western Iowa Tech Community College IT.
- All removable media must be stored in a safe and secure environment.
- The loss or theft of a **removable media** device that may have contained any Western Iowa Tech Community College information must be reported to the Western Iowa Tech Community College IT Helpdesk by calling 712-274-8733 ext. 1461.

Security Training and Awareness

- All new personnel must complete an approved **security awareness** training prior to, or within 30 days of being granted access to any Western Iowa Tech Community College **Information Resources**.
- All personnel must be provided with and acknowledge they have received and agree to adhere to the Western Iowa Tech Community College Information Security Policies before they are granted to access to Western Iowa Tech Community College **Information Resources**.
- All personnel must complete the annual security awareness training.

Social Media

- Communications made with respect to social media must be made in compliance with all applicable Western Iowa Tech Community College policies.
- Employees are personally responsible for the content they publish online.
- Creating any public social media account intended to represent Western Iowa Tech Community College, including accounts that could reasonably be assumed to be an official Western Iowa Tech Community College account, requires the permission of the Western Iowa Tech Community College Marketing Department.
- When discussing Western Iowa Tech Community College or Western Iowa Tech Community College -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an Western Iowa Tech Community College representative, and
    - Make it clear that you are speaking for yourself and not on behalf of Western Iowa Tech Community College, unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at Western Iowa Tech Community College.
- When publishing Western Iowa Tech Community College-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; “The opinions and content are my own and do not necessarily represent Western Iowa Tech Community College’s position or opinion.”
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations,

or ordinances) in published content that is affiliated with Western Iowa Tech Community College will not be tolerated.

- **Confidential information**, internal communications and non-public financial or operational information may not be published online in any form.
- Personal information belonging to customers may not be published online.
- Personnel approved to post, review, or approve content on Western Iowa Tech Community College social media sites must follow the Western Iowa Tech Community College Social Media Management Procedures.
- Western Iowa Tech Community College Social and Digital Media Guidelines:
    - Social media technology can serve as a powerful tool to enhance education, communication, and learning.
    - Platforms like Facebook, Twitter, YouTube and LinkedIn have become important and influential communication channels for our community. They can provide both educational and professional benefits, including preparing Western Iowa Tech Community College (WITCC) students to succeed in their educational and career endeavors. To assist in posting content and managing these and other sites, we have developed policies and guidelines for official and personal use of social media.
    - The purpose of using social media channels on behalf of Western Iowa Tech Community College is to support the College's mission, goals, programs and sanctioned efforts, including college news, information, content and directives. Social media is also a powerful tool for building pride and encouraging dialogue among our students, business and community members.
    - These policies and guidelines apply to college faculty, staff and students and can be used in connection with social media accounts associated with our college's departments, programs, offices, clubs and teams. These policies and guidelines do not address students' personal use of social media. This document is meant to provide general guidance and does not cover every potential social and digital media situation. Should any questions arise, please contact the WITCC Marketing and Publications Department.
    - Western Iowa Tech Community College's official social media accounts include:
        - Facebook: http://www.facebook.com/WesternIowaTech
        - Twitter: https://twitter.com/WesternIowaTech - @WesternIowaTech
        - LinkedIn: www.linkedin.com/company/westerniowatech
        - YouTube: https://www.youtube.com/WesternIowaTech
        - Instagram: http://instagram.com/westerniowatech/
    - Western Iowa Tech Community College's official hashtags are:
        - #westerniowatech
        - #witcc

- **Social Media Policy**

  Introduction and Purpose:
    - Social media technology can serve as a powerful tool to enhance education, communication, and learning. This technology can provide both educational and professional benefits, including preparing Western Iowa Tech Community College ("WITCC") students to succeed in their educational and career endeavors.
    - WITCC employees who utilize social media technology for professional purposes described below, including staff and faculty, should do so in a safe and responsible

manner. WITCC strives to create professional social media environments that mirror the academically supportive environments of our institution.

- **Instructions and Practices**
  - These Social Media Guidelines provide proper instructions and practices for WITCC employees/clubs/groups/organizations/etc. in developing professional social media platforms and presence as represented by WITCC. These Guidelines also provide guidance regarding recommended practices for professional social media communication between WITCC employees, students, businesses and community members and individual and personal use of social media as it pertains to Western Iowa Tech Community College.
  - In recognition of the public and pervasive nature of social media communications, as well as the fact that in this digital era, the lines between professional and personal endeavors are sometimes blurred, these Guidelines also address recommended practices for use of personal social media by WITCC employees. Please refer to the WITCC's Computer Conduct Policy –located online at witcc.edu/policies/computer-conduct-policy/for additional guidance.
- **Definition of Social Media**
  - Social media is defined as any form of online publication or presence that allows interactive communication, including, but not limited to, social networks and platforms, blogs, and Internet websites. Examples of social media platforms include, but are not limited to, Facebook, Twitter, YouTube, Google+, and Instagram.
  - Professional social media is a work-related social media activity that is school-based, e.g. a WITCC employee establishing a Facebook page for his/her WITCC club/group/class/blog/etc.
    - Professional Social Media Use: Maintaining Separate Professional and Personal E-mail Accounts WITCC employees who are authorized to engage in professional social media activities should maintain separate professional and personal e-mail addresses. As such, WITCC employees should not use their personal e-mail address for professional social media activities; rather, employees should use a professional e-mail address that is completely separate from any personal social media they maintain. Regular and continuous use of a personal e-mail address for professional purposes, including social media use, may result in WITCC considering the e-mail address, and the corresponding use of that address, as a professional account.
    - Communication with WITCC Students: For WITCC employees who work with students and communicate with students, professional social media sites should be designed to address reasonable instructional, educational, or extra-curricular program matters.
  - Personal social media use is a non work-related social media activity, e.g. an employee establishing a Facebook page or a Twitter account for his/her own personal use.
- **Social Media Platform Development**
  - Entities of WITCC may request to develop a social media platform. All requests are subject to approval by the Digital Media Coordinator and the Marketing and Publication Department.
  - Prior to engaging in any form of social media involving Western Iowa Tech Community College, a few first steps are recommended:
    - Consult with your supervisor and/or your department head and let him/her know that you are interested in utilizing social media in your area.

        - Read over the social media guidelines provided here to familiarize yourself with WITCC policies and expectations.
        - Contact the Digital Media Coordinator, for assistance in determining which, if any, social media channels are right for you and your area. You may be asked to fill out a questionnaire explaining your motive and goals.
        - Work with the Marketing and Publications Department to ensure proper WITCC branding for your social media sites and to help gain friends and followers.
        - Read and acclimate yourself with social media best practices and guidelines.
    - Upon approval, to ensure that all platforms representing WITCC adhere to the design and policy standards of the College and that the efforts are not tied specifically to any personal account, all official WITCC social media accounts must be created by Digital Media Coordinator within the Marketing and Publications Department.
        - The Digital Media Coordinator will then grant the appropriate person(s) administrative access to those accounts. The administrator will be responsible for posting and regularly monitoring postings and content.
        - The Digital Media Coordinator must remain an administrator and have administrative access to the social media platform in use.
        - The Digital Media Coordinator and the Marketing and Publications Department reserves the right to disable, deactivate or temporarily unpublish WITCC social media accounts that are dormant (no posts, no activity) for more than SIX months, as such stagnancy reflects poorly on the College.
- **Best Practices for Posting on Behalf of Western Iowa Tech Community College**
    - Be mindful of all College policies regarding privacy, personnel, and records. Do not post confidential or proprietary information about WITCC students, prospective students, faculty, staff or alumnae. Employees using social media on behalf of the college must follow all applicable federal requirements such as the Educational Rights and Privacy Act.
    - Be mindful of Terms and Policies enforced by each social media platform being used, e.g. Facebook Terms and Policies are available online at www.facebook.com/policies/?ref=pf.
    - Commercial Promotion and Partnerships. WITCC is a non-profit institution. We discourage commercial promotion via college social media channels, e.g. a promotion for roses at commencement time from a local florist. Do not use WITCC's brand to promote or endorse any product, cause or political party or candidate. Avoid conflicts of interest and maintain a distinction between your personal identity and the identity you represent on behalf of the university. However, the College does partner and establish several business relationships. If the College does have an established partnership with another business, you are free to post at your discretion in regards to that business or product, e.g. a post promoting free tickets for students and faculty to the upcoming the Sioux City Bandits game.
    - Plan in advance. Set up a content calendar with pre-planned posts. Work with the Digital Media Coordinator to discuss how often you should post for your preferred platform. Keep in mind, if you decide to setup pre-scheduled posts and a cancelation occurs, such as inclement weather, remember to check pre-scheduled posts to edit accordingly.
    - Posting and content management.

        - Be factual. Make sure that you have all the facts before you post. Verify information with a source first to avoid having to post a correction or retraction later.
        - Use proper grammar.
        - Cite, @mention, and link to your sources whenever possible--that's how you build community.
    - React quickly. Hopefully you'll be receiving positive feedback on social media, but chances are you'll also get complaints. It is crucial to act quickly and respond to those complaints.
    - Press Inquiries. Any press inquiries received via professional social media sites should be referred to the Marketing and Public Relations Department.
- **Individual and Personal Use of Social Media as it pertains to Western Iowa Tech Community College**
    - In order to maintain a professional and appropriate relationship with students, WITCC employees are encouraged not communicate with students on personal social media sites who are currently enrolled with the College and/or are in a faculties' class or program.
        - WITCC employees' communication with WITCC students via personal social media is subject to the following exceptions: (a) communication with relatives and (b) if an emergency situation requires such communication, in which case the WITCC employee should notify his/her supervisor of the contact as soon as possible. Be mindful of all College's policies regarding privacy and confidentiality as it is previously stated.
    - WITCC employees' must clearly brand their online posts as personal and purely their own when referencing the College. The College should not be held liable for any repercussions the employees' content may generate.
    - Employees should not use WITCC's logo or make representations that their personal social media sites speak in an official WITCC capacity. However, use of the College logo that is automatically populated on personal social media sites, such as LinkedIn, is permitted. For outstanding circumstance or to request permission to use the logo, contact the WITCC Marketing and Publications Department.

VoiceMail

- Personnel are prohibited from disclosing **confidential** or **internal information** in voicemail greetings, such as employment data, location information or other sensitive data.
- Personnel are prohibited from accessing another user's voicemail account unless it has been explicitly authorized via the Access Request approval form.
- Personnel must not disclose **confidential** information in voicemail messages.

Incidental Use

- As a convenience to Western Iowa Tech Community College personnel, incidental use of **Information Resources** is permitted. The following restrictions apply:
    - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to Western Iowa Tech Community College approved personnel; it does not extend to family members or other acquaintances.
    - Incidental use should not result in direct costs to Western Iowa Tech Community College.

  - Incidental use should not interfere with the normal performance of an employee's work duties.
  - No files or documents may be sent or received that may cause legal action against, or embarrassment to, Western Iowa Tech Community College or its customers.
- Storage of personal email messages, voice messages, files, photos, videos and documents within Western Iowa Tech Community College **Information Resources** must be nominal.
- All information located on Western Iowa Tech Community College **Information Resources** are owned by Western Iowa Tech Community College may be subject to open records requests and may be accessed in accordance with this policy.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	February 2022			Document Origination
1.1	March 2022	3/14/2022	Exec Council	official to put into process