XX.01.01 Information Resource Acceptable Use

Created: **July 2020**
Approved:
Next scheduled review: **September 2022**

Procedure Statement and Reason for Procedure

North Central Texas College (NCTC) policies and regulations require established rules and procedures consistent with organizational policy and regulation requirements. This procedure establishes standards and responsibilities for the acceptable use of information resources.

Table of Contents

Procedures and Responsibilities

1. General

1.1 The rules and procedures specified are based on Federal, State, and NCTC (organization) requirements. A complete list of all related requirements are located in the resources area, Related Statutes, Policies, Regulations, or Rules, at the bottom of this document.

1.2 These guidelines apply to students, faculty, staff partners, contractors, consultants, temporary employees, library patrons, visitors, guests and all other employees of NCTC. This includes all personnel third party affiliates who are using any systems, equipment or resources that are owned, leased or operated by NCTC.

1.3 Any systems used remotely are the property of NCTC and are subject to these regulations.

2. Responsibilities

2.1 The Chancellor is responsible for the security of organizational information resources. The Chancellor or the Chief Information Officer (CIO), shall ensure that senior organization officials and information owners, in collaboration with the Information Security Officer (ISO), support the provision of information security for the information systems used to support all operations and assets under their direct or indirect (e.g., cloud computing or outsourced) control.

2.2 Department Heads are responsible for promptly informing human resources (HR) when an employee has resigned or been terminated so that an employee's network access may be disabled.

2.3 The ISO has the responsibility to:

2.3.1 develop and maintain information security policies and procedures which address the requirements set forth by Texas Administrative Code (TAC) § 202, Subchapter C and the organization's information security risks.

2.3.2 develop and recommend policies and establish procedures and practices, in cooperation with the organization's information resources manager (IRM), i.e., CIO, information owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure.

2.4 "Information Owner" Responsibilities are defined in section 10.

2.5 "Information Custodian Responsibilities" are defined in section 11.

2.6 "User Responsibilities" are defined in section 12 and apply to all who use organizational resources.

3. User Sanctions

3.1 Users of NCTC-owned information resources who fail to comply with NCTC information security regulation and requirements outlined in this document are subject to disciplinary action, up to and including termination of employment, termination of business relationships for contractors or consultants, dismissal for interns and volunteers, and/or suspension or expulsion for students. Additionally, individuals are subject to loss of information resource access privileges as well as civil and criminal prosecution.

4. Information Security Awareness

4.1 Users who have a network account are required to have annual security awareness training (Texas Government Code § 2054.5191).

4.1.1 Any contractor with access to organizational information must complete annual information security awareness training that is approved by the State of Texas, Texas Government Code § 2054.5192.

4.2 Users are required to read and understand this document.

4.3 Employees are responsible to keep up-to-date on rules and procedural changes regarding information resources.

4.4 Employees agree to comply with the Data Use Agreement electronically during the security awareness training.

5. Required Reporting

5.1 Users must report any information security incident to the help desk by submitting a helpdesk ticket or email to itshelpdesk@nctc.edu or report it to the CIO or Information Technology Services (ITS) staff. If a user receives a suspicious email, they shall send the original as an attachment to preserve the email's metadata.

5.2 Users must report lost, stolen, or found equipment such as computers, laptops, USB, and any mobile or storage device.

5.3 Users will report any security violations, signs of wrongdoing, significant security issues discovered, and signs of unauthorized activity.

5.4 Users agree to report any compromise of security which could lead to divulging confidential information including, but not limited to, posting social security numbers, grades, date of birth (DOB), etc. to the internet.

5.5 Users shall report an insider threat if anyone with authorized access to information resources either wittingly or unwittingly attempts to inflict harm to the resources of the organization.

5.6 If criminal activity is suspected, the NCTC Police Department or other appropriate law enforcement agencies must be notified. All further access to data on information resources must be in accordance with directives from law enforcement agencies. If law enforcement is notified, employees must also notify the ISO at iso@nctc.edu.

6. Privacy

6.1 There is no expectation of privacy when using organizational information resources (e.g., devices, email, instant messaging, etc.) beyond that which is expressly provided by applicable privacy laws.

6.2 Users should not store private information (e.g., personal passwords, pictures, and emails, etc.) on organization-controlled devices. Information can become the property of the organization, be collected for legal use, or be subject to the Texas Public Information Act (TPIA), Texas Government Code § 552.

6.3 Information created, stored, or transmitted on information resources may be subject to disclosure under the Texas Public Information Act or through legal or administrative proceedings.

6.4 To manage the efficient operation of information systems, appropriate security practices, and issues relating to inappropriate or illegal use, the organization may log, review, and otherwise use any information stored on or passing through its information resources. All such actions shall be in accordance with the provisions and safeguards provided in the Texas Administrative Code § 202, information resource security standards, and other applicable rules and laws.

6.5 The organization collects and processes many different types of information from third parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations, e.g., General Data Protection Regulation (GDPR), Gramm-Leach-Bliley Act (GBLA), and Texas Administrative Code § 206.

6.6 Users shall not attempt to access any data or information resources for which they do not have appropriate access, authorization, or explicit consent from the data owner.

6.7 The ability to read a file does not imply authorization to read or alter it. Under no circumstances may a user alter a file that does not belong to them or the department, unless given explicit consent by the file's owner.

6.8 Departmental Heads own departmental data unless specifically delegated.

6.9 Information resource owners or custodians will provide access to information (requested by auditors) on the performance of their jobs. Notification to file owners will be sent as directed by the auditors.

6.10 Users who have special access to information because of their position have the absolute responsibility of not abusing that access. If information is inadvertently gained (e.g., seeing a copy of a test or homework) which could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the organizational unit head.

6.11 Websites available to the general public shall contain a Privacy Policy and follow EIR accessibility requirements as specified in Texas Administrative Code § 213.

6.12 Additional resources regarding privacy concerns can be found here

6.12.1 https://www.nctc.edu/research-reporting/privacy-concerns.html

7. Privacy of HIPAA Data

7.1 Computers and devices that access HIPAA-protected data will be located on an isolated network segment. All traffic into and out of the network is logged. Access to certain internet sites may be restricted or forbidden.

7.2 Computers and devices that access HIPAA-protected data are primarily for HIPAA-protected data. The use of an organizational computer for personal business may be a violation.

7.3 No HIPAA-protected data may be saved outside of the Electronic Medical Records (EMR) system, including the hard drive(s) in the local system or externally attached storage.

7.4 All computers must begin with a known, clean image, free of malicious hardware/software, before any software with access to the EMR system is loaded. In the event of a data breach, hard drives in the affected machines will be removed and replaced with a new hard drive with a known, clean image.

7.5 End users will not be granted administrative access to any computer that can access HIPAA-protected data and may not install, uninstall, or otherwise alter the computer's software unless the request is made through and approved by ITS.

7.6 Approval from the ISO is required before installing any newly acquired software to prevent increasing the risk for an information breach.

7.7 Under HIPAA privacy rules, all medical information and any other individually identifiable health information in any form, whether electronic, hard copy, or oral, is considered protected health information (PHI). This includes any information related to the past, present, or future physical or mental health or condition of an individual. Individually identifiable health information includes, but is not limited to, the following:

7.7.1 names

7.7.2 addresses (including subdivisions smaller than state such as street, city, county, and zip code)

7.7.3 dates (except years) directly related to an individual, such as DOB, admission/discharge dates, death dates, and exact ages of individuals older than 89

7.7.4 telephone numbers

7.7.5 fax numbers

7.7.6 email addresses

7.7.7 Social Security numbers

7.7.8 medical record numbers

7.7.9 health plan beneficiary numbers

7.7.10 account numbers

7.7.11 certificate and license numbers

7.7.12 vehicle identifiers

7.7.13 device identifiers and serial numbers

7.7.14 website URLs

7.7.15 IP addresses

7.7.16 biometric identifiers, including fingerprints, voice prints, iris and retina scans

7.7.17 full-face photos and other photos that could allow a patient to be identified, and

7.7.18 any other unique identifying numbers, characteristics, or codes.

7.8 A person is subject to punishment under the law when they knowingly and in violation of the HIPAA Privacy Rule:

7.8.1 use, or cause to be used a unique health identifier;

7.8.2 obtain individually identifiable health information relating to an individual; or

7.8.3 disclose individually identifiable health information to another person.

8. Privacy of FERPA Data

8.1 All employees shall follow the FERPA requirements found at

8.1.1 https://www.nctc.edu/current-students/ferpa.html

8.1.2 https://www.nctc.edu/catalog/academic-policies/student-rights-concerning-educational-records-under-ferpa.html

9. Data Use

9.1 To use any data, the information owner must approve the use of the data under their responsibility.

9.2 The Vice Chancellor of Enrollment Management is the owner of student admissions, advising, and registration data.

9.3 The Provost and VP for Academic Affairs is the owner of faculty data.

9.4 The Vice Chancellor of Fiscal Affairs is the owner of financial data.

9.5 The Vice Chancellor of Administrative Affairs is the owner of employee and student employee data.

9.6 The Vice Chancellor of External Affairs is the owner of alumni and donor data.

9.7 Together, they will be responsible for maintaining the accuracy of their data and approving access requests to the data under their authority.

10. Information Owner Responsibilities

10.1 The information owner or their designated representative(s) are responsible to:

10.1.1 classify information under their authority, with the concurrence of the Chancellor or their designated representative(s), in accordance with organization's established information classification categories;

10.1.2 approve access to information resources and periodically review access lists based on documented risk management decisions;

10.1.3 formally assign custody of information or an information resource;

10.1.4 coordinate data security control requirements with the ISO;

10.1.5 convey data security control requirements to custodians;

10.1.6 provide authority to custodians to implement security controls and procedures;

10.1.7 document, justify, and be accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the ISO; and

10.1.8 participate in risk assessments as provided under Texas Administrative Code § 202.75.

11. Information Custodian Responsibilities

11.1 Custodians of information resources, including third-party entities providing outsourced information resources and/or services to the College, shall:

11.1.1 implement controls required to protect information and information resources required by Texas Department of Information Resources Security Control Standards Catalog based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the organization's information security program;

11.1.2 provide owners with information to evaluate the cost-effectiveness of controls and monitoring;

11.1.3 adhere to monitoring techniques and procedures, approved by the ISO), for detecting, reporting, and investigating incidents;

11.1.4 provide information necessary to provide appropriate information security training to employees; and

11.1.5 ensure information is recoverable in accordance with risk management decisions.

12. User Responsibilities

12.1 The user of an information resource has the responsibility to:

12.1.1 use the resource only for the purpose specified by the organization or information owner;

12.1.2 comply with information security controls and organization policies and procedures to prevent unauthorized or accidental disclosure, modification, or destruction; and

12.1.3 formally acknowledge that they will comply with the security policies and procedures in a method determined by the Chancellor or their designated representative.

12.2 Organization-owned information resources, designated for use by the public, shall be configured to enforce security policies and procedures without requiring user participation or intervention. Users are required to accept a banner or notice prior to using an information resource provided by the organization (see System Use).

13. Data Use Agreement

13.1.1 The organization shall include a data use agreement and updates to that agreement for employees who handle sensitive information, including financial, medical, personnel, or student data. Each employee shall sign the distributed data use agreement and each update to the agreement (Texas Government Code § 2054.135).

13.1.2 Employees agree to comply with the Data Use Agreement electronically during security awareness training.

14. System Use

14.1 Resources may not be used for personal purposes except for incidental use in accordance with this document. The incidental use of organizational resources for personal purposes must not:

14.1.1 result in additional expense to the organization;

14.1.2 impede normal business functions;

14.1.3 be used for non-approved private commercial purposes;

14.1.4 be used for illegal activity;

14.1.5 be used to intentionally access, create, store, or transmit obscene materials;

14.1.6 be used to compete unfairly with private sector entities or private consultants; or

14.1.7 result in embarrassment to the organization.

14.2 Incidental personal use of organization computers (including, but not limited to, the internet and email), telephones, facsimile (fax) machines, and other means of communication must meet the requirements above and must not unduly impede an employee's assigned responsibilities or the normal functioning of an office. The use of organizational telecommunication, email, and internet services for any illegal activity or to intentionally access, create, store, or transmit obscene materials, as defined in Texas Penal Code § 43.21 (other than in the course of academic research), is strictly prohibited, regardless of whether or not it results in an additional charge to the organization.

14.3 No employee shall entrust organization property or resources to any official or employee, or to anyone else, to be used for any reason other than organization purposes. Employees shall not use equipment, property, or resources for their benefit unless it benefits the organization.

14.4 Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with records retention schedules.

14.5 Users must not attempt to access any data or programs contained on systems for which they do not have authorization or explicit consent.

14.6 Family members or other non-employees are not allowed to access information resources.

14.7 Software or hardware purchased with organizational funds may not be installed on non-organization systems or networks without prior authorization from ITS.

14.8 Software or hardware purchased with personal funds may not be installed on organization-owned computers or networks.

14.9 Desktops/Laptops and other information resources must remain powered on to allow patching and updating activities to occur. In the course of normal operations maintenance

14.10 An information resource must be used only for the purpose specified by the organization or information or resource owner.

14.11 Logon Banner

14.11.1 Welcome to the North Central Texas College Network. This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

******* It is a violation of policy to download and/or install software or programs on NCTC-owned computers. *******

15. Credential Use

15.1 Users can view the Password Policy here

15.1.1 https://my.nctc.edu/ICS/Faculty__Staff/Business_Policies.jnz?portlet=Free-form_Content

15.2 Passwords must not be inscribed on sticky notes posted on or under a computer, monitor, or peripheral (i.e., keyboard, mouse, etc.), nor may they be left written down in any accessible location.

15.3 Passwords will expire.

15.4 Computing devices should not be left unattended without enabling a password-protected screensaver or automatic logoff.

15.5 Passwords must be treated as confidential information. Passwords shall not be shared or revealed to anyone.

15.6 Passwords must never be transmitted in plaintext unless the account is used only for accessing publicly accessible data.

15.7 If the security of a password is in doubt, the password should be changed immediately.

15.8 If a password has been compromised, the incident should be reported to ITS at itshelpdesk@nctc.edu.

15.9 Users should not circumvent password entry with automatic logon, application remembering, embedded scripts, or hard-coded passwords in client software for systems that process/store mission-critical and/or confidential data. Exceptions may be made for specific applications (e.g., automated backups) with the approval of the information resource owner.

15.10 Hardware tokens must not be shared or loaned to others. If a hardware token is shared, lost, or stolen, it must be reported to ITS department for deactivation as soon as possible.

15.11 Security access codes, access cards, and/or keys to information resource facilities must not be shared or loaned to others. If a revocable resource, such as a card or access code, is shared, it must be deactivated upon notification.

16. Network Use

16.1 Users are not to connect to or install any equipment, including computers, printers, and network management/control devices to the network infrastructure without prior approval from ITS.

16.2 Users must not plug any unknown devices into any organization computer or network.

16.3 ITS is responsible for the organization's network infrastructure configuration.

16.4 Network management/control devices shall not be connected to network infrastructure without prior consultation with ITS. Network management/control devices include, but are not limited to: routers, gateways, switches, hubs, wireless access, devices or software advertising or serving network services (including BOOTP, DHCP, DNS, IPv6 router, VPN, SMTP, ICS, OSPF or other routing protocols), devices or software transmitting multicast or broadcast traffic at high rates, etc.

16.5 Users are not permitted to install or run devices or software designed or intended to conduct network reconnaissance, vulnerability probing, reveal or exploit weaknesses, or conduct denial of service (DoS) or distributed denial of service (DDoS) attacks.

16.6 Users must not run password cracking programs, packet sniffers, port scanners, or any other unapproved hardware devices or software on information resources.

16.7 VPN implementers which backhaul data from a location to a central site, thus masking its true location, are not allowable on the organization's network. Contact ITS for allowable VPN use.

16.8 Users are permitted to use only those network addresses issued to them by ITS.

16.9 All connected devices are subject to monitoring and management.

16.10 Guest access is provided for conferences and similar meetings. The organizer should contact the ITS Help Desk for details as part of planning the event.

16.11 Users shall not alter or disable organizational network infrastructure devices or equipment.

16.12 All computers connecting to the network must run authorized, current malware protection software that is updated with current signatures and security patches.

16.13 Malware protection software must not be disabled or bypassed except as required for the temporary installation of software or other special circumstances.

16.14 Computers infected with a virus or other malicious code will be disconnected from the network until deemed safe by ITS.

16.15 If a device causes any disruption, malware, vulnerability, or exploit to run on information resources or the network, the device will be disconnected from the network until the problem is resolved.

16.16 Users must not purposely engage in activity that may harass, threaten, or abuse others, degrade the performance of information resources, deprive authorized user access to an organization resource, obtain extra resources beyond those allocated, or circumvent organizational computer security measures.

16.17 Software or hardware purchased with organizational funds may not be installed on non-organization systems or networks without prior authorization from ITS.

17. Media Use

17.1 All removable media that contains confidential data shall be properly destroyed. The user must notify the help desk for secure disposal of media.

17.2 The user must protect the media until it can be disposed.

17.3 Device that contain sensitive data must be disposed of by the ITS department.

18. Software Use

18.1 Software must be used in accordance with license agreements, contract agreements, and applicable copyright laws. Where feasible, such agreements should be maintained in the department that operates the system on which the software is installed. In cases where this is not feasible, individuals or departments should maintain enough documentation [e.g., End User License Agreements (EULA), purchase receipts, terms of service (ToS), etc.] to validate that the software or hardware is appropriately licensed.

18.2 The organization shall provide enough licensed copies of software so employees can fulfill their responsibilities in an expedient and effective manner. Each department may make appropriate arrangements with ITS for additional licensed copies.

18.3 It should be noted that some software licenses allow the user to make a copy for home use in conjunction with the business use of the software. A user of licensed software should not assume

this provision is in place but instead check with the license agreement before making copies for other machines.

18.4 Software not licensed to the organization shall not be installed on organization-owned systems, networks, or computers. ITS will remove such unlicensed software.

18.5 Licensed software may only be copied and used to the extent permitted under the license. Unauthorized copies or illegally distributed copyrighted software are prohibited.

18.6 Users must not use non-standard software without ITS management approval.

18.7 Privately acquired commercial software shall not be installed.

18.8 All software must be evaluated for accessibility by Electronic Information Resources (EIR).

18.9 If software is deemed a security risk or duplicates the functionality of existing, approved software or hardware, the software will not be installed.

18.10 Software purchased with organizational funds may not be installed on non-organization systems or networks without prior authorization from ITS.

18.11 Peer-to-Peer (P2P) software that allows content distribution in which digital files are transferred between "peer" computers and is not permitted.

18.12 Systems may be scanned for unauthorized software.

18.13 Unapproved or unauthorized software will be removed unless proof of authorization from the rightful owner(s) is provided, and it may require a license (or system) transfer.

19. Email Use

19.1 Email is considered an official means of communication, NCTC Student Handbook.

19.2 Users required to conduct official business via email are required to do so with their assigned NCTC email account. Email systems used to conduct the business of the organization require appropriate security, backup, and records retention measures.

19.3 Retention of records shall be in accordance with the NCTC's records retention procedures. Email stored on the email server has a three year retention cycle.

19.4 Requests to substitute non-organization email addresses for purposes of official communication will not be honored. Use of non-approved email exposes that email to Office of General Counsel's Legal collection and open records request per Texas Government Code § 552.004.

19.5 Email is subject to the same policies regarding information disclosure as other methods of communication. The privacy of personally identifiable information (PII) must be protected under the laws and regulations provided by Family Educational Rights and Privacy Act of 1974 (FERPA), Gramm-Leach-Bliley Act (GLBA), and State of Texas. The confidentiality of email cannot be assured, and any confidentiality may be compromised by access consistent with applicable law or policy, including this procedure, by unintended redistribution or due to current technologies inadequate to protect against unauthorized access.

19.6 Sensitive and/or confidential material must not be transmitted via email unless encrypted. Users must exercise extreme caution in using email to communicate confidential or sensitive matters and shall not assume that their email is private or confidential. Examples of confidential and controlled data can be found in the Data Classification Standard.

19.7 Email must be used in a manner that achieves its purpose without exposing any technical, financial, or legal risks.

19.8 The following activities are prohibited:

19.8.1 Using personal email accounts for business purposes without written approval from a supervisor or the Chancellor allowing the use of such an account for a specific and limited purpose. Official emails shall not be forwarded from business email accounts to personal accounts.

19.8.1.1 In the event a personal email account it approved, the password for the account must be provided to the supervisor.

19.8.2 Sending an email that is intimidating or harassing.

19.8.3 Using email for conducting non-approved private commercial purposes.

19.8.4 Using email for purposes of political lobbying or campaigning.

19.8.5 Violating copyright laws by inappropriately distributing protected works.

19.8.6 Unauthorized posing as anyone other than oneself when sending an email.

19.8.7 Using unauthorized email software.

19.8.8 Sending or forwarding chain letters.

19.8.9 Sending unsolicited messages to large groups except as required to conduct College business.

19.8.10 Sending excessively large messages.

19.8.11 Sending or forwarding an email that is likely to contain computer viruses.

19.9 Users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the organization or any department unless appropriately authorized to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing organization. An example of a simple disclaimer is: "The opinions expressed are my own and not necessarily those of my employer."

19.10 Storage of personal email messages, voice messages, files, and documents within organizational information resources is not authorized.

19.11 All users of organization networks and information resources should not subscribe to mailing lists or mail services strictly for personal use and should not participate in electronic discussion groups (i.e., list server, Usenet, IRC, news groups, chat rooms) for personal purposes.

19.12 Any email that constitutes an organizational record must be retained according to the retention policy. This requires information or documents to be filed in an appropriate system that will allow for retention. Individuals are responsible for making this designation by filing the information appropriately.

20. Instant Messaging /Texting

20.1 The content and function of an instant message (IM) or short message service (SMS), i.e., text message, determines whether it is an organization record. Only IMs that meet the criteria for organization records are subject to records retention requirements. An IM is not an organization record unless the message uniquely documents organizational business and is NOT merely a convenience copy or transitory information. Any IM that is an organization record must be retained in an appropriate electronic records management system (not in an IM account), in accordance with the organization's records retention requirements.

20.2 Confidential or sensitive data, including PII, shall never be sent through IM or text message.

20.3 The use of IM services provided by the organization should be limited to the sharing of short-term messages requiring immediate action or confirmation of presence. Information of an enduring nature (in this case, required after 48 hours) should utilize email messaging services or other storage provided by the system.

20.4 Use of non-approved IM (such as personal cell phones) is not permitted for business use. Further it exposes the device to Office of General Counsel's Legal collection and open records request per Texas Government Code § 552.004.

21. Video Conferencing

21.1 Meeting solutions blend communications, collaboration and content sharing to enable informal and formal meetings. These solutions may be part of a larger unified communications package or a standalone web conferencing product.

21.1.1 Limit use of meeting solutions for conducting business to those solutions approved and centrally administered.

21.1.2 Meeting access codes are only reused, such as in cases of recurring meetings, when the meeting is protected by additional screening controls (e.g., waiting room, authenticated users).

21.1.3 Meeting hosts use a roll call or other means of identifying each meeting attendee when beginning the meeting and as additional attendees join.

21.1.4 Meeting hosts do not record the meeting unless necessary and only after informing each attendee that remaining in the meeting constitutes consent to recording.

21.1.5 Meeting hosts or co-hosts monitor attendees to ensure unidentified participants do not enter the meeting.

21.1.6 Meeting hosts retrieve and delete recordings of meetings containing sensitive information from the meeting provider's platform immediately once the recording is made available.

21.1.7 Meeting hosts utilize user authentication or a lobby/pre-conference/waiting room to identify attendees before admitting them to a meeting, and/or lock the meeting room once all scheduled attendees have joined the meeting, to prevent uninvited attendees from joining the meeting.

21.1.8 Meeting access codes (e.g., meeting or room ID) are protected with a passcode, password, or PIN.

21.1.9 Attendees are not permitted to enter the meeting room before the host begins the meeting.

21.1.10 The ability to share screen content is restricted to the meeting host or attendees explicitly permitted by the meeting host.

21.1.11 Lobbies and pre-conference/waiting rooms are enabled by default for all meetings.

21.1.12 When supported, hardened default settings for meetings are locked by the account administrator and cannot be changed by meeting hosts.

22. Internet Use

22.1 All internet activity is logged and may be reviewed for inappropriate use.

22.2 Only officials who are expressly authorized to speak to the media or to the public on behalf of the organization may represent the organization via any electronic communication.

22.3 Supervisors should work with employees to determine the appropriateness of using the internet for professional activities and career development. Written permission is needed and should be obtained for these activities, or the activities should be included in the employee's job description. All users of organizational networks and information resources using the internet shall identify themselves honestly, accurately, and completely (including one's affiliation and function where requested) when providing such information.

22.4 Personal internet use should not impede the conduct of business; only incidental use is allowed. Users are responsible to exercise good judgment regarding the reasonableness of personal use in accordance with all guidelines associated with acceptable use of information resources.

22.5 The Information Security Office monitors for breaches of websites. If the Information Security Office identifies any user account has been compromised, a password reset of the user's local account will be issued. It is recommended for all users to register a different password for every site/login.

22.6 Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.

22.7 Organizational internet access must not be used for personal gain or solicitation.

22.8 All downloaded files shall be scanned by software to safeguard against malicious threats.

22.9 Sensitive or confidential information must not be posted publicly.

22.9.1 All sensitive or confidential information transmitted over external networks (e.g., internet) or shared externally must be encrypted including email, cloud, and third party sharing, contact the helpdesk or ISO for guidance.

22.10 Do not reuse any organization password with any internet or external system unless it has been approved by ITS, CIO, and the ISO.

22.11 Peer to Peer (P2P) software allowing illegal content distribution in which digital files are transferred between "peer" computers is not permitted.

22.12 Anti-virus software will be installed on all devices operated by the user that are connected to the NCTC Internet/Intranet/Extranet, whether owned by the user or by NCTC. The anti-virus software must be continually executing approved virus scanning software.

22.13 All files downloaded from the internet must be scanned for malware using the approved malware/virus detection software.

22.14 Personal internet use should not incur a direct cost in addition to the general overhead of an internet connection; consequently, users are not permitted to print or store personal electronic files or material on the network.

23. NCTC-Owned Portable Computing

23.1 All sensitive or confidential data stored on portable computing devices shall be encrypted. ITS will maintain a list of suitable encryption mechanisms.

23.2 Users must use the approved Virtual Private Network (VPN) connection when remotely connecting to the organization's network.

23.3 Confidential or controlled data shall not be transmitted via a wireless connection to, or from, a portable computing device unless appropriately secure wireless encryption methods, i.e., Transport Layer Security (TLS) or Remote Desktop Protocol (RDP) over VPN, are utilized.

23.4 All remote access (e.g., dial in services, cable/DSL modem, etc.) to confidential information from a portable computing device shall utilize approved encryption techniques, such as Virtual Private Network (VPN), secure File Transfer Protocol (sFTP), or TLS.

23.5 Unattended portable computing or storage devices, containing confidential information, shall be kept physically secure using means commensurate with the associated risk.

23.6 Export control regulation may apply when traveling outside the U.S. Contact the export control officer (ECO) for further information.

24. Bring Your Own Device (BYOD)

24.1 Only NCTC authorized systems are allowed on the production network. No personal devices are permitted on the production network.

24.2 Employees, contractors, and network users must not send, forward, store, or receive confidential information on unencrypted or unsecured mobile devices, such as two-way pagers,

personal digital assistants (PDAs), cell phones, or tablets. Only devices authorized by ITS or the ISO may receive and store confidential information.

24.3 It is not advisable to use a personal device for business use. The practice exposes the personal device to litigation procedures (copying of data) or Public Records Request. The organization is not liable for any damage incurred through an individual's use of a personal device(s) for business purposes. All risk is retained by the user; however, the organization will not be put at risk. Texas Government Code § 552.004

24.4 Two-factor authentication (2FA) verification is not considered business use; therefore, it is acceptable to use 2FA for identity confirmation on a personal device.

24.5 BYOD equipment and personal computers are only allowed on the wireless (guest) network and appropriate authentication is required.

24.6 A current or former officer or employee of a governmental body who maintains public information on a privately owned device shall (Texas Government Code § 552.004):

24.6.1 forward or transfer the public information to the governmental body or a governmental body server to be preserved; or

24.6.2 preserve the public information in its original form in a backup or archive and on the privately owned device.

25. Third-Party Use

25.1 All connection of the network infrastructure to third-party networks requires consultation with ITS prior to the purchase/installation of any software/hardware or associated service.

25.2 Information owners must approve the use of data sharing (e.g., FERPA, Directory Data, PII, HIPAA-PHI, PCI) with a third-party.

25.3 NCTC collects and processes many different types of information from third parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations, e.g., Gramm-Leach-Bliley Act, Texas Administrative Code § 202.

25.4 Third-Parties must adhere to EIR Accessibility standards, Texas Administrative Code § 213.

25.5 In instances where the department is the owner or custodian of the system hosting software or hardware, the department is responsible for ensuring End User License Agreements (EULAs) are appropriately stored and maintained.

25.6 System owners are required to review access and disable and/or remove any user accounts of individuals who are terminated, transferred and no longer need access, or do not use the system.

25.7 System owners and custodians are required to perform, at a minimum, annual account reviews for access.

26. Web Publishing

26.1 The organization's primary website is considered a public site, and all materials published online are considered public. Information on the public website does not require any permission to access.

26.2 No confidential information may be posted on the public website. Hidden links are not an acceptable method of preventing information from being accessible (i.e., security through obscurity). All content on the primary website will be discovered and catalogued by search engines automatically.

26.3 NCTC must publish a privacy notice that describes applicable provisions of its privacy policy on its home page, including all key public entry points or its site policies page, Texas Administrative Code § 206.72.

26.4 Domain names should be purchased through, or with the coordination of, ITS.

26.5 Before deploying an internet website or mobile application that processes confidential information, a vulnerability and penetration test must be reviewed and approved by the information security officer, Texas Government Code § 2054.516.

26.6 Websites must adhere to EIR Accessibility standards, Texas Administrative Code § 213.41.

27. Clean Desk requirements

27.1 Employees are required to ensure that all confidential information in hard copy or electronic form is secured in their work area at the end of the day and when they are expected to be gone for an extended period.

27.2 Computer workstations must be locked when not in use or unattended.

27.3 Computer workstations should be logged off at the end of the workday.

27.4 Any confidential information must be removed from the desk and secured in a drawer or locked office when not in use or unattended.

27.5 File cabinets containing confidential information must be kept closed and locked when not in use or unattended.

27.6 Keys used for access to confidential information must not be left at an unattended desk.

27.7 Passwords shall not be left on sticky notes anywhere, nor may passwords be written down in an accessible location.

27.8 Upon disposal, confidential documents must be shredded in the official shredder bins or placed in the locked, confidential document disposal bins.

27.9 Whiteboards containing confidential information should be erased immediately after use.

27.10 Treat mass storage devices such as CD-ROM, DVD, BD, or USB drives as confidential data, and secure them in a locked drawer.

27.11 All printers and fax machines must be cleared of papers as soon as they are printed. This helps to ensure confidential documents are not left in printer trays for unauthorized persons to pick up or view.

28. Payment Card Acceptance

28.1 The Vice Chancellor of Fiscal Affairs, in coordination with the ITS must approve any acceptance of payment methods by credit or debit card in accordance to organization financial guidelines.

Related Statutes, Policies, Regulations, or Rules

---

29. Federal

29.1 U.S. Department of Education FISMA, NIST SP 800-171 R1

29.2 U.S. Department of Education FERPA

29.3 Gramm-Leach-Bliley Act (15 U.S. Code § 6801)

29.4 Health Insurance Portability and Accountability Act (HIPAA)

29.5 Payment Card Industry (PCI) Data Security Standard (DSS)

30. State of Texas

30.1 Texas Government Code, Chapter 552. Public Information

30.2 Texas Government Code, Chapter 2054. Information Resources

30.3 Texas Administrative Code § 202 Subchapter C, Information Security Standards for Institutions of Higher Education

30.4 DIR Acceptable Use of the Internet

30.5 DIR Security Control Standards Catalog

31. NCTC Policies and Procedures

31.1 Privacy Concerns

31.2 Password Policy

31.3 NCTC Social Media Policy

31.4 FERPA

Contact Office

Information Technology Services (ITS)
Gainesville, 940-668-4284
itshelpdesk@nctc.edu