Information Technology Cyber Security Policy

North Central Kansas Technical College

2017

North Central Kansas Technical College

Subject: **CYBER SECURITY POLICY**

Approved: _____ Effective Date: _____

1 DEFINITION

The use of the term "NCK Tech" is representative to the following organization: North Central Kansas Technical College.

2 INTRODUCTION

This Cyber Security Policy is a formal set of rules by which those people who are given access to company technology and information assets must abide.

The Cyber Security Policy serves several purposes. The main purpose is to inform company users: employees, students, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of NCK Tech. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

The Cyber Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of NCK Tech computer systems and networks and best practices.

3 WHAT ARE WE PROTECTING

It is the obligation of all users of NCK Tech computer systems and networks to protect the technology and information assets of NCK Tech. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of NCK Tech are made up of the following components:

- Computer hardware, CPU, storage media, Email, web and application servers, PC systems, application software, system software, etc.
- System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments within NCK Tech. This includes custom written software applications, and commercial off the shelf software packages.
- Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, servers, switches, firewalls, on private and public networks, as well as associated network management software and tools.

3.1 Classification of Information

User information found in computer system files and databases shall be classified as either confidential or non-confidential. NCK Tech shall classify the information controlled by them. The Information Technology department is required to review and approve the classification of the information and determine the appropriate level of security to best protect it. Furthermore, the Information Technology department shall classify information controlled by units not administered by an employee.

3.2 Classification of Computer Systems

Security Level	Description	Example
RED	This system contains confidential information – information that cannot be revealed to personnel outside of NCK Tech. Even within NCK Tech, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life threatening consequences and/or an adverse financial impact on the business of NCK Tech.	Servers containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information.
GREEN	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access Server and application(s). Management workstations used by systems and network administrators.
WHITE	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	Student use systems
BLUE	This system is not externally accessible. It is on an isolated LAN segment, able to access RED systems. It may contain sensitive information or perform critical services.	Faculty / staff systems, Intranet.
BLACK	This system is externally accessible. It is isolated from RED, WHITE, BLUE or GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public Web server with non-sensitive information.

3.3 Local Area Network (LAN) Classifications

A LAN will be classified by the systems directly connected to it. For example, if a LAN contains just one RED system then all network users will be subject to the same restrictions as RED or GREEN systems users' contingent upon their authorization to the RED system. A LAN will assume the Security Classification of the highest level systems attached to it.

4 DEFINITIONS

Externally accessible to public. The system may be accessed via the Internet by persons outside of NCK Tech without a logon id or password. The system may be accessed via dial-up connection without providing a logon id or password. It is possible to "ping" the system from the Internet. The system may or may not be behind a firewall. A public Web Server is an example of this type of system.

Non-Public, Externally accessible. Users of the system must have a valid logon id and password or have an approved IP to access the system. The system must have at least one level of firewall protection between its network and the Internet. The system may be accessed via the Internet or the private Intranet. A private Intranet web server is an example of this type of system.

Internally accessible only. Users of the system must have a valid logon id and password. The system must have at least two levels of firewall protection between its network and the Internet. The system is not visible to Internet users. It may have a private Internet (non-translated) address and it does not respond to a "ping" from the Internet. A private intranet Web Server is an example of this type of system.

Chief Information Officer / IT Security Administrator. The Director of the Department of Information Technology (IT) shall serve as the Chief Information Officer and an IT department employee shall be designated as the IT Security Administrator for NCK Tech.

5 Threats to Security

5.1 Employees

One of the biggest security threats are employees. They may do damage to systems either through incompetence or on purpose. Multiple layers of security will be utilized to reduce any possible employee threats. This will be accomplished by the following.

- ✓ Only give out appropriate rights to systems. Limit access to only business hours when possible.
- ✓ Don't share accounts to access systems when possible. Never share personal login information with co-workers.
- ✓ When employees resign, retire or are disciplined, access to systems will be limited or removed.
- ✓ Physically secure computer assets behind locked doors or cabinets, so that only staff with appropriate needs can have access.

5.2 Amateur Hackers and Vandals.

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

5.3 Criminal Hackers and Saboteurs.

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

6 User Responsibilities

This section establishes usage policy for the computer systems, networks and information resources of the office. It pertains to all employees, students and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the networks for the business purposes of NCK Tech.

6.1 Acceptable Use

All users must review and agree to NCK Tech's Information Systems Use Policy. User accounts on company computer systems are to be used only for business of NCK Tech and are not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of NCK Tech computing system and facilities may constitute grounds for either civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords and the backup of their data files to a secure or offline location. Furthermore they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of NCK Tech.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.

Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from NCK Tech's IT department.
Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Users are required to report any weaknesses in NCK Tech computer security, any incidents of misuse or violation of this policy to NCK Tech's IT department.

6.2 Use of the Internet

The use of the Internet and local area network by employees, students and guests of North Central Kansas Technical College is permitted and encouraged where such use supports the business and educational goals, objectives and policies of the North Central Kansas Technical College. Failure to comply may result in the interruption or termination of Information Systems use privileges and/or legal action without prior notification.

NCK Tech will provide Internet access to employees, students and contractors who are connected to the internal network ***and*** who have a business need for this access. Employees, students and contractors must first review, agree and sign NCK Tech's Information Systems Use Policy prior to access. This signed policy will be kept on file in the IT department.

The Internet is a business tool for NCK Tech. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information, educational resources and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for "chain letters" or any other purpose which is illegal or for personal gain.

6.3 Monitoring Use of Computer Systems

NCK Tech has the right and capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including e-mail messages and usage of the Internet. It is not NCK Tech policy or intent to continuously monitor all computer usage by employees or other users of NCK Tech computer systems and network. However, users of the systems should be aware that NCK Tech may monitor usage without notice, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with company policy.

6.4 User Classification

All users are expected to have knowledge of these security policies and are required to report violations to the IT department. Furthermore, all users must conform to the Acceptable Use Policy defined in this document. NCK Tech has established the following user groups and defined the access privileges and responsibilities:

User Category	Privileges & Responsibilities
Department Users (Employees)	Access to application and databases as required for job function. (RED and/or GREEN cleared)
System Administrators	Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only.
IT Security Administrator/IT Department staff	Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
Systems Analyst/Programmer	Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices.
Contractors/Consultants	Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to company information and systems must be approved in writing by NCK Tech director/CEO.
Current NCK Tech Students	Access allowed to selected (White clearance) computer systems and applications. Access to NCK Tech's public Wi-Fi network.
Other Agencies and Business Partners	Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws.
General Public	Access is limited to applications running on public Web servers. Access to NCK Tech's public Wi-Fi network. The general public will not be allowed to access any internal or confidential information.

7 Access Control

A fundamental component of our Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

7.1 User System and Network Access – Normal User Identification

All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management or supervisory personnel and/or any other employees whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer systems or otherwise be readily accessible in the area of the computer systems.
- Passwords should be changed at minimum twice a year.
- User accounts will be suspended after 3 to 5 failed logon attempts for a minimum of 5 minutes.
- Logon IDs and passwords will be suspended without use or after termination of employment.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, suspended, placed on leave, or otherwise leaves the employment of NCK Tech.

Supervisors / Managers shall immediately and directly contact NCK Tech IT Manager to report change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must call the IT department to have it reset or a new password assigned to their account. The employee must identify himself/herself by name and their department to the IT department.

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's ID and password. Employees shall not logon to a computer with their personal account ID and password and then allow another individual to use the computer.

7.2 System Administrator Access

System Administrators, network administrators, and security administrators will have full access to host systems, routers, hubs, and firewalls as required to fulfill the duties of their job.

All system administrator passwords will be changed after any employee who has access to such passwords is terminated, or otherwise leaves the employment of NCK Tech.

7.3 Special Access

Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by NCK Tech and require the permission of the college's IT department. Monitoring of the special access accounts is done by the college's IT department.

7.4 Connecting to Third-Party Networks

This policy is established to ensure a secure method of connectivity provided between NCK Tech and all third-part companies and other entities required to electronically exchange information with company.

"Third-party" refers to vendors, consultants and business partners doing business with NCK Tech, and other partners that have a need to exchange information with NCK Tech. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of NCK Tech. The third-party company will ensure that only authorized users will be allowed to access information on NCK Tech network. The third-party will not allow Internet traffic or other private network traffic to flow into the network. A third-party network connection is defined as one of the following connectivity options:

- A network connection will terminate on completion and the third-party will be subject to standard company authentication rules.

This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

All requests for third-party connections must be made by submitting a written request and be approved by the companies IT department.

7.5 Connecting Devices to the Network

Only authorized devices may be connected to NCK Tech private network(s). Authorized devices include PCs and workstations owned by NCK Tech that comply with the configuration guidelines of NCK Tech. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the private network(s) with any computers not controlled or managed by NCK Tech IT. Users are specifically prohibited from attaching personal devices to NCK Tech's private network. All non-company, personal computers or devices are ONLY permitted to connect to NCK Tech's public "CAMPUS" network.

NOTE: Users are not permitted to attach any device that would alter the topology characteristics of the Network or add any unauthorized access points, routers, switches or other network devices.

7.6 Remote Access

Only authorized employees may remotely access NCK Tech's networks. Remote access is provided to those employees, contractors and business partners of NCK Tech that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to company network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

7.7 Unauthorized Remote Access

The attachment of networking equipment, repeaters, etc. to a user's PC or workstation that is connected to NCK Tech LAN is not allowed, NCK Tech's IT staff are the only users allowed to alter NCK Tech's networks. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

8 Security Incident Handling Procedures

This section provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of NCK Tech network. Some examples of security incidents are:

- Illegal access of an NCK Tech computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to an NCK Tech computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against an NCK Tech web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computer outside of NCK Tech network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.
    - These security incidents will be reported to the college's IT department for further investigation and may be reported to the college's President for possible disciplinary actions.

- Ransomware, malware, spyware, Trojan or virus infections that compromise NCK Techs networks or connected systems.
    - Compromised system(s) will be removed from NCK Techs network and repaired if possible or securely erased by NCK Techs IT department. If the compromised system is securely erased and re-loaded, all attempts to restore an employee's personal data files from backups will be taken. However, since it is the individual employee's responsibility to make regular backups of their personal data files to a safe, secure and if possible offline storage source, their data files will then be restored to the newly loaded system if available. If the employee has neglected to make regular backups of their data, no data will be restored.

Any employees, who believe their computer system(s) may have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the NCK Tech's IT department immediately. The employee shall not turn off the affected computer or delete suspicious files. The employee will promptly disconnect the computer from the college's network and then leave the computer in the condition it was in when the security incident was discovered which will assist in identifying the source of the problem and in determining the steps that should be taken by the IT department to remedy the problem.

9 Penalty for Security Violation

NCK Tech takes the issue of security seriously. Those people who use the technology and information resources of NCK Tech must be aware that they can be disciplined if they violate this policy. **Upon violation of this policy, an employee of NCK Tech may be subject to discipline up to and including discharge and/or possible legal action.** The specific discipline imposed will be determined by the college's President on a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information.
Discipline which may be taken against an employee shall be administrated in accordance with any appropriate rules or policies of NCK Tech's Information Systems Use Policy.

In a case where the accused person is not an employee of NCK Tech (student or visitor) the matter shall be submitted to the college's President. The college's President may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

10 Best Practices for NCK Tech

10.1 Train employees in security principles

Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect college information. All policies, trainings and practices are posted on our Intranet.

10.2 Protect information, computers, and networks from cyber attacks

Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scans to run automatically. Install other key software updates as soon as they are available.

10.3 Provide firewall security for your Internet connection

A firewall is a set of related hardware and software programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled. If employees work from home, ensure that their home system(s) are protected by a firewall.

10.4 Create a mobile device action plan

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password-protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Employees are required to report any lost or stolen equipment.

10.5 Make backup copies of important business data and information

Regularly backup the data on computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, PowerPoint presentations, and accounts receivable/payable files. Users should backup data automatically if possible, or at least weekly and store the copies either offsite or on a portable hard drive.

10.6 Control physical access to your computers and create user accounts for each employee

Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so employees should lock them up when unattended. A user account is created for each employee and strong passwords are required. Administrative privileges should only be given to trusted IT staff and key personnel only.

10.7 Secure networks

All networks, wired and wireless are to be managed by NCK Tech's IT staff and the Wireless keys should be changed regularly.

10.8 Employ best practices on payment cards

Limit employee's online college purchases to authorized personnel only.

10.9 Limit employee access to data and information, limit authority to install software

Employees are given access to the specific data systems that they need for their jobs, and students should not be able to install any software on college computers.

10.10 Passwords and authentication

Employees are required to use unique and strong passwords that require changing a minimum of every 180 days.