COLUMBUS STATE

COMMUNITY COLLEGE

Information Security Program

Information Security Committee Approved Version: 20091021
This version: 20120104

This Standard falls under Columbus State Community College Information Technology Policy 15-01.

1 Purpose

The purpose of the Information Security Program is to develop and maintain standards and guidelines for the protection of information in compliance with all applicable laws and regulations.

2 Scope

This standard applies to all CSCC owned devices to include all college departments and labs as stated in CSCC's Information Technology policy 15-01.

3 Document Owner

This document is owned by the Information Security Committee. All considerations for altering this document must first be reviewed by the Information Security Committee and follow the review cycle as stated in section 3.0. The task of Information Security is assigned to the Chief Security Officer or other security- knowledgeable member of management.

4 Information Security Standard Document Review Cycle

This document will be reviewed by Network Systems bi-annually or as needed. Any proposed amendments must be presented to the Information Security Committee and approved before proposed amendments are considered applicable and enforceable.

5 Revision History

Date	Change	Made By
2/6/09	Added content to sections 1-6, 10; reformatted document's outline	R. Clifford
2/10/09	Added 8.6, changed references from Network Services to Network Systems	J. Gaines
2/11/09	Modified 19.4, Created 20. ,moved 9.14 to under 20.1,added 20.2,need to add index for 20.	J. Gaines
2/12/09	Added 9.8, 9.9	J. Gaines
3/18/09	Changed document owner to the Information Security Committee	R. Clifford
5/14/09	Added section 19 "Passwords"	R. Clifford
5/20/09	v1.9 approved by the Information Security Committee; changed on cover page	R. Clifford
6/22/09	Added "centralization" text in section 10.1	R. Clifford
7/22/09	Changed document title, "Purpose" statement	R. Clifford
9/18/09	Added section 9.17	R. Clifford
1/4/12	Added content under section 11 "Patch Management"	R. Clifford
10/06/16	Added Section 22 "Payment Card Data"	D. Rellick
10/06/16	Added section 16.4	D. Rellick
12/08/16	Added comment to 3.0 Document Owner	D. Rellick

6 Key Terminology & Acronyms

This section will outline any key terminology and acronyms used throughout this document.

- CSCC: Columbus State Community College
- End user: Considered to be staff and faculty, not students

7 Network Interior & Perimeter Security

7.1 Firewall technology shall be employed at the interior and perimeter of Columbus State networks to protect sensitive internal assets and infrastructure from unauthorized access.

7.2 Network traffic filtering rules for traffic that traverses the Internet shall include the following:

7.2.1 An incoming packet shall ***not*** contain Internet Control Message Protocol (ICMP) traffic.

7.2.2 An incoming packet shall have a publicly registered destination address associated with the internal network if using static or dynamic Network Address Translation (NAT).

7.2.3 Sources of traffic from Internet sites that are known to contain malicious content (such as spam, viruses, spyware, etc.), may be blocked at the discretion of CSCC, per policy 15-01.

7.3 Internal and perimeter firewalls shall have audit logging turned on. Logs should be accessible for "live" searches for 3 months. Offline storage should be stored off-site for one year. All incidents, violations, etc. shall be reported to the Information Security Committee for review.

7.4 Firewall policies should be reviewed, tested, and audited bi-annually by Information Technologies authorized personnel.

7.5 Remote management of firewall technologies should be via encrypted communications. Outside interfaces must deny firewall management traffic. Access lists must be put in place to deny management traffic from unapproved VLAN's.

7.6 Unneeded services shall be turned off and unused ports disabled.

7.7 All outbound traffic coming from Internal Server VLAN's and or DMZ segments must be blocked unless specified by access control lists.

7.8 Any firewall configuration change(s) must be saved and a backup performed for off-site storage.

7.9 All firewall access control configuration requests must be submitted 24 hours prior to the change. If circumstances require for an immediate change, authorization is required by the Director of Communication Technologies + PC Services.

8 End Point Security

8.1 Client devices, including CSCC owned assets, client devices used by remote workers, as well as consulting entities, connected to the internal or DMZ network should be protected from sending or receiving hostile threats from unauthorized network traffic or software applications.

8.2 CSCC owned client devices shall utilize virus-scanning software and be at the latest operating system updates/patches.

8.3 CSCC owned client devices and any third party entities externally connecting to CSCC networks for management purposes shall encrypt all traffic.

8.4 CSCC client firewalls shall be deployed on all systems by Columbus State and should be centrally managed.

8.5 All end point devices connecting to CSCC campus networks (LAN, WAN, or wireless) shall have network admission control (NAC) technology deployed, when supported.

8.6 All CSCC owned client devices connecting to campus networks shall have the approved version of the Network Systems directory client installed as the primary authentication client and shall be uniquely authenticated to the campus user directory.

9 Internetworking Devices & Server Platforms

9.1 Internetworking devices (including routers, firewalls, switches, controllers etc.) and shared platforms (including workstations, servers, etc.) provide both access to and information about networks. They shall be controlled by Information Technologies to prevent unauthorized access to sensitive data/technologies.

9.2 Access to Internetworking devices and shared platforms shall be restricted to authorized employees and consultants.

9.3 For deploying network systems and servers on CSCC networks, a systems development lifecycle approach must be followed to ensure IT standards are adhered to and proper change control procedures are met.

9.4 Access to network management tools such as Simple Network Management Protocol (SNMP), Secure Socket Shell (SSH), and Remote Monitoring (RMON), etc., shall be controlled. Telnet shall not be used to manage Columbus State devices.

9.5 Internetworking devices connected to the network shall have an access control list implemented to deny telnet.

9.6 If dial-in access is required to access network resources, RADIUS, LDAP or Terminal Access Controller Access-Control System Plus (TACACS+) should be used.

9.7 Internetworking devices and server platforms shall have unneeded services turned off, unused ports disabled, and logging capability turned on. Logs should be reviewed, on a frequency determined by Information Technology; authorized personnel shall review all incidents, violations, etc., and report the activity to the Security Committee. All Activity logs shall be logged to a Security Information and Event Management (SIEM) centralized database. Window server logs shall include the Security Log and System Logs, alerts shall be generated when these logs are cleared.

9.8 Internetworking devices and server platforms that support NTP (network time protocol) shall reference their clocks to the CSCC stratum 1 time server at time.cscc.edu.

9.9 All server platforms shall be built and configured in accordance with the Network Systems Server Build Standard document.

9.10 Internetworking device default passwords shall be immediately changed before or upon device installation and current passwords shall conform to requirements set forth by the password standard.

9.11 Internetworking devices shall be configured to retain their current configuration, security settings, passwords, etc., during a reset or reboot process.

9.12 When disposing of internetworking devices that are no longer used all data and configuration information shall be cleared to prevent disclosure of network configurations, keys, passwords, etc.

9.13 Internetworking configurations shall be backed up and stored in a secure environment.

9.14 Audit scanning shall be performed on a quarterly basis by Information Technologies.

9.15 Internetworking devices and servers should be physically secured in an access-controlled environment.

9.16 Internetworking devices and servers are prohibited from operating from uncontrolled cubicle or office areas.

9.17 Network devices such as Routers/Gateways, Firewall's, IPS's and Switches that specifically provide access to Layer 1 - 4 services of the OSI model must be administered by Network Systems. All IOS/NXOS configuration changes or device control plane settings must follow a strict change control process before production deployment, and must be reviewed by the Supervisor of Network Systems for change approval. In cases where technologies such as VoIP or other virtual applications are providing additional layers of service on these devices, Network Systems can give access via protocols such as MGCP to allow changes in the specific environment. Read only or show access can also be given by Access Control levels or SNMP protocols to grant approved user(s) or application(s) access.

10 Antivirus

10.1 All CSCC owned computers and servers must have CSCC 's approved antivirus software installed, pointing to the central AV infrastructure, and configured in accordance with CSCC Information Security standards. Any activities with the intent to create and/or distribute malicious code (viruses, worms, Trojans, etc.) into CSCC 's network are prohibited in accordance with CSCC's Information Technology Policy 15-01.

10.2 Clients

10.2.1 Client devices will receive virus definitions daily

10.2.2 It is the responsibility of the end user to verify their machine is receiving updated virus definitions. If they are not, the client is required to call the help desk to resolve possible communication issues between the client and AV parent server.

10.2.3 Scheduled scans are not required nor scheduled on client devices. The AV client is set to scan files when accessed or modified.

10.3 Servers

10.3.1 Servers will receive virus definitions daily

10.3.2 Server administrators are responsible for ensuring their servers are receiving updated virus definitions. If not, the server administrator is responsible for ensuring their servers receive daily virus definition updates.

10.3.3 Servers are required to perform a weekly scheduled scan as determined by Network Systems and/or the owning department. Additionally, servers are configured to scan all files when accessed or modified.

10.4 Certain file extensions may be exempt from accessed or modified scans as it may impact performance. If this is the case, Network Systems and Information Security must review such an exemption request to determine security risks and whether to allow/disallow a scanning exemption.

11 Patch Management

11.1 Patch management shall include servers and clients

11.2 Designated employees shall proactively monitor and address vulnerabilities of all internetworking devices in the network (routers, firewalls, switches, servers, operating systems, applications, etc.) by ensuring that applicable patches are acquired, tested, and installed in a timely manner.

11.3 Where practical and feasible, Information Technologies shall test patches in a test environment prior to installing the patch.

11.3.1 While testing the patches, the subject matter expert will submit a change control request listing the patches that will be deployed to the campus. Information Technology will review the proposed change request during the Change Management meeting on the third Tuesday of each month.

11.4 Patches shall be installed on all affected internetworking devices or servers

11.4.1 Once the change request has been reviewed and approved, the patches will be released to campus on the fourth Wednesday of each month.

11.4.2 Any patches that need to be deployed to the campus outside of this schedule will be submitted under a separate change request.

11.4.3 Designated employees shall monitor the status of patches once they are deployed.

11.5 All CSCC owned client devices shall receive the latest patches via a local Windows Server Update Services (WSUS) server.

12 Demilitarized Zones (DMZ)

12.1 Services provided through the Internet (Web-enabled applications, FTP, Mail, DNS, etc.) shall be deployed on a Demilitarized Zone (DMZ).

12.2 All communication from servers on the DMZ to internal applications and services shall be controlled by an access control list in the firewall. Specific source and destination addresses and ports shall be used.

12.3 Dial-in access to networks shall be authenticated against an authentication mechanism that is encrypted, and terminations are to be in an isolated DMZ separate from primary servers and applications.

13 External Connection to Networks

13.1 External connections to networks shall be routed through secure gateways such as a virtual private network (VPN) or encrypted terminal service.

14 Wireless Network Access

14.1 Columbus State shall have centralized user authentication in accordance with encryption technologies. All wireless connectivity shall be authenticated and endpoint security posture must be assessed with Network Admission Control (NAC) systems.

14.2 The Wired Equivalent Privacy (WEP) algorithm, which is part of the 802.11 standard, is susceptible to compromise; therefore, WEP is prohibited. All access to Columbus State Administrative systems via wireless shall be encrypted with WPA or WPA2 when supported. Staff, Faculty, and Administrators accessing sensitive data shall use the encrypted "CSCC-SECURE" non-broadcasted service set identifier (SSID). Only authorized personnel shall know the key to Columbus State secure Wi-Fi networks. Under no circumstances shall the key be given out to unauthorized individuals.

14.3 WLAN access point device security:

14.3.1 All wireless access points shall be inventoried, approved and deployed by Information Technologies. It is prohibited to install any access point on Columbus State networks without first getting approval by Information Technologies.

14.3.1.1 To increase network security, a wireless location solution shall be deployed to detect unauthorized wireless devices connecting to the CSCC network.

14.3.2 The SSID shall be changed from the factory default setting.

14.3.3 The broadcast SSID feature should be disabled on Columbus State secure administrative networks.

14.3.4 Management access passwords must be changed from their default and default cryptographic keys shall be changed from the factory default setting.

14.3.5 Access point devices shall operate with a central controller.

14.4 CSCC client platforms connecting to Columbus State networks using public access points and the Internet shall use encryption technologies and should use centrally managed individual firewall software solutions.

14.5 Passwords for wireless devices shall conform to requirements set forth by the password standards.

14.6 Technologies shall be implemented at wireless application gateways and connection points between wireless and wire-based LANs to reduce unauthorized access to internal administrative networks.

14.7 To increase network security, a wireless location solution shall be deployed to detect unauthorized wireless devices connecting to the CSCC network.

15 Intrusion Detection & Prevention

15.1 Internal and perimeter facing intrusion detection (IDS) mechanisms or intrusion prevention systems (IPS) should be incorporated into the network.

15.2 Systems shall be deployed that prevents access to internet hosts or web-sites that are known to contain malicious content.

15.3 IDS or IPS shall be installed for ingress and egress traffic external and internal to firewall technologies protecting the network. Logs should be reviewed by authorized Information Technologies personnel and pertinent incidents, violations, etc., reported to the security committee.

16 Vulnerability Scanning

16.1 Network and host vulnerability scanners should be used to test for the vulnerabilities of internal systems and of network perimeter defenses. Scans should occur at a minimum of every quarter on production systems.

16.2 All servers shall undergo a vulnerability scan prior to deployment in a production environment. Scanners should have the ability to do the following:

16.2.1 Map the network or inventory systems and services on the network,

16.2.2 Identify security holes by confirming vulnerabilities in web applications, databases, and network infrastructure devices.

16.2.3 Provide comprehensive reports and charts for effective decision making and improved security,

16.2.4 Define and enforce valid security policies when used during security device installation and certification,

16.2.5 Provide a detailed remediation plan for vulnerabilities.

16.3 All quarterly scan summary results shall be reviewed by the IT Directors.

16.4 Configuration standards are updated as new vulnerability issues are identified.

17 Destruction of Networking & Server Documentation

17.1 Destruction of hardcopy and electronic documentation of network/server device configurations, network diagrams, etc., shall be destroyed, when superseded, or no longer needed. Such destruction may be completed on-site by the use of a document shredder.

18 Backups & Storage

18.1 Meeting the following requirements ensures that CSCC will be able to recover from interruptions in services in a timely manner, and to restore critical information and services.

18.2 Backups shall be taken periodically using a defined cycle, as determined by IT or the owner of the data, frequently enough to meet the time-criticality of business processes, business continuity plans as well as legal, regulatory, and contractual obligations. The frequency and depth of backups shall be based on defined business requirements of IT or the college department(s).

18.3 Backup media types (disks, RAID storage, tape, etc.) shall be selected based on the business requirements, including business continuity planning for critical services, and regulatory obligations relative to permanence of data/information.

18.4 IT shall use automated back-up management software to perform the backups on designated systems.

18.5 Storage of removable media

18.5.1 Backups of mission-critical data shall be stored in a secured, offsite location.

18.5.2 Access to backups of mission critical data shall be limited to IT personnel authorized to handle sensitive data.

18.5.3 Backups shall be clearly and consistently labeled to facilitate restoration and testing and to guard against mishandling, loss, or accidental overwriting.

18.5.4 Media shall be stored in compliance with manufacturer's storage requirements.

18.5.5 Backups shall be transported to designated storage locations by personnel authorized by IT or by an authorized vendor.

18.6 Backups shall include all supported operating system software, application software, related software, utilities, etc., necessary to configure and restore critical information and services.

18.7 Proper documentation (event logs) shall be established within IT for performing backups, transporting media, and testing backup media.

18.8 Backups shall be tested on a regular basis, determined by IT, for restorability of operating systems and recoverability of data.

19 Data Encryption & Securing Sensitive Data

19.1 "Sensitive Data" means any electronic information that CSCC collects and maintains but must keep confidential as required by law. It also includes "personal information," which consists of an individual's last name along with the first name or first initial, in combination with any one or more of the following data elements: social security number; driver's license number; state identification card number; financial account number; or credit or debit card number.

19.2 CSCC shall secure sensitive data in transmission. Whenever data travels over the Internet or other untrusted channels, as a minimum, the measures used to secure sensitive data in transmission shall include encryption. In particular, following forms of transmission over untrusted channels shall be encrypted:

19.2.1 E-mail

19.2.2 Pages on CSCC controlled web sites that enable users to send or receive sensitive data

19.2.3 Instant messaging

19.2.4 Remote printing

19.2.5 Data transfers

19.2.6 Telnet and ftp shall use the secure equivalent protocols such as SSH and SFTP

19.2.7 Any wireless transmission

19.3 CSCC can check transmissions of data in motion for activities that risk unauthorized access to or disclosure of sensitive information. There are different means of checking for these types of activities and they include increased activity logging, audits, and the use of content monitoring analysis tools, and etc.

19.4 Do not store on or copy sensitive data to local, mobile, external storage devices such as CD, DVD, floppy disks, laptops, desktops, USB memory keys, PDAs, cell phones, or any other device that can easily be stolen or compromised.

19.5 CSCC shall secure sensitive data at rest. If implementing encryption is either cost prohibitive or technically infeasible, sensitive data shall be protected through sufficient compensating controls such as operating system configurations, access restrictions, or audit devices.

20 Passwords

20.1 Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Columbus State Community College's (CSCC) entire corporate network. As such, all CSCC employees (including contractors and vendors with access to CSCC systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

20.2 The scope of this standard includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Columbus State Community College facility, has access to the CSCC network, or stores any non-public CSCC information.

20.3 General

20.3.1 All passwords must be changed at least every 90 days.

20.3.2 User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

20.3.3 Passwords must not be inserted into email messages or other forms of electronic communication.

20.3.4 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.

20.3.5 All passwords must conform to the requirements and guidelines described below.

20.4 Requirements and Guidelines

20.4.1 Password Protection Requirements

20.4.1.1 Password must contain both upper and lower case characters (e.g., a-z, A-Z).

20.4.1.2 Passwords must have a minimum of eight alphanumeric characters (ex. Z9Rxw32x).

20.4.1.3 Do not use the same password for CSCC accounts as for other non-CSCC access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various CSCC access needs. For example, Network Administrators should select one password for general network access accounts and a separate password for core IT server systems.

20.4.1.4 Do not share CSCC passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential CSCC information.

20.4.1.5 If someone demands a password, refer them to this document or have them call the helpdesk at (614) 287-5050.

20.4.1.6 Do not use the "Remember Password" feature of applications (e.g., OutLook, IE).

20.4.1.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

20.4.1.8 Change passwords at least once every 90 days.

20.4.1.9 If an account or password is suspected to have been compromised, report the incident to the helpdesk and change all passwords.

20.4.1.10 Password cracking or guessing may be performed on a periodic or random basis by Information Technologies or its delegates. If a password is obtained during one of these scans, the user will be required to change it.

20.4.1.11 Do not use the same password twice.

20.4.2 General Password Construction Guidelines

20.4.2.1 Passwords are used for various purposes at CSCC. Some of the more common uses include: system accounts, user level accounts, web accounts, email accounts, screen saver protection, and local router/switch logins. Since few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

20.4.2.2 Poor, weak passwords have the following characteristics

20.4.2.2.1 The password contains less than eight characters.

20.4.2.2.2 The password is a word found in a dictionary (English or foreign).

20.4.2.2.3 The password is or contains a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.

20.4.2.2.4 Computer terms and names, commands, sites, companies, hardware, software.

20.4.2.2.5 The words "Columbus State", “CSCC”, "Ohio", "Columbus" or any derivation.

20.4.2.2.6 Birthdays and other personal information such as addresses and phone numbers.

20.4.2.2.7 Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

20.4.2.2.8 Any of the above spelled backwards.

20.4.2.2.9 Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

20.4.2.3 Strong passwords have the following characteristics

20.4.2.3.1 Are not words in any language, slang, dialect, jargon, etc.

20.4.2.3.2 Are not based on personal information, names of family, etc.

20.4.2.3.3 Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R3" or "Tmb1Wtr5" or some other variation.

20.4.2.4 Maintain password confidentiality by adhering to the following:

20.4.2.4.1 Do not reveal a password over the phone to ANYONE.

20.4.2.4.2 Do not reveal a password in an email message.

20.4.2.4.3 Do not reveal a password to the manager.

20.4.2.4.4 Do not talk about a password in front of others.

20.4.2.4.5 Do not hint at the format of a password (e.g., "my family name").

20.4.2.4.6 Do not reveal a password on questionnaires or security forms.

20.4.2.4.7 Do not share a password with family members.

20.4.2.4.8 Do not reveal a password to co-workers while on vacation.

20.4.3 Application Development Standards

20.4.3.1 Application developers must ensure their programs contain the following security precautions

20.4.3.1.1 Should support authentication of individual users, not groups.

20.4.3.1.2 Should not store passwords in clear text or in any easily reversible form.

20.4.3.1.3 Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

20.4.3.1.4 Should support TACACS+ , RADIUS and/or with LDAP security retrieval, wherever possible.

20.5 Enforcement

20.5.1 Enforcement is governed by Information Technology Policy No. 15-01.

21 Physical Infrastructure

21.1 Access to Information Technology infrastructure, such as communication vaults, handholes, aerial routes, wiring closets etc. shall be controlled and access approved by Communication Technologies & PC Services.

21.2 IT copper and fiber infrastructures must be designed, installed, and maintained by the supervision of Communication Technologies & PC Services and adhere to documented Network Systems cabling standards for business continuity and risk purposes.

22 Payment Card Data

22.1 Unprotected Primary Account Numbers (PANs) are not to be sent via end-user messaging technologies under any circumstances.

22.2 Card Holder Data, such as PANs / Card Authentication & Verification Values, etc... are not to be documented and/or stored within the Columbus State Community College(CSCC) environment.

22.3 Personnel interacting with Credit Card information are required to adhere to the Payment Card Industry Data Security Standards (PCI DSS).

22.4 Personnel are required to complete CSCC Credit Card training on an annual basis.

22.5 Multi-factor authentication is required for all remote network access into the PCI networks (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.

22.6 Card Holder data must be encrypted before transmitted.