

**COMMUNITY COLLEGES OF
SPOKANE**

**INFORMATION TECHNOLOGY
SECURITY PROGRAM**

In Compliance with the
Information Services Board
Information Technology Security Policy and Standards

Prepared and Reviewed by the Information Systems
Department and Technology Support Staff of CCS

November 14, 2003

TABLE OF CONTENTS

<u>I. A. SECURITY PROGRAM</u>	
<u>INTRODUCTION</u>	8
<u>SCOPE</u>	8
<u>OVERVIEW</u>	8
<u>APPENDIX A -- CHANGE LOG</u>	9
<u>I.B. IT SECURITY POLICY</u>	
<u>1.70.08 CCS INFORMATION TECHNOLOGY – SECURITY POLICY</u>	10
<u>PURPOSE</u>	10
<u>SCOPE</u>	10
<u>POLICY</u>	10
<u>1.71.02 INFORMATION TECHNOLOGY</u>	11
<u>I.C BUSINESS IMPACT AND RISK ANALYSIS</u>	
<u>INTRODUCTION</u>	14
<u>SCOPE</u>	14
<u>BUSINESS IMPACT AND RISK, THREAT AND VULNERABILITY ANALYSIS</u>	14
<u>A. Business Impact Analysis:</u>	14
<u>IS Department Services</u>	14
<u>IS Department Application Systems (includes Support Documentation</u>	15
<u>IS Department Assets</u>	15
<u>B. Risk Threat and Vulnerability Analysis:</u>	16
<u>1. Identify Risks:</u>	16
<u>2. Probability of Occurrence:</u>	16
<u>Natural Hazards</u>	16
<u>Accidents</u>	17
<u>Environmental Failure</u>	17
<u>Intentional Acts</u>	17
<u>3. Vulnerability of IT Resources to Threats:</u>	18
<u>4. Loss Potential:</u>	18
<u>AMENDMENTS</u>	18
<u>APPENDIX A -- CHANGE LOG</u>	18
<u>APPENDIX B – REFERENCES</u>	18
<u>I.D IT SECURITY STRATEGY</u>	
<u>INTRODUCTION</u>	19
<u>SCOPE</u>	19
<u>SECURITY STRATEGIES</u>	19
<u>Strategy 1 – Security Access:</u>	19
<u>Strategy 2 – Personnel Security:</u>	20
<u>Strategy 3 –Physical Security:</u>	20
<u>Strategy 4 –E-Commerce Security:</u>	20
<u>APPENDIX A -- CHANGE LOG</u>	20
<u>I.E.1 PERSONNEL SECURITY</u>	
<u>INTRODUCTION</u>	21
<u>SCOPE</u>	21
<u>STANDARD</u>	21
<u>1. Hiring Practices</u>	21
<u>Community Colleges of Spokane Staff:</u>	21
<u>Contract or Consultant Staff (TBD)</u>	21
<u>New Employee Orientation</u>	21
<u>Access Security (TBD)</u>	22

<u>Ongoing Training</u>	22
<u>Disciplinary Action</u>	22
<u>Separation (TBD)</u>	22
<u>2. Reference Checks</u>	22
<u>3. Security Awareness Training (TBD)</u>	22
<u>4. Security Program Training (TBD)</u>	23
<u>5. Employee Performance Requirements</u>	23
<u>6. Vendor and Service Personnel Monitoring</u>	23
<u>Contractual Issues</u>	23
<u>7. Background checks where appropriate</u>	24
<u>AMENDMENTS</u>	24
<u>APPENDIX A -- CHANGE LOG</u>	24
<u>APPENDIX B – REFERENCES</u>	24

I.E.2 PHYSICAL SECURITY

<u>INTRODUCTION</u>	25
<u>SCOPE</u>	25
<u>STANDARD</u>	25
<u>1. Location and layout of facility</u>	25
<u>2. Physical security attributes for computer or telecommunications rooms</u>	25
<u>3. Facility Access Control</u>	26
<u>Restricted Access IT Areas (Internal controls)</u>	26
<u>Access Controls -- Keys and Key Cards</u>	26
<u>4. Data Storage and Telecommunications Controls</u>	27
<u>Fire Suppression</u>	27
<u>Flood/Water Protection</u>	28
<u>Climate Control</u>	28
<u>Electrical Power and Backup Power</u>	28
<u>Evacuation Planning and Building Safety</u>	28
<u>5. Off-Site Media Storage</u>	28
<u>Data Storage</u>	28
<u>6. Mobile/Remote Computing Security Control-Laptops-Data Storage Devices</u>	29
<u>CCS Lap Top Pool</u>	29
<u>AMENDMENTS</u>	29
<u>APPENDIX A -- CHANGE LOG</u>	29
<u>APPENDIX B – REFERENCES</u>	29

I.E.3 DATA SECURITY

<u>INTRODUCTION</u>	30
<u>SCOPE</u>	30
<u>STANDARD</u>	30
<u>1. Agency Data Security Policy Statements</u>	30
<u>2. Software Version Control And Its Currency</u>	30
<u>Administrative Application Software (CIS/WCTC)</u>	30
<u>Administrative Application Software (Local)</u>	30
<u>HP3K Operating System</u>	31
<u>P/C & Office Application Software</u>	31
<u>Network System Software/Configuration</u>	31
<u>3. Access Control Techniques</u>	31
<u>Elevated Privileges</u>	32
<u>System Monitoring</u>	33
<u>4. Data Entry Processes</u>	33
<u>5. Processing Accuracy</u>	33
<u>6. Distribution Of Output Reports/Introduction Or Release Of Data</u>	33
<u>7. Data And Program Backup</u>	34
<u>Media Protection</u>	34
<u>8. Controls To Prevent Unauthorized Use Or Removal Of Media</u>	34
<u>Facility Access Control</u>	34

<u>Restricted Access IT Areas (Internal controls)</u>	34
<u>Access Controls -- Keys and Key Cards</u>	35
<u>Data Storage And Telecommunications Controls</u>	36
<u>Electrical Power and Backup Power</u>	36
<u>Evacuation Planning and Building Safety</u>	36
<u>Off-Site Media Storage</u>	36
<u>Data Storage</u>	36
<u>10. Data Encryption Standards For Storage And Transmission</u>	37
<u>Data Encryption Algorithms</u>	37
<u>Key Management</u>	37
<u>Specific Tools and Protocols</u>	37
<u>11. Processing Audit Trails</u>	37
<u>12. System Access Violations</u>	38
<u>Indications Of A Potential Compromise</u>	38
<u>General Guidelines For Incident Response</u>	38
<u>Stage 1 – Make Initial Assessment</u>	38
<u>Stage 2 – Protect Evidence</u>	38
<u>Stage 3 – Contain The Damage And Minimize Risk</u>	39
<u>Stage 4 – Identify Type And Severity Of Compromise(S)</u>	39
<u>Stage 5 – Notify External Agencies</u>	39
<u>Stage 6 – Recover Systems</u>	39
<u>Stage 7 – Compile And Organize Incident Documentation</u>	39
<u>13. Intrusion Detection</u>	39
<u>Monitoring And Preventive Measures</u>	39
<u>14. Virus Protection</u>	40
<u>General</u>	40
<u>Microsoft Exchange Servers</u>	40
<u>Maintenance Of The Antivirus Systems</u>	40
<u>When A New Virus Is Spreading</u>	40
<u>If The Site Becomes Infected</u>	41
<u>15. Control Of Interactive Internet Technology (TBD)</u>	41
<u>16. Appropriate Disposal Of Hardcopy Data</u>	41
<u>17. Software Testing</u>	41
AMENDMENTS.....	41
APPENDIX A -- CHANGE LOG.....	41
APPENDIX B – REFERENCES.....	41

I.E.4 NETWORK AND TELECOMMUNICATIONS SECURITY..... 42

INTRODUCTION.....	42
SCOPE.....	42
STANDARD.....	42
<u>1. Network and Telecommunications Management</u>	42
<u>Password</u>	42
<u>Services (TBD)</u>	42
<u>2. Internetworking Servers</u>	43
<u>MPE Configuration</u>	43
<u>Windows Server Configuration</u>	43
<u>Web Server Configuration</u>	43
<u>Microsoft Mail Servers</u>	43
<u>Network Time Services</u>	44
<u>Firewall Logical Specification (TBD)</u>	44
<u>3. Network Infrastructure Equipment</u>	44
<u>Access Controls</u>	44
<u>Telecommunications Controls</u>	44
<u>4. Data Transmission within Agency Intranet and Extranet</u>	45
<u>Configurations Specific to the CCS PIX Firewall (TBD)</u>	45
<u>Router Access Control Lists (ACL) for the K20 Border Routers</u>	45
<u>E-mail Transfers</u>	46
<u>Web-based Transfer</u>	46
<u>Dial-in Transfers</u>	46

Secure Shell (SSH) and File Transfer Protocol (FTP).....	46
College User VPN Access: (TBD).....	46
5. <u>Remote Access to Applications in these Areas</u>	47
Documentation of Firewall Rules (TBD)	47
6. <u>Physical Network Infrastructure</u>	47
Access Controls.....	47
7. <u>Secure Location of Communications Equipment to Prevent Theft and Tampering</u>	48
8. <u>Terminal, Remote Job Entry, and network node (bridges, routers, etc.) access security (including Telnet, RLOGIN, GDP, etc.</u>	48
Console and Terminal Access.....	48
Dial-in Access and Modems.....	48
Windows System Configuration:.....	48
MPE System Configuration:.....	49
9. <u>Controls to Prevent Unauthorized Programs in to Computer Systems</u>	49
Audit/Assessment of Firewall (TBD).....	49
Windows System Configuration:.....	49
Windows Virus Protection:.....	49
Microsoft Exchange Servers.....	50
Maintenance of the Antivirus System.....	50
When a New Virus Is Spreading.....	50
If the Site Becomes Infected.....	50
Unix System Configuration:.....	50
11. <u>Network Breach Detection and Incident Response</u>	51
Indications of a Potential Compromise.....	51
Incident Response.....	51
General Guidelines.....	51
Stage 1 – Make Initial Assessment.....	51
Stage 2 – Protect Evidence.....	52
Stage 3 – Contain the Damage and Minimize Risk.....	52
Stage 4 – Identify Type and Severity of Compromise(s).....	52
Stage 5 – Notify External Agencies.....	52
Stage 6 – Recover Systems.....	52
Stage 7 – Compile and Organize Incident Documentation.....	52
12. <u>Remote Access Services</u>	53
College Administrative User VPN Access to HP 3000:.....	53
Staff VPN Access to CCS Internal Network:.....	53
Electronic Mail Configuration.....	53
13. <u>Wireless Communications</u>	54
General.....	54
Non CCS-owned Workstation.....	54
14. <u>VPN Methodology</u>	54
Staff VPN Access to CCS Internal Network.....	54
15. <u>VPN Solutions must use Industry Standard Protocols</u>	54
16. <u>VPN solution through a CCS Firewall</u>	54
17. <u>VPN Solutions using Smartcards</u>	55
AMENDMENTS.....	55
APPENDIX A -- CHANGE LOG.....	55
APPENDIX B – REFERENCES.....	55
I.E.5A GENERAL ACCESS SECURITY.....	56
INTRODUCTION.....	56
SCOPE.....	56
STANDARD.....	56
1. <u>Access Security Controls</u>	56
A. Mainframe (HP3000).....	56
B. Client Server.....	57
C. Security Groups.....	58
Administrative security groups.....	58
Other security groups.....	58
2. <u>Passwords</u>	59
A. Mainframe Passwords.....	59

B. Client Server	59
3. <u>Additional Requirements</u>	60
A. Dial-up Lines	60
B. Lock-out Mechanisms	60
C. Protecting Scan Codes	61
D. Recording Telecom Access	61
E. Monitoring Vendor Access	61
<u>TERMS</u>	61
Multi-user Account, Generic User Account	61
Least privilege principle	62
Hardened password, strong password	62
Domain Administrator Privilege, Rights	62
Local Administrator Privilege, Rights	62
Limitations	62
<u>AMENDMENTS</u>	62
<u>APPENDIX A -- CHANGE LOG</u>	62
<u>APPENDIX B -- REFERENCES</u>	62

I.E.5B INTERNET ACCESS SECURITY

<u>INTRODUCTION</u>	63
<u>SCOPE</u>	63
<u>STANDARD</u>	63
1. <u>Web Admissions (provided by the CIS):</u>	63
2. <u>Web Transaction Server (WTS) (provided by the CIS):</u>	65
3. <u>CCS Public Web Sites (Dist, Iel, Scc, Sfcc)</u>	67
4. <u>District Web Applications</u>	69
5. <u>SCC Web Applications</u>	72
6. <u>SFCC Web Applications</u>	74
<u>AMENDMENTS</u>	76
<u>APPENDIX A -- CHANGE LOG</u>	76
<u>APPENDIX B -- REFERENCES</u>	76

I.F SECURITY TRAINING

<u>INTRODUCTION</u>	77
<u>SCOPE</u>	77
<u>STANDARD</u>	77
1. <u>Training Aims</u>	77
2. <u>Training Activities</u>	77
Employee Security Awareness Training (TBD)	77
Policy and Standards Awareness	77
Security Training (TBD)	77
New Employee Orientation	77
Ongoing Training	78
Physical Security	78
3. <u>Training Schedule (TBD)</u>	78
4. <u>Administrator for agency IT Security Training</u>	78
5. <u>Address regularly occurring training activities</u>	79
<u>AMENDMENTS</u>	79
<u>APPENDIX A -- CHANGE LOG</u>	79
<u>APPENDIX B -- REFERENCES</u>	79

I.G SECURITY PROGRAM MAINTENANCE

<u>INTRODUCTION</u>	80
<u>SCOPE</u>	80
<u>STANDARD</u>	80
1. <u>Plan to maintain the IT security program</u>	80
2. <u>IT Security Program review process</u>	80
3. <u>Changes that will require review</u>	81

<u>4. Annual certification to the ISB</u>	81
<u>5. Agencies assigned responsibility for maintaining their security program</u>	81
<u>CCS Security Strategy</u>	81
<u>IT Security Administrator Position</u>	81
<u>6. Change management process for the IT Security Standards</u>	81
<u>7. Distribution Procedures</u>	81
<u>AMENDMENTS</u>	82
<u>APPENDIX A -- CHANGE LOG</u>	82
<u>APPENDIX B – REFERENCES</u>	82

II. INTERNET BROWSER/SERVER CONFIG AND USE

<u>INTRODUCTION</u>	83
<u>SCOPE</u>	83
<u>STANDARD</u>	83
<u>1. Internet Use and Connectivity</u>	83
<u>2. Minimum Web Client Security Requirements</u>	84
<u>3. Web Server Security Requirements</u>	84
<u>Web Content Review</u>	84
<u>Web Server Software</u>	85
<u>Remote Control of Web Servers</u>	85
<u>Web Servers Not To Be Used as a Repository</u>	85
<u>AMENDMENTS</u>	85
<u>APPENDIX A -- CHANGE LOG</u>	85
<u>APPENDIX B – REFERENCES</u>	85

III. STANDARDS FOR DIGITAL GOVERNMENT (INTERNET) APPLICATION SUBMITTAL86

<u>INTRODUCTION</u>	86
---------------------------	----



IT Security Program

Audit Ref: I.A

Effective Date: January 12, 2004

Date last modified: November 14, 2003

I. A. SECURITY PROGRAM

Introduction

This document provides an overview of the Community Colleges of Spokane (CCS) Information Technology (IT) Security Program that is developed to protect the integrity, availability and confidentiality of the district's electronic data and to safeguard its IT resources... The development of this program is in compliance with ISB standards and guidelines and will adhere to the State Auditor's Office compliance audit to be conducted once every three years. The CCS IT Security Program and its associated policies and standards will be reviewed annually for changes and updates. The purpose of this document is to define the common assumptions and topics covered in this program

Scope

The CCS IT Security Program applies to all faculty, staff and administration within the CCS community, with specific duties and responsibilities placed upon Information Systems and the technology support departments at each of the four operating units.

The Community Colleges of Spokane is a multi-campus educational district consisting of the following four units: Spokane Community College (SCC), Spokane Falls Community College (SFCC), the Institute for Extended Learning (IEL) and the district office. This standard applies to all members of the CCS community, with specific duties and responsibilities placed upon the Information Systems and Technology Support staff within the district. This IT Security Program applies to all district-wide facilities; equipment and services and will govern all IT functions across the district.

Overview

1. The CCS IT Security Program will consist of the following components:

- IT Security Policy
- Acceptable Use Policy

- IT Security Program
- Risk Analysis
- IT Security Strategy
- Personnel Security
- Physical Security
- Data Security
- Network & Telecom Security
- General Access Security
- Internet Access Security
- Security Training
- Security Program Maintenance
- Internet Browser/Server Configuration and Use

CCS recognizes the importance of an enterprise approach to IT security confirmed by the decision to have the CEO and each of the unit presidents sign the Assertions letter that will be submitted to the State Auditor's Office. CCS is confident that its security program will:

- Enable management to assure the agency's ability to protect the integrity, availability and confidentiality of information, and
 - Protect its IT assets from unauthorized use or modification from accidental or intentional damage or destruction.
2. The CCS security program will reference the Center for Information Service (CIS) IT security information since they are the provider of administrative software and support services to the Washington State Community and Technical College system. Any inter-local agreements with other state agencies or educational institutions regarding technology or exchange of information or services will be filed in the Information Systems and contracts department.
 3. CCS will ensure that any IT services purchased from another organization will meet the IT security standards outlined in the overall CCS IT Security Program. Appropriate contracts, purchase terms and conditions as well as support and security needs will be clearly identified and documented.
 4. All security policies and standards related to end-user roles and responsibilities will be written in a non-technical manner, however, standards focused on specific technical configurations and goals will incorporate appropriate technical descriptions to be useful for IT support staff. ***CCS acknowledges that not all standards or procedures outlined in this document are fully implemented. Our primary goal is to ensure compliance with ISB standards and guidelines in a written form. The next goal is to ensure that CCS is adhering to all standards outlined in the security program. To facilitate the implementation process, any steps that are not fully adhered to will be noted by the initials TBD meaning (To Be Determined). A list of TBD standards and procedures will be developed and implemented as part of future IT work assignments.***

Appendix A -- Change Log

Date	By	Version	Notes
10/20/03	D. Hol	1.0	

I.B. IT SECURITY POLICY

1.70.08 CCS INFORMATION TECHNOLOGY – SECURITY POLICY

Note: This policy is new and in the process of final adoption at the December, 2003 board meeting. It has passed preliminary review and acceptance by the various executive and staff cabinets and councils.

Purpose

The purpose of this Information Technology (IT) Security Policy is to create an environment within the Community Colleges of Spokane (CCS) that maintains system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data.

This policy governs all other Community Colleges of Spokane standards and procedures pertaining to IT usage for on-campus and off-campus use and complies with the Washington State Department of Information Services (DIS) IT Security policies, standards and guidelines.

Scope

The scope of this policy extends to all campus Information Technology facilities, equipment and services that are managed by Spokane Community College, Spokane Falls Community College, the Institute for Extended Learning and the district office as well as off-site data storage, computing and telecommunications equipment. This policy also includes application-related services purchased from other state agencies or commercial concerns, and Internet-related applications and connectivity.

It is not the intent of this policy to restrict academic freedom in any way, therefore this policy exercises the exemption granted in the Washington State Department of Information Services (DIS) Information Technology (IT) Security Policy for Institutions of Higher Education, pursuant to RCW 43.105.200 which states; “In the case of institutions of higher education, the provisions of chapter 20, Laws of 1992, apply to business and administrative applications but do not apply to academic and research applications.”

Policy

IT security is defined as:

- Protecting the integrity, availability and confidentiality of information assets managed by CCS.
- Protecting information assets from unauthorized release or modification, and from accidental or intentional damage or destruction.
- Protecting technology assets such as hardware, software, telecommunications, networks (infrastructure) from unauthorized use.

It is the IT Security Policy of CCS that:

1. Compliance with DIS Security Policies: CCS shall operate in a manner consistent with the goals of the Department of Information Systems IT Security Policies and Standards to maintain a shared, trusted environment within the Washington Community and Technical College (WCTC) system for the protection of sensitive data and business transactions. CCS shall provide secure business applications, infrastructures, and procedures for addressing the business needs of its four operating units.

2. **Principles of Shared Security:** Furthermore, CCS will subscribe to the following principles of shared security:
 - CCS shall assure that appropriate security standards are considered and met when developing or purchasing application systems or data access tools;
 - CCS shall recognize and support the necessity of authenticating external parties needing access to sensitive information and applications;
 - CCS shall develop and follow security standards for securing workstations, servers, telecommunications, and data access within its network; and
 - CCS shall follow security standards established for creating secure sessions for application access.

3. **Secure Internet Applications:** CCS will ensure that all Internet based applications that conduct transactions for state business, with other public entities, citizens and business adhere to the DIS standards for developing and documenting secure Internet applications.

4. **Employee Training:** CCS will ensure all staff is trained in IT security awareness, and that technical staff receive the appropriate training commensurate with their job responsibilities. .

5. **Annual Review:** CCS will review its IT security processes, procedures, and practices annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment.

6. **Compliance Audit:** CCS will conduct a compliance audit of its IT Security Policy and Standards once every three years in accordance to State Auditor’s requirements. CCS will maintain documentation showing the results of its audit and the plan for correcting material deficiencies revealed by the review. The State Auditor may audit CCS IT security processes, procedures, and practices, pursuant to RCW 43.88.160 for compliance with this policy.

7. **Oversight:** Pursuant to RCW 43.105.017(3), the executive for each of the four operating units of the Community Colleges of Spokane is responsible for the oversight of their respective IT security program and will confirm in writing that the agency is in compliance with this policy. The annual security verification letter will be submitted to the ISB, as required. The verification indicates review and acceptance of CCS security processes, procedures, and practices as well as updates to them since the last approval. It is the responsibility of all members of the college community to adhere to this policy and the standards contained in the IT Security Program.

The CCS IT security standards and practices contain information that may be confidential or private regarding CCS business, communications, computing operations and employees. Persons responsible for distribution of these documents should consider the sensitive nature of the information as well as the related statutory exemptions from public disclosure See RCW chapter 42.17.

Related Standards and Guidelines

DIS Information Technology Security Policy	http://www.wa.gov/dis/portfolio/
DIS Information Technology Security Standards	http://www.wa.gov/dis/portfolio/
DIS Information Technology Security Guidelines	http://www.wa.gov/dis/portfolio/
SAO Information Technology Security Policy Audit Standards	http://www.wa.gov/dis/portfolio/
CCS Information Technology Security Standards	http://ccsi.spokane.cc.wa.us/manform.htm
CCS Acceptable Use Policy	http://ccsi.spokane.cc.wa.us/manform.htm
CCS Information Technology Security Policy	http://ccsi.spokane.cc.wa.us/manform.htm

1.71.02 INFORMATION TECHNOLOGY

Note: This policy is currently enforced and has been adopted.

Community Colleges of Spokane (CCS) will provide, within available resources, a comprehensive program of appropriate information technologies to include technological infrastructure, and related services to support effective instruction and learning, efficient operations, and enhanced communications district wide, and to provide requisite skills to students and staff.

The management and use of information technology resources will follow a district-wide technology plan that will address planning, implementation, and support systems required to ensure and maintain the efficient and effective use of such technology. Separate college and IEL information technology plans may be developed to address unique campus needs and shall be coordinated and compatible with the district-wide plan.

The district-wide technology plan will be developed and reviewed annually by appropriate individuals and groups and shall include but not be limited to the following:

- Defining technological infrastructure to include but not be limited to networks, hardware, and software along with all aspects of acquiring, installing, maintaining, and replacing such resources and the coordination of such infrastructure with present and future telecommunication services;
- Support services to include but not be limited to help desks, administrative information systems, curriculum support, research and development, web development, distance learning, and electronic communication tools;
- Tactical plans necessary to meet CCS's programs and operational needs;
- A proposed budget that identifies staffing, facilities, and infrastructure required to support the plan;
- Reliable access to technology resources for students, faculty, and staff;
- Safeguards to ensure technology security and compliance with applicable laws;
- Specific definitions for the roles and responsibilities of district, college, and IEL prime information technology staff to provide integrated and complementary support services;
- Training in the use of technology for staff and faculty;
- Programs that focus on customer support and operational procedures;
- Ensure compatibility with state technology systems and organizations;
- Develop processes to review and address variances and unique needs within the campuses.

Procedural guidelines will be developed to create a district-wide technology council to develop the technology plan and provide for its maintenance and revision as needed. The council will be led and chaired by the district director of information systems.

Passed by District Deliberative Body: March 8, 1999

Passed by Board of Trustees: April 20, 1999

Procedural Guidelines

1. An ongoing district-wide information technology council will be established to develop, implement, maintain, and revise the technology plan. The plan shall be strategic and not an operations plan.
2. The council shall be chaired, and its activities directed and led, by the district director of information systems. Members of this council, other than the chair, shall be the prime information technology person and a faculty member as designated and appointed by the chief executive at the colleges and the IEL.

3. The council shall set its meeting schedule to develop the technology plan in accordance with Board of Trustees Policy No. 1.71.02. The initial plan shall be completed during fall quarter 1999, reviewed annually and presented to the chancellor/chief executive officer for approval. The chancellor/chief executive officer may share and consult with other individuals and groups as appropriate. The council may be called to meet, review and make recommendations for short-term emerging initiatives not part of the initial plan.
4. The approved plan will be shared with the college community and shall be reviewed and revised as necessary by the council. All revisions shall be approved by the chancellor/chief executive officer.
5. The approved plan and all subsequent revisions and its associated budget are to be given due consideration during the development of the overall CCS operation and capital budgets.
6. All information technology decisions must fall within the approved plan, and any variances must be prior approved by the council.

Passed by the District Deliberative Body: March 8, 1999

I.C BUSINESS IMPACT AND RISK ANALYSIS

Introduction

This standard assesses the business impact, risk, threat and vulnerability of mission critical systems and applications. The following information provides an overview of the elements of a business impact and risk analysis that should be considered.

Scope

The purpose of the business impact analysis and risk, threat, and vulnerability analysis is to help CCS identify its principal security exposures and the probability of occurrence and vulnerabilities.

Business Impact and Risk, Threat and Vulnerability Analysis

The Community Colleges of Spokane must place a tremendous amount of trust in the honesty and integrity of its staff as well as in their technical competence. The CCS staff designs, manages, and supports the core services and core business applications of the colleges. Should this trust be broken, either through malicious acts or carelessness, severe damage could be done to the organization or to the whole college system.

Given the high level of dependence on the staff, the most significant threats are:

- Unauthorized access to data -- malicious
- Unauthorized modification of data -- malicious
- Unintentional or incorrect modification of data (e.g., while performing support) -- accidental
- Theft of equipment or resources -- malicious
- Damage to equipment or resources -- malicious or accidental
- Denial/loss of service -- malicious or accidental

Given the nature of the asset, the nature of the threat, and the history of the organization, the primary risk associated with the CCS staff is loss of service by accident. This loss of service does have follow-on risks of: loss of revenue, dissatisfaction of customers, interruption of productive work, and to some degree a loss of reputation. Secondary to this threat is the unintentional or incorrect modification of data. This can include such things as severe program bugs or failures and incorrect procedures during recovery or support operations.

The computing systems within the scope of this standard include critical infrastructure to the daily business and operations of CCS. While not true across the board, some vendor access opens another possibility to jeopardize the integrity of the computer system, or its data..

A. Business Impact Analysis:

The following impact analysis was done as part of the CCS Disaster Recovery Plan and is included for reference in this standard:

The priority scheme used to determine the criticality should be accomplished by ranking each area from 1 to 5, with 5 being the most critical. The staff recognized data control and computer operations, active file protection, and network management as the most critical IS services. The major applications of SMS, MIS, FAS, PPMS, and FMS are the most critical applications, with exact criticality depending on the timing in each cycle. The IS Department's most critical assets are the computer processors, air conditioners, power conditioner, file servers, and the network.

IS Department Services

Service	Ranking	Value
Application Program Development	1	Lowest

Service	Ranking	Value
Equipment Evaluation and Selection	1	Lowest
Network Design and Implementation	1	Lowest
Documentation (User Manuals)	2	Low
Training	2	Low
Forms Acquisition and Storage	2	Low
Delivery	3	Medium
Report Distribution	3	Medium
Historical File Storage	3	Medium
Consultation, Communications, and Public Relations	4	High
Report Processing	4	High
Telecommunications and Online Access	4	High
Data Control and Computer Operations	5	Highest
Active File Protection (Data and Libraries)	5	Highest
Network Management and Security	5	Highest

IS Department Application Systems (includes Support Documentation

Applications	Ranking	Value	Critical Dates
Job Accounting System	1	Lowest	
Electronic Mail System	2	Low	
Mailing Label System	2	Low	
Forms Inventory System	3	Medium	
Tape Library System	3	Medium	
System Support Software	4	High	
Job Scheduling System	4	High	
Student Management Student (SMS)	5	Highest	During Registration and Grades
Management Information System (MIS)	5	Highest	10th Day of Each Quarter
Financial Aid System (FAS)	5	Highest	
Payroll/Personnel System (PPMS)	5	Highest	
Financial Management System (FMS)	5	Highest	10th Day, 13th and 25th Months

IS Department Assets

Asset	Ranking	Value
Office Equipment	1	Lowest
Distribution Equipment	2	Low
Personal Computers	3	Medium
500KW Generator	3	Medium
Air Conditioner and Power Conditioner	4	High
Network Management Tools	4	High
Computer Processor and Server	5	Highest

B. Risk Threat and Vulnerability Analysis:

1. Identify Risks:

In preparation for Y2K, the Information Systems department conducted an extensive study and Y2K planning exercise in preparation for the year 2000. This included a thorough business and risk assessment ranging from infrastructure to administrative applications. CCS systems and services were categorized into five vital services identified as follows:

- Vital Service 1: Provide a safe and healthy environment for our students and employees
- Vital Service 2: Admit, register and advise students
- Vital Service 3: Provide Instruction
- Vital Service 4: Provide financial services
- Vital Service 5: Protect vital records and fulfill mandatory reporting requirements

For each vital service, staff analyzed what systems supported each service, the components for each system were identified and special notes documented for each item.

Given the high level of dependence on the staff, the principle security exposures are:

- Unauthorized access to data -- malicious
- Unauthorized modification of data -- malicious
- Unintentional or incorrect modification of data (e.g., while performing support) -- accidental
- Theft of equipment or resources -- malicious
- Damage to equipment or resources -- malicious or accidental
- Denial/loss of service -- malicious or accidental

2. Probability of Occurrence:

The probability of occurrence can range from low to high. This can be reduced through careful screening and monitoring of personnel, training, and documented checks and balances for mission critical systems and functions. Given the nature of the asset, the nature of the threat, and the history of the organization, the primary risk associated with the CCS staff is loss of service by accident. This loss of service does have follow-on risks of: loss of revenue, dissatisfaction of customers, interruption of productive work, and to some degree a loss of reputation. Secondary to this threat is the unintentional or incorrect modification of data. This can include such things as severe program bugs or failures and incorrect procedures during recovery or support operations.

The IS assessment of vulnerability is based upon an approach that evaluates the likelihood of occurrences for each potential threat. The focus of the IS control is centered on human errors or vandalism, for which training and security are the prevalent protective measures. However, unintentional acts that may have significant impacts are also considered.

Listed below are value assessments for possible disasters caused by nature, loss of utilities, software failure, and/or human-induced destructive acts. Also listed are the IS preventative measures taken for each potential threat.

Natural Hazards

Potential Threats	Likelihood of Occurrence (Yearly)	Preventative Measure
Fire*	Low	Fire Extinguishers, Smoke Alarms, Off-Site Tapes, FM-200 System
Flooding	Medium	Water Detectors
Landslide	Low	None
Earthquake	Medium	None

High Winds*	Medium	Circuit Breakers, Isolation Transformer, 500KW Generator
Snow/Ice Storm	Medium	Heating System, Power Generator
Volcano	Medium	None

*Thunder and lightning storms are included in the fire and high winds categories.

Accidents

Potential Threats	Likelihood of Occurrence (Yearly)	Preventative Measure
Power Loss	Low	Power Generator, UPS, 500KW Generator
Power Failure	Low	Power Conditioner, UPS, 500KW Generator
A/C Failure	Medium	Two Air Conditioners with Auto-Restart
Power Spikes	Medium	UPS Power Conditioner
Software	Medium	System Backups
Telecom Loss	Medium	Dialup Modem

Environmental Failure

Potential Threats	Likelihood of Occurrence (Yearly)	Preventative Measure
HP Processor Failure	Low	16 Processors
Fire	Low	Fire Extinguishers Smoke Alarms Off-Site Tapes FM-200 System
Operating System Failure	Low	Backup Solution Software Release Tape
Water Damage	Low	Water Detectors
Application Software Failure	Medium	Backup Solution Patches
Communication Failure	Medium	Training on Various Controls
Data File Failure (crashes)	Medium	Recovery Analysis Backup Solution
Hardware Failure	Medium	
Operator/User Error	Medium	Training on Various Controls

Intentional Acts

Potential Threats	Likelihood of Occurrence (Yearly)	Preventative Measure
Employee Sabotage	Low	Alarm Monitoring Services
Theft	Low	Alarm Monitoring Services
Unauthorized Use	Low	System Security (password, account control, etc.)
Vandalism	Low	Alarm Monitoring Services
Bomb Threat	Low	None
Computer Virus	High	Anti-Virus and Backup Solution

3. Vulnerability of IT Resources to Threats:

Vulnerabilities can be reduced by following specific procedures for system testing and updates. Wherever possible, CCS will develop a separate test lab of equipment and software apart from production systems to minimize the negative impact on production systems. The computing systems within the scope of this standard also include critical infrastructure to the daily business and operations of the CCS. While not true across the board, some vendor access opens another possibility to jeopardize the integrity of the computer system, or its data. Additionally, some vendor access may require direct access to confidential data.

Given the nature of vendor access, the most significant threats are:

- Loss of service -- accidental
- Unauthorized access for "research"-- malicious
- Physical damage to components -- accidental
- Theft of information -- malicious
- Misconfiguration of computer resources that create an operational or security flaw -- accidental

Given the nature of the asset and the nature of the threat, the primary risk associated with vendor access is either loss of service or misconfiguration. Both of these risks have follow-on risk associated with them of loss of revenue, dissatisfaction of customers, interruption of productive work, and to some degree a loss of reputation. In the event of damaged equipment, there may also be the replacement cost of that equipment.

4. Loss Potential:

It is difficult to estimate a quantitative or qualitative loss regarding a potential threat. Generally, unanticipated loss of services due to accidents or system malfunctions can best be described through loss of employee productivity. Malicious threats could result in the value of stolen equipment or software or the transfer of funds

For example, in my fourteen years of service in the IT department I have experienced one major hardware failure on the HP 3000 mini computer. A hard disk failed in the middle of the backup which was rendered useless. While we had a full backup from the previous day, it meant that all of the days input transactions were lost. In addition, it took the vendor approximately eight hours to repair the system due to a variety of reasons. This meant that our users lost approximately two days of productivity considering they had to re-input the first days data along with the transactions of the second day.

The best way to calculate the loss is to multiply and average hourly rate times the number of hours lost for all of the users affected by the downtime. This was a significant cost and provided the justification I needed to purchase and install and completely new and redundant hard disk system for the HP 3000.

Amendments

Appendix A -- Change Log

Date	By	Version	Notes
11/13/03	D. Hol	1.0	

Appendix B – References

CCS Information Systems Disaster Recovery Plan

I.D IT SECURITY STRATEGY

Introduction

This document provides an overview of the Community Colleges of Spokane (CCS) Information Technology (IT) Security Program and the strategies necessary to protect its data and IT assets. The purpose and focus of these strategies is to define the level of protection that should be accorded to protect the information assets of the colleges.

Scope

The Community Colleges of Spokane is a multi-campus educational district consisting of the following units: Spokane Community College (SCC), Spokane Falls Community College (SFCC), the Institute for Extended Learning (IEL) and the district office. This standard applies to all members of the CCS community with specific duties and responsibilities placed upon the Information Systems and Technology Support departments at CCS. This IT Security Program applies to all campus and off-site facilities; equipment and services.

Security Strategies

This document does not replace any specific security standards. Its purpose is to define the common assumptions and strategies used within those documents. The following are high level goals and strategies that are consistent with ISB guidelines. The detail of how each of the following strategies are to be accomplished is further defined in the security standards that follow. It is important to recognize that CCS' ability to apply these protective measurements is dependant on available monetary and human resources. In some cases, adjustments to specific standards may be required if it is determined that additional resources are needed but not available or approved. CCS technology needs, projects and priorities will dictate IT staff's ability to comply with standards and procedures that are not currently implemented.

Strategy 1 – Security Access:

The strategy to ensure secure access to CCS mission critical applications and systems requires that the following are clearly defined:

1. Specific security practices for IT personnel, district-wide users of computer services, students and anyone else who may need access to sensitive or confidential information...
 - *The standards and practices that satisfy this requirement can be found in IT Security Standard I.E.5 General Access Security*
2. Focus on preventing unauthorized access, misuse, modification, damage to, or loss of IT hardware, software, data and facilities
 - *The standards and practices that satisfy this requirement can be found in IT Security Standard I.E.2 Physical Access Security, I.E.3 Data Security, I.E.5A General Access Security; and I.E.5B Internet Access Security*
3. Identify systems access and user authentication methods as part of a security architecture that will ensure secure applications.
 - *The standards and practices that satisfy this requirement can be found in IT Security Standard, I.E.3 Data Security, I.E.5A General Access Security; and I.E.5B Internet Access Security.*

Strategy 2 – Personnel Security:

The strategy that ensures that personnel security is maintained for IT staff that are responsible for implementing and supporting applications and system security will require that the following are clearly defined:

1. IT security duties will be assigned to an individual or group responsible to maintain and support IT resources.
 - *The standards and practices that satisfy this requirement can be found in IT Security Standard, I.A. Security Program, I.E.1. Personnel Security, I.F Security Training, I.G Security Program Maintenance*
2. Identify training goals for IT staff to ensure they have the skills to administer security responsibilities.
 - *The standards and practices that satisfy this requirement can be found in IT Security Standard, I.E.1. Personnel Security, I.F Security Training*
3. Ensure that IT staff has appropriate authority to enforce the security policy and standards and processes identified in the CCS IT Security Program.
 - *The standards and practices that satisfy this requirement can be found in IT Security Policy and CCS Letter of Assertions*
4. Outline actions to be taken for failure to observe security rules and procedures through appropriate awareness and training programs.
 - *The standards and practices that satisfy this requirement can be found in IT Security Standard I.E.1 Personnel Security.*

Strategy 3 –Physical Security:

The strategy that ensures that physical security is provided for all IT facilities and equipment will require that the following controls are in place:

1. Specify physical security attributes and controls for computer and telecommunications rooms.
 - *The standards and practices that satisfy this requirement can be found in IT Security Standard I.E.2 Physical Security.*
2. Ensure that off-site storage and location and layout of central network/server rooms are identified.
 - *The standards and practices that satisfy this requirement can be found in IT Security Standard I.E.2 Physical Security.*

Strategy 4 –E-Commerce Security:

The strategy that ensures that E-Commerce applications are secure and that confidential or sensitive data is protected will require that the following controls are in place:

1. E-Commerce and application development will incorporate appropriate security measures and documentation to ensure the following:
 - Handling software and hardware component failure
 - Unauthorized browsing of sensitive or private information
 - Application misuse
 - Unauthorized deletion, modification or disclosure of information
 - Penetration and privilege escalation
 - Misrepresentation of data or credentials
- *The standards and practices that satisfy this requirement can be found in IT Security Standard I.E5B Internet Access Security, and II. Internet Browser/Server Configuration and Use.*

Appendix A -- Change Log

Date	By	Version	Notes
11/10/03	D. Hol	1.0	

I.E.1 PERSONNEL SECURITY

Introduction

This standard defines the specific steps needed to implement the Community Colleges of Spokane (CCS) Security Policy and other standards as they relate to personnel issues. This in no way is meant to supersede the organizations personnel policies, but rather gathers in one place those practices for managing the human side of IT security. The standard should be reviewed, at minimum, on an annual basis.

Scope

This document is intended to augment, not supersede any CCS personnel policy or procedures. This document focuses on selection, orientation, and supervision of employees and contractors related to their duties and roles in supporting IT systems. The objective is to ensure that a high level of integrity and satisfactory staff conduct is achieved and maintained, and to promote an awareness of security matters amongst all levels of CCS staff.

Agencies must develop, document, and implement processes for the selection, orientation, and supervision of employees and contractors. The objective is to ensure that a high level of integrity and satisfactory staff conduct is achieved and maintained, and to promote an awareness of security matters. Include the following: Hiring practices, reference checks, security awareness training, security program training, employee performance requirements, vendor and service personnel monitoring, and background checks where appropriate.

Standard

1. *Hiring Practices*

Community Colleges of Spokane Staff:

- Standard fair hiring practices, as defined by the CCS personnel policy will be followed. These practices are defined in the CCS Administrative Procedure 2.10.04 and individual on-line forms located on the CCS Intranet.

Contract or Consultant Staff (TBD)

- Contract or consultant staff that will be on-site at CCS for any extended period of time will be made aware of and expected to comply with the policies and procedures of the CCS. The contractor will be required to sign a document acknowledging these policies and procedures.
- If they are granted keys, key cards, or accounts to computer systems, their end-of-engagement will be treated as an employee separation.
- If they are granted an account, that account will be configured to expire after 60 days or at the end of the engagement, whichever comes first. The account may be re-activated for additional 60-day periods if they are still engaged with the CCS.

New Employee Orientation

- All new hires will be given a basic orientation that covers the following policies and procedures as well as the location of the full collection of documents for future review and reference.
- Emergency and Safety Procedures
 - CCS Emergency Management Plan
 - Medical and First Aid Information
 - Fire Procedures
 - State policies
 - Cellular Telephone Use Policy
 - Conflict of Interest Policy
 - Drug Policy

- Ethical Conduct Executive Order: Standards of Ethical Conduct
- Service of Process
- Anti-Harassment Discrimination Policy
- Whistleblower Program
- Acceptable Use Policies
 - CCS Acceptable Use Policy
- CCS IT Security Standards (TBD)
 - Security Training

Access Security (TBD)

- Written copies of these policies and standards will be available to all employees on the CCS Intranet. New employees receive an orientation and will receive information regarding these resources at that time. After their review of the documents, new employees will be presented a statement for signature acknowledging that they have read these and that they understand their responsibility for compliance with these policies. Other policies may also be included in the initial orientation.

Ongoing Training

- It is the responsibility of each CCS employee to annually review the various policies that pertain to their ongoing employment with the CCS, including those listed in the New Employee Orientation section above

Disciplinary Action

- Failure to comply with the policies and standards of the CCS may lead to disciplinary action. See CCS Supervisor Handbook that specifically outlines employee disciplinary action.

Separation (TBD)

- As noted in existing CCS handbooks and procedures, upon separation or being relieved of duties, a) An employee will be required to surrender all keys and key cards, and b) All account access will be disabled and any shared passwords that were known by the employee will be changed.
- By use of the CCS Exit Interview Form, the employee's director will inform the following persons of the situation no later than the day of separation or relief of duties occurs: Facilities Department, Campus Technology Department and Information Systems Department...

2. Reference Checks

- Three references will be requested, and all three will be attempted to be contacted. An effort will be made to gain a clear sense of the applicant's competence, levels of prior performance, and their personal integrity. If possible, the first level references should be queried about other possible references that could be contacted for information. Checks with former peers and/or supervisors at places of prior employment should also be considered.

3. Security Awareness Training (TBD)

- Each staff member will undergo an initial Security Awareness program within three months of hire.
- Sufficient time will be made available for staff to periodically participate in security awareness programs.
- CCS will provide each employee annual security awareness training through district-wide and campus e-mails and specific staff meetings and training sessions. [At present the CCS does not have a formal program in place; we will be looking to formalize a program in calendar year 2004].
- The CCS Security Administrators will be responsible for administering the CCS Security Awareness Program.

4. Security Program Training (TBD)

- As appropriate security training opportunities become available, staff will be encouraged to participate.
- The CCS Security Administrators will maintain a list of security courses, programs, and conferences that s/he is aware of, as a resource to the staff.
- Sufficient time will be made available for staff to periodically review CCS security policies and standards.
- Annually the staff will be required to review a subset of the CCS security policies and standards. Some documents they will be required to review in their entirety, others they will be provided a summary. Summaries will be used where the majority of a particular standard has a very narrow target audience (e.g., the systems administrator of a particular operating system), but there is a subset of points that pertain to a large segment of the staff. The CCS Security Administrators will prepare the summaries where needed.

5. Employee Performance Requirements

- Directors and managers must provide specific supervision for new employees working in sensitive areas or on sensitive processes.
- When reassignment of duties takes place, the individual being reassigned must arrange for the proper updates to account access and password use to ensure appropriate security is maintained. If the reassignment of duties is a result of disciplinary action, the manager or director must arrange for any needed security updates.

6. Vendor and Service Personnel Monitoring

- Access to CCS computer systems should provide the vendor's support person the least privilege required to accomplish their tasks. Generally, the vendor should not be given system administrator (or equivalent) privileges.
- The vendor's access should be limited to short durations, and only active during the length of time required to address the specific support incident. After the completion of the task, their access will be disabled.
- If vendors are given access to "standard" accounts (with a password that is shared among their support staff) on a computer system, that password must be changed after the vendor completes their work. If the account is especially sensitive and the access requirements are extended in time, the password will be changed more frequently.
- Software installations and upgrades (new functionality) to be installed by a vendor, will be clearly documented and reviewed by the site's systems administrator, and possibly the security administrator, early in the planning phase.
- Vendor software installations must not be assumed secure. After a vendor installs or upgrades a product, the site's systems administrator will review the application and related software systems to assure they are both functioning properly and securely. If defects (functional or security) are found they should be remedied immediately. If an obvious course of action is not apparent, the system will be returned to a known safe state while a solution is worked through with the vendor and site management.
- To the extent possible, the activities of the vendor should be monitored. This may take many forms depending on the technology available and the nature of the vendor's work, but could include: visual supervision, review of command history, and operating system level processes auditing.

Contractual Issues

- Support requirements, including computer system access, will be spelled out clearly in the negotiated contract with the vendor. (This may, in some cases, be an appropriate RFP item...)
- Vendors that have access to potentially sensitive data (e.g., student or employee records); will be required to sign a document that clearly defines our expectations and their legal obligations regarding the protection of that data. (TBD)
- It is recognized that the CCS have contracted with third party vendors for specific services. The CCS will define procedures to assure that the vendors can perform their contractual obligations as efficiently as possible without putting the security and integrity of the computer systems we manage at undue risk.

7. Background checks where appropriate

- For sensitive positions, more complete background checks will be done. These background checks may include questions concerning the applicant's levels of management responsibility, security clearances, previous employment, reasons for leaving previous employer and any criminal history.

Amendments

Appendix A -- Change Log

Date	By	Version	Notes
10/20/03	D. Hol	1.0	

Appendix B – References

- CCS Ethics Handbook – CCS Intranet
- CCS Personnel Handbook – CCS Intranet
- CCS Acceptable Use Policy – CCS Intranet
- CCS IT Security Strategy
- CCS IT Security Training Standard
- CCS General Access Security Standard
- WA State Ethics Laws – WA State Web Site

I.E.2 PHYSICAL SECURITY

Introduction

This standard defines the steps needed to implement the CCS IT Security Policy regarding physical security. The standard should be reviewed, at minimum, on an annual basis.

Scope

This standard addresses procedural and configuration elements that define the physical security of the various CCS technology support units and the Information Systems data processing facilities. This standard also includes the network server rooms, wiring closets, switch closets, and office areas for all information and telecommunications technology.

CCS management is responsible for assuring that adequate protective measures are implemented for all IT computing resources. The purpose of the physical security component of the IT security program is to reduce the risk of compromise of data due to physical break-ins or unauthorized access to server resources.

Note: The following standards apply primarily to the data center and the college campus facilities. CCS has approximately twelve off-campus education centers that are owned by the Foundation and operated by CCS staff that adhere to the following standards, however, CCS provides educational programs at dozens of other locations where we provide access and equipment but do not own the buildings. While security is a priority for these locations, upgrading them to follow these standards will take time and funding.

Standard

1. Location and layout of facility

- The CCS Information Systems data center is located in a secure environmentally controlled facility that has a raised computer room floor, a separate HVAC system and humidity control. It also has emergency lighting in the event of a power failure and an alarm system that warns of flooding.
- The computer room also has a sliding metal door sealing all access to the report distribution center in addition to separately keyed doors and combination locks to the Information Systems offices and computer work area. Access is restricted to all student and unauthorized personnel
- The I.S. offices and computer room are locked at the end of the shift and main access restricted and controlled by the night shift personnel.
- Asset tags are applied to all equipment as defined by the district's inventory standards. Annual inventory audits are performed and exception reports produced for any discrepancies from the fixed asset records. Inventory reports receive scrutiny from executive management and must be reviewed and accounted for by department management within thirty days of the physical inventory.
- See Appendix C, below for location of the CCS data center shown on the SCC map, building 50.

2. Physical security attributes for computer or telecommunications rooms

- Physical access to the mainframe computer room is controlled by a key card and key pad Omni-lock system. This door is kept shut at all times. Staff are required to enter the premises by using their id card with magnetic

strip or a personally assigned numeric code. All keys, id cards and numeric key pad assignments are strictly controlled and managed by the Facilities department. (See section 3 Facility Access Control for specific procedures)

- Campus telecommunication rooms and server rooms are secured and locked at all times. Access is only permitted by authorized IT or Telecommunications staff. CCS is in the process of changing standard keys locks with Onmi-lock systems that require ID cards and will log all entries. Departing or terminated employees are required to turn in keys and id cards. All workstations and consoles have secure logon and password access to prevent unauthorized use.

3. Facility Access Control

Restricted Access IT Areas (Internal controls)

- Certain areas of the facilities will have restricted access. Some of these rooms are numbered, but are otherwise unidentified as to purpose and not specifically marked as secure areas. These restricted access areas are:

IS Network/Server/Computer Rooms	These rooms will be restricted by keypad and/or key access. Those having unescorted access will be limited to <u>authorized</u> IS staff
IS Offices	Access will be restricted by keypad and/or key access.
IS Work Areas	These areas are non-public work areas. Those having unescorted access will be limited to authorized ITS and IS staff. All doors external to these work areas will remain closed and locked at all times and will be restricted by keypad and/or key access.
Network and Phone closets	The central Telecom rooms at each of the college campuses will be restricted by ID card access. Secondary phone closets and telecom rooms will be secured by key access. When possible, lockable cabinets within these rooms will be used to provide an extra layer of security. Outside vendors needing access to these areas will either be escorted by IT staff and/or Phone room staff.
Electrical closets	Each electrical closet on campus, as well as the main power distribution closet, will be restricted by traditional key access. Those having unescorted access will be limited to IS staff, computer support staff and Facilities staff. Outside vendors needing access to these areas will either be escorted by IT staff. or check in with Campus Facilities to be temporarily issued a key, if authorized.

Access Controls -- Keys and Key Cards

- Keys, proximity cards, and/or access codes will be assigned to all authorized IS staff.
 - Their access rights will be determined by their affiliation with the CCS as well as their specific job duties.
 - Access codes are to be treated like passwords and never shared with another person.
- Keys, proximity cards, and/or access codes will be assigned on an as needed, permanent basis to CCS employees only.
- All keys to Community Colleges of Spokane (CCS) facilities are the property of Community Colleges of Spokane. The CCS includes Spokane Community College (SCC), Spokane Falls Community College (SFCC), and the Institute for Extended Learning (IEL) and the District Offices (Dist).
- Keys shall be issued on a clearly defined “need” basis. Keys are considered to be tools necessary to complete assigned duties. Guidelines for determining the need for keys include the following:

- Keys to CCS facilities may be assigned only to individuals with an official CCS affiliation; i.e. faculty, staff and administration. No individual shall possess CCS keys that have not been appropriately issued to him/her. "Facilities" include buildings or portions of buildings under the control of the CCS, e.g. rental and leased buildings.
- An employee with a continuing need to frequently access an area during the hours it is locked may be issued a key(s). Upon reassignment or termination of employment, keys will be returned to the immediate supervisor who shall return the keys to the Facilities Department.
- An employee, student, vendor, or contractor with a temporary need to access an area during the hours it is locked may be issued a key(s) for the required period. Keys shall be returned to the Facilities Department at the end of the period.
- All keys shall be issued by the Facilities Department per procedure described in the District Key Control Administrative Procedures.
- Keys shall be issued upon the proper completion of the Key Check-out form signed and dated by the key holder and appropriate approving authority .If additional keys are needed at a later date, an additional Key Check-out form shall be used for each request.
- Each building administrator is responsible for establishing and maintaining a key inventory and control system for keys issued to him/her. Each building administrator may designate a key coordinator who will be responsible for obtaining, issuing and reclaiming furniture and utility keys to doors and equipment that are the responsibility of the building administrator. The Facilities Department will be notified of all key coordinators. Key coordinators may sign the Key Check-out form on behalf of their department when receiving furniture and utility keys issued to their department. Key coordinators shall, in turn, keep a record of keys they issue to key holders so there is a complete record of each key issued. Departmental key records shall be audited periodically at the discretion of the district director of facilities.
- All keys (except furniture and utility keys) shall be issued to the key holder who will actually be using the key. No CCS key shall be loaned to an individual not authorized to use CCS keys. A key that is loaned is the responsibility of the individual who signed for and received the key.
- Keys shall not be transferred from the authorized key holder of record to another person.
- Key assignments, access codes and proximity cards will be reviewed no less than annually to assure that the assignments are still appropriate. Division/Department heads will review this report for their area and arrange for necessary key returns. Ideally, quarterly reviews should be done.
- The loss of a key compromises the security of every door it accesses and shall be reported to the Facilities Department immediately.
 - Reissuance of a lost or stolen key requires the same approvals as described above for the issuing of keys.
- Upon separation from college employment, any employee will surrender to the Campus Facilities Department all keys and proximity cards that have been assigned. The employee's supervisor will ensure that the Campus Facilities department has been notified so that person's access code can be deactivated.
- Any students who have been authorized keys, but are not returning to the college for the next quarter, will turn in all keys and proximity cards before leaving the college.

4. Data Storage and Telecommunications Controls

Fire Suppression

- Fire suppression equipment must be provided for all computer rooms (including network closets). The fire suppression equipment must be a type designated for computer and electronic equipment.
- Designated staff will receive periodic training on the use of the fire suppression equipment.
- Smoke and fire detection devices should be located in each computer room and tied into the main fire alarm system.
- The fire detection and suppression systems should be inspected and tested at least annually.

Flood/Water Protection

- A water detection device is located on the true floor (beneath any raised floor) of the data center. This water detection device is monitored by a separate alarm system that can be detected by IS staff working in the data center.
- Designated staff will receive periodic training on responding to a flood situation (typically a burst pipe). This training may be in the form of reviewing documentation instead of formal training. (TBD)
- The water detection and control systems should be inspected and tested at least annually by a qualified technician. (TBD)

Climate Control

- All rooms containing computers will be provided with an adequate heating, ventilation, air conditioning (HVAC) system to assure computing equipment is maintained within its safe operating temperature.
 - Preferred operating environment is 68 - 77 degrees Fahrenheit at 40 - 60% humidity.
 - Network server rooms and switch rooms will be kept at a cooler temperature. The preferred operating environment in these rooms is 63 – 75 degrees Fahrenheit 40 - 60% humidity.
 - If computer room temperature exceeds 79 degrees, Operations staff will continuously monitor the room's environment.
 - If computer room temperature exceeds 85 degrees, Operations staff will notify the HVAC vendor or the Facilities Department.
 - If the temperature continues to increase above 85 degrees computer room doors will be opened and fans will be deployed. As all access controls will have been disabled to address an emergency temperature condition, Operations staff will be responsible for closely monitoring access to the room.
- Designated staff will receive periodic training on responding to HVAC failures. This training may be in the form of reviewing documentation instead of formal training. (TBD)

Electrical Power and Backup Power

- All primary telecommunications/data rooms for each college will be provided filtered power as well as backup power via separate uninterruptible power system (UPS). The UPS will provide backup power for all mission critical equipment in the telecommunication rooms. Critical computers and network equipment not located in one of the two telecom rooms protected by the building's UPS will need a local UPS.
- Designated staff will receive periodic training on responding to power failures. This training may be in the form of reviewing documentation instead of formal training. (TBD)
- All network and telecommunications cabling is installed in ceilings, raceways or shielded according to DIS wiring and cabling standards.
- The CCS data center is equipped and wired to support a standby generator in the event of long term power failure. This system should be tested on an annual basis in conjunction with Facilities staff. (TBD)

Evacuation Planning and Building Safety

- Emergency information, including building evacuation plans will be posted in all computer classrooms, labs, offices, work areas and server rooms in compliance with CCS Public Safety policies and procedures.
- All designated work areas will be equipped with an emergency first aid kit.
- The evacuation plan will be tested in accordance to the CCS Emergency Management Plan.

5. Off-Site Media Storage

Data Storage

- All data center mainframe and server backup tapes are stored off-site in separate campus building in a fireproof vault. Tapes are rotated daily based on a rotation schedule outlined in the CCS Computer Operations Manual

- Any waste or discarded output (including such things as paper, tape) that contains sensitive data will be stored in a secure location until such time as it can be destroyed in compliance with current CCS procedures for destroying sensitive information.
- Sensitive documents (such as the college's check stock) will be stored only in the designated secured vault in the data center area. Checks stock is controlled and distributed by the business office according to strict audit controls and procedures.
- Media (paper, tape, fiche) being prepared for distribution to CCS staff will be maintained in secure cabinets in the IS area until it is picked up by CCS Mail Services for delivery.
- Storage media (for example; tapes, CD, diskettes) that have reached end of life (cannot be reused) must be magnetically or physically destroyed prior to disposal.
- Backup and system recovery media must be stored in physically secure locations at all times. These include all copies stored locally as well as those at an off-site storage facility. Access to backup media must be restricted to Operations and Systems Administration staff.

6. Mobile/Remote Computing Security Control-Laptops-Data Storage Devices

CCS Lap Top Pool

- The CCS Technology Support groups maintain a pool of laptops available to staff for check out for business use. The pool will be managed as follows:
- Technical Services reviews the laptops in the checkout pool on a regular basis ensuring that it has appropriate virus checking software, and current versions of the operating system and related software.
- When a staff member checks a laptop out for offsite use, s/he will be required to complete a Temporary Checkout form that is to be approved by the technology support person responsible for managing the pool and the department supervisor.
- It is important to note that CCS is self insured in the event of a lost or stolen Laptop.

Amendments

- The Institute for Extended Learning is not able to comply with all of the physical security standards due to the variety of off-campus locations as explained in the following paragraph:

Note: The following standards apply primarily to the data center and the college campus facilities. CCS has approximately twelve off-campus education centers that are owned by the Foundation and operated by CCS staff that adhere to the following standards, however, CCS provides educational programs at dozens of other locations where we provide access and equipment but do not own the buildings. While security is a priority for these locations, upgrading them to follow these standards will take time and funding

Appendix A -- Change Log

Date	By	Version	Notes
10/20/03	D. Hol	1.0	

Appendix B – References

I.E.3 DATA SECURITY

Introduction

The following standard describes the various controls, processing and distribution steps, audit trails and protections for CCS' data and information resources.

Scope

This standard presents guidelines to develop, document, and implement a security program component that is appropriate for the level of sensitivity/confidentiality of the information being processed. The purpose of the data security component of the IT security program is to reduce the risk associated with the compromise or destruction of agency-controlled data. Content should include rules for the storage and dissemination of data shared with other organizations.

Standard

1. Agency Data Security Policy Statements

- The CCS shall operate in a manner consistent with the goals of the DIS IT Security Policies to maintain a shared, trusted environment within the WCTC for the protection of sensitive data and business transactions.
- CCS shall assure that appropriate security standards are considered and met when developing or purchasing application systems or data access tools
- CCS shall assure full implementation and support of the security mechanisms provided within the Administrative Applications provided to it by the Center for Information Services (CIS).
- CCS shall recognize and support the necessity of authenticating external parties needing access sensitive information and applications
- CCS shall develop, follow and support security standards for securing workstations, servers, telecommunications, and data access with its network.

2. Software Version Control And Its Currency

Administrative Application Software (CIS/WCTC)

- CCS's major Administrative Application software is provided by the CIS which serves the WCTC colleges with a standard application suite. The WCTC colleges receive periodic software updates from the CIS, the implementation of these updates are reviewed and tracked by CCS & CIS staff. Therefore the lion's share of CCS Administrative Application Software version control is as sound as the CIS delivers.
- The deployment policy standards, procedures and guidelines of the CIS cover all application software that CCS receives from them.

Administrative Application Software (Local)

- Local design and implementation must respect the principle of "least privilege"; that is; use the absolute minimum access privileges necessary to perform the task.
- Passwords used to access subsystems and resources will be stored securely. The following criteria will be used:
 - Follow industry standards regarding embedding of passwords directly in the "program" (e.g., scripts, jobs, executables, and configuration files) itself.
 - Password must be difficult to discern. The more sensitive a resource the more strongly guarded the passwording scheme needs to be. File system security of the password data store must be very strong.
 - Authentication to access the password store will be based on the process's previous authentication to the operating system or the application

- No less than two people, each of whom must be authorized to sign off on releasing a program into production, will do testing of the application software. The testing process must validate the correctness of both the technical and the functional operation of the program. (TBD)
- CCS Deployment standards and procedures are being developed at this time; we are a small development team and resource availability precludes appropriate separation of duties. The following are “goals” that our deployment procedures would like to attain. (TBD):
 - Production version of source code, control data, and the final tested executables should be stored in a repository that prevents unauthorized modification.
 - Access to the production code repository should be restricted to only those staff (or consultants) that have been granted explicit permission to access it.
 - The repository of production code should provide sufficient logging to detect if tampering has occurred, when it occurred, the changes that were made, and by whom.
 - The repository should allow the re-creation and recovery of a prior version of the production code for researching problems or recovering from a disaster.
 - The deployment process, used to manage the development and release of application code to production, must be well documented.
 - The deployment process should assure that only applications that have been tested and approved are allowed to move into production.
 - The deployment process should track the flow of application components through development to final deployment. This should include for each step of the process, such things as:
 - Who initiated/authorized and when the change (modification of the application or approval to release it)
 - What changed, and why.

HP3K Operating System

- All Operating System software updates are provided either directly from the vendor or via CIS, both organizations are trusted by CCS.
- All OS updates are logged by the HP System Administrator (TBD).

P/C & Office Application Software

- PC software version control is somewhat dictated by the PC hardware capabilities. Generally, the latest version of the PC operating system and application software is installed for student labs and workstations. Faculty and staff PC's may not always have the latest version of the software due to the lack of adequate processing power or staff resources to implement the current version on a timely schedule.
- CCS is licensed to use the Microsoft Campus Agreement that supports the current and new releases of the operating system and office applications.

Network System Software/Configuration

- CCS will attempt to maintain a common version of the operating system for enterprise network switches where possible. Vendor maintenance agreements generally require the latest version of their software to be installed to maintain support.

3. Access Control Techniques

No one has access to application data either via CIS provided applications or locally developed applications without approval from their supervisor and/or the “data owner” via appropriate access and security forms.

Users are never allowed update/write access to data using native OS tools such as EDT, Query, or other tools that do not enforce adequate data integrity and business rules. Support staff may use native OS tools against CIS provided data in read only mode and only in support of trouble-shooting tasks.

Systems housing college data will not be connected to any network until the system has been made secure and safe for connectivity.

CCS's HP3000 based administrative applications (provided by CIS) are architected so that the:

- Application users will be captured in a menu system with no access to the command shell.
- Application users will be granted access to processes based on controls in the menu system and its configuration data.
- Application users will be authenticated and be granted application access at an individual level, so that individual accountability is maintained.
- Access to specific functions within a program by application users will be configured and controlled by the assigned “security manager” for each logical business grouping (i.e. SMS, FAS, PPMS, etc.).
- Where appropriate, the application user's activity will be logged for later review.

Detailed documentation for the administration of Security-3000 on CCS’s HP3K is found in the I.S. Operations Procedure manual and is titled “Security 3000 Policies and Procedures”. This document is reviewed and updated on an annual basis (normally during the summer) prior to the annual security audit.

The following summarizes the access control features enforced for user access to CCS’s Administrative Application data and computing resources (HP3K):

- All users should have their own user profiles for logging on. User profile sharing is not allowed (TBD).
- MPE Session Name, User, and Account are the required components to defining an MPE user login profile in the Washington Community and Technical College (WCTC) environment.
- All profiles will have Security3000 passwords. In addition, all profiles with SM capability will also have MPE user and or account passwords at the discretion of the system administrator..
- Profiles are granted for specific business need; when that need no longer exists, the profile will be expired.
- Profile access will be controlled by password authentication
- No more than nine consecutive incorrect login attempts (password attempts) will lock a profile, requiring a systems administrator to unlock it.
- Appropriate warning banners will be displayed at login; this includes but is not limited to the FERPA mandated warning banner displayed to users prior to accessing student data.
- Inactive profile (those that have not been logged into within the last ninety days) will be locked. If an account persists in an inactive state, the systems administrator will attempt to determine if it can be deleted. (TBD)
- Idle terminal sessions that have not set a terminal lock will be logged off after 30 minutes of inactivity. If the session is for a user account with SM capabilities, the idle time will be shortened to 15 minutes.
- The Security 3000 violations report will be reviewed on a daily basis
- The Security 3000 maintenance report will be reviewed on a daily basis to assure all changes were correct and appropriate. (TBD)
- System logging will be enabled for at least the following events: (TBD)
 - Interactive and batch logins and logouts
 - Password changes
 - System startup, shutdown, and power failure
 - System logging configuration and management
 - Hardware diagnostic messages
- Security issues will be reported to the Security Administrator.

Elevated Privileges

- System administration privileges (and responsibilities) will be granted only to the MPE Systems Administrators. This is defined as those user accounts that have been assigned the System Manager (SM) or Privileged Mode (PM) capabilities. The user account SECURITY.SYS is an exception to this, as SM is required on the account to perform its function; but users are captured within a restricted menu, limiting their available commands and actions.
- Other system capabilities that must be tightly controlled are: System Supervisor (OP), Network Administrator (NA), Node Manager (NM), and Account Manager (AM). These privileges will be granted to non-MPE Systems Administration. ([Historically, and with cause, applications support staff have been granted access to the MGR.Pnnn accounts, which have both AM and OP capabilities; and the CCS user CONSULT.Pnnn account has OP capability. This is necessary for support staff to perform their job functions.])
- Backdoor programs (whether third party or home-grown) that allow users to elevate their privileges (to acquire SM, PM, NA, or NM) will be disabled.(TBD)

- Files and especially databases must not be released across accounts. The systems administrator, with an explanation of why it is necessary, will document any file that is released.
- No account or group granted PM capability may have unrestricted save access (e.g., SAVE:ANY).
- The business application software, as well as the system software must be protected from users on the computer system.
- When an MPE user, group, or account is created, the default security assigned by the operating system will be reviewed for appropriateness.

System Monitoring

- Nightly CCS Operations staff monitors batch production processing. The operations staff addresses any problems or ensures that the issues are communicated to others.

4. Data Entry Processes

- Data will only be inserted into the database via CIS approved applications or interface to assure that all the appropriate business rule and data integrity edits have been performed.
- Data built and maintained for CCS by CCS IS staff will only be inserted into the database via CCS approved applications or interface to assure that all the appropriate business rule and data integrity edits have been performed
- In the event of a catastrophic (fatal) program error, the program will terminate as gracefully as possible, will not leave a memory core, but will leave a log of as much useful post-mortem debugging information as possible. A graceful termination, in this context, would also include, to the extent possible, assuring data is not left in a inconsistent state, closing all open files, purging temporary files, and logging out of databases, and remote computers.

5. Processing Accuracy

- Every precaution must be taken to assure the program's execution environment cannot be tampered with.
- In the event of a fatal program error, an application will terminate gracefully, ensuring that sensitive data is not left in memory.
- Data validation must be performed on the application server.
- Nightly CCS Operations staff monitors batch production processing. The operations staff addresses any problems or ensures that the issues are communicated to others.

6. Distribution Of Output Reports/Introduction Or Release Of Data

- All hard copy reports created for use at the CCS must be protected commensurate with the sensitivity of the data they contain. When they are no longer needed, they should be disposed of properly -- for printouts that contain any sensitive data they should be shredded. (TBD)
- All printed material generated in the computer room that is retained there (alignment forms or damaged forms that have been reprinted) should be shredded prior to sending to recycling center (TBD) – (we need a shredder in our computer room area)
- Printed material that is destined for users is under lock and key until picked-up by authorized individuals, they are considered authorized if they have the access key to their report locker. These keys are strictly controlled by CCS's Facilities staff.
- Accounts payable checks are shipped to the accounting office via Intercampus Courier, they are locked in a courier pouch by the operations staff following processing, and the only keys for these pouches are held in the accounting office.
- The only data introduced to or released from the HP3K system is through CIS provided interfaces, that are built to adequately secure CCS's data from loss, corruption or inadvertent release.
- No data in any form is released to anyone without authorization by the data owner.
- The CCS firewall will be configured to block all incoming access to the Microsoft SQL Server service ports (1433/tcp, 1434/tcp) from outside the CCS network. (If the service is configured to listen on non-default ports, those ports will also be blocked at the firewall.)

7. Data And Program Backup

- System recovery media (tape, CD, floppy...) will be created and kept current so the system can be recovered to a known good state in the event of a system failure or compromise.
- System recovery documentation, outlining how to recover a system "from bare metal" will be available. (TBD)
- The recovery media and documentation will be stored in a location providing restricted access control, known to all systems administration staff, and be reasonably accessible in the event it is required.
- All backup media is stored in a vault in a separate building on campus.
- Backup cycles will vary by computer system, dependant on the nature of the computer's task and the data stored on the computer. The most typical backup scenarios are:
 - Full backups five nights a week
 - Partial backups as deemed necessary by administrative staff.
 - Full backups once a week -- disaster recovery of special purpose servers only.
- Restoring files from tape is an operation that may be performed only by system administration staff. Requests for restores are made in writing and are logged. (TBD)
- Backup media retention is generally as follows:
 - Monday-Thursday media cycles weekly
 - Friday media cycles every fourth week
 - End of month media cycles annually
 - End of year tapes are retained indefinitely

Media Protection

- All backup media is stored in a vault in a separate building on campus.
- All media is either stored in a vault or in the controlled access computer room.
- Media is destroyed in a controlled manner when no longer needed.
- Surplused disc's are erased and formatted at the lowest level.

8. Controls To Prevent Unauthorized Use Or Removal Of Media

Facility Access Control

Restricted Access IT Areas (Internal controls)

- Certain areas of the facilities will have restricted access. These restricted access areas are:
-

IS Network/Server/Computer Rooms	These rooms will be restricted by keypad and/or key access. Those having unescorted access will be limited to <u>authorized IS staff</u>
IS Offices	Access will be restricted by keypad and/or key access.
IS Work Areas	These areas are non-public work areas. Those having unescorted access will be limited to authorized IS staff. All doors external to these work areas will remain closed and locked at all times and will be restricted by keypad and/or key access.

Network and Phone closets	The network and phone closets across campuses will be restricted by ID card access. When possible, lockable cabinets within these rooms will be used to provide an extra layer of security. Outside vendors needing access to these areas will either be escorted by IT staff and/or Phone room staff.
Electrical closets	Each electrical closet on campus, as well as the main power distribution closet, will be restricted by traditional key access. Those having unescorted access will be limited to IS staff and directors and the Facilities Engineer. Outside vendors needing access to these areas will either be escorted by IS staff or check in with Campus Facilities to be temporarily issued a metal key, if authorized.

Access Controls -- Keys and Key Cards

- Keys, proximity cards, and/or access codes will be assigned to all authorized IS staff.
 - Their access rights will be determined by their affiliation with CCS as well as their specific job duties.
 - Access codes are to be treated like passwords and never shared with another person.
- Keys, proximity cards, and/or access codes will be assigned on an as needed, permanent basis to CCS employees only.
- All keys to Community Colleges of Spokane (CCS) facilities are the property of Community Colleges of Spokane. The CCS includes Spokane Community College (SCC), Spokane Falls Community College (SFCC), and the Institute for Extended Learning (IEL) and the District Offices (Dist).
- Keys shall be issued on a clearly defined “need” basis. Keys are considered to be tools necessary to complete assigned duties. Guidelines for determining the need for keys include the following:
 - Keys to CCS facilities may be assigned only to individuals with an official CCS affiliation; i.e. employees, students, contractors. No individual shall possess CCS keys that have not been appropriately issued to him/her. “Facilities” include buildings or portions of buildings under the control of the CCS, e.g. rental and leased buildings.
 - An employee with a continuing need to frequently access an area during the hours it is locked may be issued a key(s). Upon reassignment or termination of employment, keys will be returned to the immediate supervisor who shall return the keys to the Facilities Department.
 - An employee, student, vendor, or contractor with a temporary need to access an area during the hours it is locked may be issued a key(s) for the required period. Keys shall be returned to the Facilities Department at the end of the period.
- All keys shall be issued by the Facilities Department per procedure described in the District Key Control Administrative Procedures (See Appendix B- References)
- Keys shall be issued upon the proper completion of the Key Check-out form signed and dated by the key holder and appropriate approving authority .If additional keys are needed at a later date, an additional Key Check-out form shall be used for each request.
- Each building administrator is responsible for establishing and maintaining a key inventory and control system for keys issued to him/her. Each building administrator may designate a key coordinator who will be responsible for obtaining, issuing and reclaiming furniture and utility keys to doors and equipment that are the responsibility of the building administrator. The Facilities Department will be notified of all key coordinators. Key coordinators may sign the Key Check-out form on behalf of their department when receiving furniture and utility keys issued to their department. Key coordinators shall, in turn, keep a record of keys they issue to key holders so there is a complete record of each key issued. Departmental key records shall be audited periodically at the discretion of the district director of facilities.
- All keys (except furniture and utility keys) shall be issued to the key holder who will actually be using the key. No CCS key shall be loaned to an individual not authorized to use CCS keys. A key that is loaned is the responsibility of the individual who signed for and received the key.
- Keys shall not be transferred from the authorized key holder of record to another person.
- Key assignments, access codes and proximity cards will be reviewed no less than annually to assure that the assignments are still appropriate. Division/Department heads will review this report for their area and arrange for necessary key returns. Ideally, quarterly reviews should be done.(TBD)

- The loss of a key compromises the security of every door it accesses and shall be reported to the Facilities Department immediately.
 - Reissuance of a lost or stolen key requires the same approvals as described above for the issuing of keys.
- Upon separation from college employment, any employee will surrender to the Campus Facilities Department all keys and proximity cards that have been assigned. The employee's supervisor will ensure that the Campus Facilities department has been notified so that person's access code can be deactivated.
- Any students who have been authorized keys, but are not returning to the college for the next quarter, will turn in all keys and proximity cards before leaving the college.

Data Storage And Telecommunications Controls

Electrical Power and Backup Power

- All primary telecommunications/data rooms for each college will be provided filtered power as well as backup power via separate uninterruptible power system (UPS). The UPS will provide backup power for all servers in the computer rooms. Critical computers and network equipment not located in one of the two computer rooms protected by the building's UPS will need a local UPS.
- Designated staff will receive periodic training on responding to power failures. This training may be in the form of reviewing documentation instead of formal training.
- All network and telecommunications cabling is installed in ceilings, raceways or shielded according to DIS wiring and cabling standards.
- The CCS data center is equipped and wired to support a standby generator in the event of long term power failure. This system should be tested on an annual basis in conjunction with Facilities staff. (TBD)

Evacuation Planning and Building Safety

- Emergency information, including building evacuation plans will be posted in all computer classrooms, labs, offices, work areas and server rooms in compliance with CCS Public Safety policies and procedures.
- All designated work areas will be equipped with an emergency first aid kit.
- The evacuation plan will be tested in accordance to the CCS Emergency Management Plan.

Off-Site Media Storage

Data Storage

- All data center mainframe and server backup tapes are stored off-site in separate campus building in a fireproof vault. Tapes are rotated daily based on a rotation schedule outlined in the CCS Computer Operations Manual
- Any waste or discarded output (including such things as paper, tape) that contains sensitive data will be stored in a secure location until such time as it can be destroyed in compliance with the CCS IT Security Standard on Media Disposal.
- Sensitive documents (such as the college's AP check stock) will be stored only in the designated secured vault in the proximity of the data center.
- Media (paper, tape, fiche) being prepared for distribution to CIS will be maintained in the IS area until it is picked up by CCS Mail Services for CIS delivery.
- Storage media (for example; tapes, CD, diskettes) that have reached end of life (cannot be reused) are destroyed in a controlled manner by our facilities staff. The media to be disposed of is held in a controlled area until it is witnessed being destroyed by incineration.
- Backup and system recovery media must be stored in physically secure locations at all times. These include all copies stored locally as well as those at an off-site storage facility. Access to backup media must be restricted to Operations and Systems Administration staff.

10. Data Encryption Standards For Storage And Transmission

Data Encryption Algorithms

- Versign 128 bit certificates are installed on all servers that store and process confidential or sensitive data.
- Encryption routines used in CCS applications will be a generally accepted algorithm. Within the context of this standard, “generally accepted” means an open and published algorithm that has received extensive peer review and has no known weaknesses.
- Currently, CCS recognizes the following symmetric-key (or secret-key) algorithms as meeting this criteria:
 - Rijndael—also known as the Advance Encryption Standard (AES)—is the preferred algorithm.
 - Twofish, Blowfish, RC4, IDEA, CAST-256 are generally considered strong algorithms, and may be used if a specific situation warrants it, and Rijndael is inappropriate for the task.
 - Triple DES (3DES) may also be used, but should be phased out by 2005.
- Currently, CCS recognizes the following asymmetric-key (or public-key) algorithms as meeting this criteria:
 - RSA, using no less than 1024 bit keys, and DSA, using no less than 1024 bit keys, are the preferred algorithms.
 - Diffie-Hellman may also be used, if a specific situation warrants.
- Other generally accepted algorithms can be submitted to the CCS IT Security Administrator and/or Director of Information Resources for review and possible inclusion in the approved list of algorithms.

Key Management

- Management of keys, which are often the same as passwords, can present difficult problems. The CCS application developers are in the process of evaluating various solutions to support electronic signatures for locally developed applications.

Specific Tools and Protocols

- There are several common cryptographic applications that are, when used correctly, considered by the security community to be safe and of high quality. These tools will be used by CCS without further review. In all cases, key lengths will be specified to meet current cryptographic standards.
- Pretty Good Privacy (PGP) and its functional work-a-likes--OpenPGP and Gnu Privacy Guard (GPG).
 - These can be used for public or secret key encryption, as well as signing. Since PGP generally is used in a public key mode, key lengths will be at least 1024 bits.
 - Digital signing of legal/contractual documents for and with the State of Washington is under some cases controlled by RCW 19.34 and WAC 434.180. The uses considered here are for a more basic authentication of communications and other areas, not within the scope of the law.
- Secure Socket Layer (SSL) is the accepted standard for securing HTTP communications, although it can be used to secure other protocols as well.
 - Key lengths of 128-bit are considered acceptable for financial and personal data; key lengths less than that are no longer considered safe.
- Secure Shell (SSH) is the accepted standard for a secure replacement to telnet-like terminal access and ftp-like file copying.
 - SSH also has the ability to establish secure channels through which other TCP/IP protocols can be tunneled, like an ad-hoc VPN
 - Key lengths will be at least 1024 bits, and the SSH v.1 protocol will be disabled.
 - More information on the use of SSH at BCC can be found in the BCC IT Security Standard on SSH Configuration.
- IPSec is the IETF standard for encrypting and authenticating communications between two networked devices at the Internet Protocol (IP) layer of the network stack.

11. Processing Audit Trails

- Where appropriate, a user's activity within an application will be logged for later review.
- In the event of a fatal program error, an application will terminate gracefully. As appropriate, the program will assure that a log is created that contains as much useful post-mortem debugging information as possible.

12. System Access Violations

Indications Of A Potential Compromise

- The initial identification, or even suspicion, that a computer system may be compromised is not always clear-cut. There is a wide range of behaviors that might be indicators, but they are not definitive in most cases. These factors might include:
 - Unusually poor system performance
 - Unusually high and unaccounted for network traffic
 - Unusual open network ports
 - Unusual running programs
 - Unusual programs installed on disk
 - Unusual blue screen, CD drawer opening and closing, mouse moving around screen

While no one of these indicators is solid evidence of a compromised computer, any one of them could be the first sign of a compromise. If you notice these types of behaviors for a computer you are using, please mention it to the systems administrator for that computer system.

General Guidelines For Incident Response

- Gather, or at least notify and get instruction from, the appropriate people for the incident. This should include at least the Security Administrator and the Systems Administrator for the suspected device. It may also include application support staff, management, and others. Be sure to identify all the key players as early as possible.
- Document everything. Consider taping your comments. Note who did what, when, and why.
- Keep your head. Resist the tendency to overreact or panic. Methodically follow this Incident Handling standard.
- When communicating with others working on the incident, use out of band communication such as telephone, fax, and face-to-face communication. Your attacker may be able to listen in.
- Stay in constant communication across teams and with other impacted individuals.
- Avoid restarting the computer, logging on and off, or otherwise inadvertently starting malicious code. The programs on a compromised computer cannot be trusted.

Stage 1 – Make Initial Assessment

- 1.1 Ensure incident is not a false alarm.
- 1.2 Examine audit logs for unusual activity, absence of logs or gap in logs.
- 1.3 Look for attack tools (password cracking tools, Trojan horses, and so on.)
- 1.4 Check for unauthorized applications configured to start automatically.
- 1.5 Examine accounts for increased privilege or unauthorized group members.
- 1.6 Check for unauthorized processes.
- 1.7 Match compromised system performance against baseline.
- 1.8 Attempt to make a preliminary assessment of the nature, purpose, and extent of the compromise.
- 1.9 Assign an initial priority level (i.e., high, moderate, low) and an incident lead.
- 1.10 Determine if evidence will need to be preserved.
- 1.11 Communicate the incident to appropriate stakeholders and supporting staff. This may, depending on the nature of the incident, include Applications Support, K20 NOC, and CCS Management or even law enforcement.

Stage 2 – Protect Evidence

While chain of custody may not need to be rigorously followed in most incidents, creating a good system backup should be performed for any significant compromise. Some containment steps (Step 3) may be done in parallel with this step.

- 2.1 Back up systems with media never before used as early as possible in the incident response.
- 2.2 If possible, back up entire systems, including logs and system state.
- 2.3 Maintain provable chain of custody for evidence collected, if that is important.
- 2.4 Secure evidence and document who collected, how, when, and who had access to it.

Stage 3 – Contain The Damage And Minimize Risk

- 3.1 Depending on severity and security policy, isolate the affected systems by taking them offline.
- 3.2 Look for evidence of compromise on neighboring systems.
- 3.3 Change passwords on affected systems.

Stage 4 – Identify Type And Severity Of Compromise(S)

- 4.1 Determine type of attack and determine how it was accomplished.
- 4.2 Perform a system and network vulnerability analysis on the computer system to identify if there are other related or overlooked vulnerabilities that should be considered.
- 4.3 Determine probable intent of attack (specifically directed at your organization, automated attack, information gathering).
- 4.4 Identify all systems involved in attack. Revisit containment steps if additional systems are identified.
- 4.5 Reevaluate and, if necessary, reassign priority level to event.

Stage 5 – Notify External Agencies

- 5.1 Update management to ensure they have an accurate understanding of the incident and its status.
- 5.2 Under management, and possibly legal counsel direction, notify local and/or federal law enforcement.
- 5.3 Notify other appropriate agencies such as the CERT.

Stage 6 – Recover Systems

- 6.1 Determine how the computer system(s) should be recovered, with a complete reinstall or from backup.
- 6.2 Locate and validate most recent non-compromised backups or recovery media.
- 6.3 Recover the system.
- 6.4 Validate functionality and match system performance against historical baselines.
- 6.5 Verify that the vulnerability(s) that caused the incident has been adequately addressed.
- 6.6 Determine if it is acceptable to bring the computer system(s) back into production.
- 6.7 Monitor for repeat attack and for possible misconfiguration due to containment steps.

Stage 7 – Compile And Organize Incident Documentation

- 7.1 Compile all notes and records into a comprehensive security incident activity log.
- 7.2 Distribute to incident participants for review and approval.
- 7.3 Review cause of breach and improve defense to prevent it and related attacks in the future.
- 7.4 Assist finance department in assessing cost of breach.
- 7.5 Prepare report to management and other stakeholders to explain how the event occurred, the cost of the breach, and how it will be prevented in the future.

13. Intrusion Detection

- The initial point of contact for any suspected security breaches is the System Administrator for the affected CCS system. The CCS IT Security Administrator and Director of the IR unit responsible for the system should be notified immediately of a suspected incident. Systems Administrators should not hesitate to follow the appropriate steps detailed herein at the first indication of security breach.

Monitoring And Preventive Measures

- The primary responsibility for monitoring and for all preventive measures rests with the System Administrator for each networked server system.
- Events logs will be configured to monitor all network, server and computer activities. Systems Administrators will check these daily to determine if there are any unusual connections to any CCS systems.
- Twice weekly (more if a known threat exists) SMTP, IIS and FTP logs will be checked to identify any unusual occurrences for that week.
- All Internet Security and Acceleration (ISA) server logs will be checked weekly for any port probes.
- Port scans for known FTP, WWW and SMTP ports will occur at different times during the week to ensure no rogue servers are being operated on the network.

- Daily virus scans should be configured in accordance with the CCS IT Security Standards on Virus Protection.
- Probes for known Trojans on the network systems should be made quarterly. If new information on a specific Trojan is released, the System Administrator will do specific scans on those affected ports to determine risk levels. (TBD)
- Outbound traffic from all CCS switches will also be monitored and checked daily to determine any unusual and/or unexplainable traffic spikes.
 - If a particular workstation is broadcasting a great deal of traffic, the processes running on the system should be checked.
 - The system should be examined to determine if there is anything unusual about the configuration or setup of the system.
 - If appropriate, follow the Incident Response procedures outlined in this standard.
- If a particular external IP address has committed an offense, an attempt to track back to the point of origin will be made, the information recorded and appropriate steps followed as outlined in this standard.

14. Virus Protection

General

- Every network-enabled Windows server and desktop will have Antivirus (AV) software installed.
- Real-time virus protection will be enabled for servers, desktops, and mailboxes, thereby performing a proactive scan each time a new file or message is introduced onto any of the systems. This real-time protection will be configured so that the user cannot tamper with or disable it. (It is understood and accepted that System Administrators must from time to time disable AV software in order to perform certain tasks, such as installing some types of software.)
- Full scans of all mailboxes will be performed.
- Scheduled scans on the users' desktops must be performed no less than once a week and scheduled for during business hours, when the computer is expected to be on. (Note: These scans can be put into the background, by users, and not disrupt their work.)

Microsoft Exchange Servers

- As many of the latest viruses and worms have relied on email, Microsoft Exchange is also a significant component in controlling virus and worm outbreaks. In addition to the basic scanning described above, additional protection will be provided by having email scanned as it is sent and received (prior to delivery into the recipient's mailbox).
- Staff must show caution with regards to received email. If a message looks suspicious (the sender, the contents, the subject, whatever), it should be deleted from both the Inbox and the Deleted Items folders.

Maintenance Of The Antivirus Systems

- On a weekly basis, the pattern file on the master servers will be manually verified to assure it is current.
- Periodically spot-checks of other servers and desktops will be performed, to verify that they, too, have the most recent pattern file.

When A New Virus Is Spreading

- Check the major vendors' web sites to confirm that there is indeed a new virus. Avoid false alarms due to hoaxes when possible.
- If the rumor of a new virus is true, verify that the site is protected. Inform users in an appropriate manner, depending on the specifics of the incident.
- If the infection risk dictates, the Windows Systems Administration staff may also choose to protect systems by disconnecting from the network.

If The Site Becomes Infected

- If hit with an email virus, consideration will be given to taking the email server off the network until the Windows servers are clean. The CCS Windows Systems Administrators or the Security Administrators have the authority to make this call if management is not available.
- Upon virus analysis and agreement among the Technical Services Director, the Security Administrator, and the Windows Systems Administrator, if the virus is innocuous, the threat of spreading minimal and cleanup is easy, and then a cleanup may be performed instead of a rebuild.
- As a rule, infected workstations will also be rebuilt starting with a freshly formatted disk. Upon virus analysis, if the virus is innocuous, the threat of spreading minimal and cleanup is easy, and then a cleanup may be performed instead of a rebuild.

15. Control Of Interactive Internet Technology (TBD)

- Agency security training plan will include a discussion on the risks of downloading applets and other internet related threats. (TBD)
- Browser configuration will default to accepting applets from trusted servers only. (TBD)
- Firewall configuration will block the reception and distribution of applets as is appropriate for CCS needs. (TBD)
- CCS needs to implement systems administration audit procedures. (TBD)

16. Appropriate Disposal Of Hardcopy Data

- CCS's sensitive production data is frequently used for testing and/or training.
- Printouts with sensitive information will be shredded (TBD – We need a shredder) Note: Such printouts are currently stored in a secure location for pickup and properly destroyed.
- Any data shared with people outside CCS will be sanitized to protect its confidentiality.
- If data sanitation is not an alternative, the CCS IT Security Administrator and/or other appropriate member of college administration will approve the release of data to an entity outside of CCS.

17. Software Testing

- CCS's development efforts are striving for an enterprise development/testing environment but are limited by sever resource limitations. However a top priority is to develop safe, efficient and effective software solutions to local collage needs.

Amendments

Appendix A -- Change Log

Date	By	Version	Notes
10/01/03	T. Davenport	1.0	
10/21/03	D. Hol	2.0	

Appendix B – References

I.E.4 NETWORK AND TELECOMMUNICATIONS SECURITY

Introduction

The following information provides standards for developing, documenting and implementing the Network and Telecommunications aspects of a security program.

Scope

The scope of this standard documents the network and telecommunications controls related to Information Technology that address authorization, equipment approval, change control, and operational and physical security controls. These devices generally include such things as routers, hubs, firewalls and switches.

Throughout the following standards, the term desktop, when used, is defined as included Personal Computers, Laptops and MacIntosh PCs.

Standard

1. Network and Telecommunications Management

It is important to note that the technology support departments for each of the CCS units have centralized controls over all hardware, software and network configuration, installation and maintenance functions. The technical support staff for each of the four CCS units controls the receipt and installation of the following:

- PC's, printers, servers and mini-computers
- Controls for introducing new equipment to networks
- Management and distribution of all IP addresses
- Authorization and installation responsibility for all dial-up data lines.
- Management review and approval for changes and additions to the telecommunications network.
- Specific morning checklists to monitor network and system performance, unauthorized access and failures.

Application and network access is further secured by the following:

Password

- Choice of secure passwords and management of those passwords must adhere to the password standards outlined in IT Std. I.E.5a General Access Security.
- Backup copies of configuration files, which contain clear text passwords, must be protected from unauthorized access.

Services (TBD)

- SSL enabled HTTP (HTTPS) may be used for monitoring devices; if HTTPS is not supported by the device, HTTP may be used as a fallback. Management of devices via HTTPS is strongly discouraged. If HTTPS device management can be disabled independently of HTTPS device monitoring, it will be.
- Time synchronization should be maintained via NTP NTP updates should be authenticated.
 - The choice and management of authentication keys should follow the criteria defined in the Password Management standard.
 - The same key may be used on all devices in the network.
- Simple Network Management Protocol (SNMP)
 - Default community strings will never be used. Community strings, being effectively a password, will be chosen following the same criteria as defined in the Password Management standard.
 - All internal network devices may be configured to use the same community string.
 - All external border routers will use unique community strings.
 - SNMP updates will be disabled.

- Access Control Lists (ACL) to restrict access to device via SNMP, will be defined to allow access from a secure CCS network, the K20 NOC, and the colleges' own network (in the case of a college's border router).

2. Internetworking Servers

MPE Configuration

- The CCS HP 3000 Mainframe will be located in a server room that provides key card and/or keypad access, climate control, and an appropriate level of fire protection
- All server class computers (based on their function) will be located in a server room that is protected by keyed locks or key card access control, climate control, and some level of fire suppression.

Windows Server Configuration

- System builds will be performed with a supported version of Microsoft Windows. All security and recommended patch bundles will be applied.
- The computer will be configured so that it is included in the antivirus update scheme as determined by the Systems Administrator(s) in accordance with CCS IT security standard I.E.3 Data Security.

Web Server Configuration

Web Server

- There is a tremendous amount of commonality across web servers (e.g., Microsoft IIS and Apache), but there are also some distinct differences. This standard attempts to address web servers as a single class of applications, focusing on their commonality. Where there are specific platform differences, an attempt has been made to call those out.
 - When creating a web server, the systems administrator will follow the security best practices for configuration and management as defined by the vendor or user community for the given web server software.

User Access Controls and Confidentiality

- IP Address restriction will be used, where there are clearly delineated audiences, to control who may access a particular web site. This, however, is not a strong security device; if the function or content of the site is sensitive, address restrictions must be used only as a secondary security device.
- For applications that process user/customer or other sensitive data, data confidentiality protection will include:
 - SSL with 128 bit keys must be used
- If strong authentication is required, the site will use authentication layered on top of SSL encryption.

Web Server Logging

- Error and access logs of production web servers will be reviewed regularly to identify problems and attempted web server abuse (attacks). Ideally this should incorporate some level of automation for at least first-pass filtering.

Microsoft Mail Servers

- The Exchange accounts will be maintained with passwords as outlined in the IT Security Standard I.E.5a General Access Security Standard.
- On the directory (or drive) that Exchange is installed, its subdirectories, and the mapisrv.inf file, the following permissions will be set no looser than:

Domain Administrators	Full Control
SYSTEM	Full Control
Users	Read and Execute

- Anti-virus software will be used to scan incoming messages in real time as well as mailboxes.
- A current supported version of Exchange will be installed with its most current security related patches.
- To prevent being abused as an SMTP relay for UCE (i.e., SPAM), the Internet mail gateway (SMTP) will be configured to not reroute incoming SMTP mail except to other CCS hosts.

Network Time Services

- All CCS domain controllers will synchronize their time with the domain naming master at the forest root. Time updates from other sources will be ignored.
- Network devices (routers, switches, firewalls), that support time synchronization will use either CCS time server dist.spokane.cc.wa.us or the current domain naming master server

Firewall Logical Specification (TBD)

Backup and version control of the firewall configuration

- The firewall's configuration and rules (access control lists, or ACL) will be backed up onto a different server, other than the firewall itself, where they will be maintained as text files.
- Processor and file system security will be configured such that these files will have restricted access.
- On that server, these configuration file(s) will be backed up to the system backup tape on the processor's regular backup cycle.

3. Network Infrastructure Equipment

Access Controls

- The entrances to campus labs, offices and classrooms will be accessible to authorized staff via key twenty-four hours a day, 365 days a year. Any external doors to electronic classrooms and/or computer labs will not be unlocked unless an authorized faculty or staff member is present in the room, unless authorized by the CCS IT Security Administrator and/or the Director of Information Systems or authorized designee.
 - IS Network/Server/ Computer Rooms:
 - These rooms will be restricted by keypad and/or key access. Those having unescorted access will be limited to authorized IS staff
 - Network and Phone closets:
 - The network and phone closets across campuses will be restricted by ID card access. When possible, lockable cabinets within these rooms will be used to provide an extra layer of security. Outside vendors needing access to these areas will either be escorted by IT staff and/or Phone room staff.
 - Electrical closets:
 - Each electrical closet on campus, as well as the main power distribution closet, will be restricted by traditional key access. Those having unescorted access will be limited to IS and ITS staff and directors and the Facilities Engineer. Outside vendors needing access to these areas will either be escorted by IT staff or check in with Campus Facilities to be temporarily issued a metal key, if authorized.

Telecommunications Controls:

Fire Suppression

- Fire suppression equipment is provided for all the CCS Data Center. The fire suppression equipment is a type designated for computer and electronic equipment.
- Designated staff will receive periodic training on the use of the fire suppression equipment. (TBD)
- Smoke and fire detection devices should be located in each computer room and tied into the main fire alarm system.
- The fire detection and suppression systems should be inspected and tested at least annually.

Flood/Water Protection

- A water detection device is located on the true floor (beneath any raised floor) of the data center. This water detection device is monitored either via a separate alarm system that can be monitored by the IS department.
- Designated staff will receive periodic training on responding to a flood situation (typically a burst pipe). This training may be in the form of reviewing documentation instead of formal training.
- The water detection and control systems should be inspected and tested at least annually by a qualified technician. (TBD)

Climate Control

- All rooms containing computers will be provided with an adequate heating, ventilation, air conditioning (HVAC) system to assure computing equipment is maintained within its safe operating temperature.
 - Preferred operating environment is 68 - 77 degrees Fahrenheit at 40 - 60% humidity.
 - Network server rooms and switch rooms will be kept at a cooler temperature. The preferred operating environment in these rooms is 63 - 75 degrees Fahrenheit at 40 - 60% humidity.
 - If computer room temperature exceeds 79 degrees, Operations staff will continuously monitor the room's environment.
 - If computer room temperature exceeds 85 degrees, Operations staff will notify the HVAC vendor or the Facilities Engineer.
 - If the temperature continues to increase above 85 degrees computer room doors will be opened and fans will be deployed. As all access controls will have been disabled to address an emergency temperature condition, Operations staff will be responsible for closely monitoring access to the room.
- Designated staff will receive periodic training on responding to HVAC failures. This training may be in the form of reviewing documentation instead of formal training. (TBD)

Electrical Power and Backup Power

- All primary telecommunications/data rooms for each college will be provided filtered power as well as backup power via separate uninterruptible power system (UPS). The UPS will provide backup power for all mission critical servers in the computer rooms. Critical computers and network equipment not located in one of the two computer rooms protected by the building's UPS will need a local UPS.
- Designated staff will receive periodic training on responding to power failures. This training may be in the form of reviewing documentation instead of formal training. (TBD)
- All network and telecommunications cabling is installed in ceilings, raceways or shielded according to DIS wiring and cabling standards.
- The CCS data center is equipped and wired to support a standby generator in the event of long term power failure. This system should be tested on an annual basis in conjunction with Facilities staff. (TBD)

4. Data Transmission within Agency Intranet and Extranet

Configurations Specific to the CCS PIX Firewall (TBD)

- As is the default for the PIX, the stance that "that which is not explicitly permitted is denied" will be maintained.
- ICMP access beyond the DMZ (onto the internal network) will be restricted to the bare minimum to allow internal users to troubleshoot network connectivity.
- The various protocol fixup routines will be used with care, as they break some legitimate implementations of those protocols (SMTP as an example) or can generate huge amounts of log information (HTTP, SMTP for example).

Router Access Control Lists (ACL) for the K20 Border Routers

Basic access controls will be in place to provide rudimentary protection of the device itself, as well as protecting both the internal and the external networks from each other.

- Basic device protection will include allowing SNMP queries only from a defined secure CCS network and remote login access will be restricted to connections originating from a secure internal CCS network.
- Basic network protection will include blocking directed broadcasts to guard against being used as a SMURF relay.
- To prevent egress spoofing, ACL(s) will verify that all outbound packets have a source address that is from an internal network; if not it will be logged and dropped.
- To prevent ingress spoofing, ACL(s) will verify that all inbound packets have a valid source address. Address types that will be dropped and logged are: private address range (as defined by IANA), addresses on the internal network, local broadcast address, loopback address (127.0.0.0/8), and 0.0.0.0.
- Source routing will not be allowed.
- SNMP outbound from the college's network will be blocked at the K20 border router.

E-mail Transfers

- The most common method of data transfer is through the use of e-mail, usually as attachments. CCS has set up a secure e-mail system to provide communications access to the outside world. When any data from CCS is transferred in this manner, the following applies:
 - Only CCS-provided campus e-mail will be used. Personal e-mail accounts provided through servers outside CCS cannot be assumed to be secure in any manner, and will not be used to transfer CCS-sensitive information.
 - Any files being transferred will most likely be downloaded to a workstation and manipulated in some manner prior to attaching to an e-mail; therefore, care must be taken to protect the integrity and confidentiality of this data after it leaves the application server.

Web-based Transfer

- Web-based transfer tends to be a manual process, not well suited for automation. However, there are some federal agencies that use this methodology for submitting data on an annual basis (i.e., Social Security Administration, Internal Revenue Service, Immigration and Naturalization Services.) When any data from CCS is transferred in this manner, the following applies:
 - The data will be transferred over a Secured Socket Layer (SSL) encrypted link.
 - Any files being transferred will most likely be downloaded to a workstation prior to sending to the remote entity because this type of transfer is generally a manual, browser-based process.
 - Care will be taken to protect the integrity and confidentiality of this data after it leaves the application server (HP3000).
 - The data will not be stored on a shared drive and will be deleted from the workstation as soon as possible after the transfer.

Dial-in Transfers

- Dial-in transfers also tend to be a manual process, not well-suited for automation. When any data is being transferred from CCS in this manner, the following applies:
 - Since the CCS representative is dialing into a private network to transfer the file there is little inherent risk with the transfer itself.
 - Since this is a manual transfer; the file will most likely be downloaded to a workstation prior to sending to the remote entity.
 - Care will be taken to protect the integrity and confidentiality of this data after it leaves the application server (HP3000).
 - The data will not be stored on a shared drive and will be deleted from the workstation as soon as possible after the transfer.

Secure Shell (SSH) and File Transfer Protocol (FTP)

- Data may be exchanged (sent or received) with business partners via SSH or FTP, if the following criteria are met. SSH will be used at all times in preference to FTP. However, it is recognized this may not always be possible.
 - SSH transfers will be compliant with the CCS IT Security Standard on SSH Configuration.
 - Firewall rules will be configured to restrict access to the smallest range of IP addresses (ingress or egress) as possible.
 - Any account passwords required, either internally or those to be used by CCS personnel to log into an external entity's site will be managed in accordance with the CCS IT Security Standard on Password Management, recognizing that the external entity also has policies and procedures to be respected.

College User VPN Access: (TBD)

Staff VPN Access to CCS Internal Network (general)

- Connectivity to the CCS internal network via a VPN is not a "right" conferred on staff with employment, but rather a privilege CCS makes available. With the use of VPN connectivity, CCS staff will recognize the responsibilities assumed when they, in effect, connect a home workstation into the network. These include:
 - Connection from outside the college network into the secure CCS network will be through the VPN server

- The CCS employee's home workstation will have current, high-quality antivirus software installed and running. Further, virus pattern files will be updated and full disk scans performed at least once a week.
- The CCS employee is expected to install on a home workstation all security patches appropriate for the workstation's software bundles in a timely manner and will stay current with other operating system and application patches.
- The CCS employee's home workstation is subject to all applicable CCS, CIS, and DIS networking security and acceptable use policies while connected to the CCS network via the VPN.
 - Internet connectivity during a VPN session is provided by CCS.
- One very common use of VPN connectivity is to access files and data stored at CCS.
 - Staff will use extreme care to assure both the confidentiality and integrity of this data as it is easily transferred to a home workstation's hard disk, even without intending to do so.
 - Whenever possible, this data will not be transferred to the employee's home workstation's hard disk, but will rather be accessed on the CCS storage device (e.g., drive, directory, or folder) where it resides.
 - If data must be copied to the home workstation, it will be carefully protected while it is on that computer and deleted from the home workstation as soon as possible.

5. Remote Access to Applications in these Areas

Documentation of Firewall Rules (TBD)

- The CCS IT Security Administrator will maintain documentation of the firewall rule-set. This documentation entitled "Firewall Logical Specifications" (Confidential) will include:
 - The characteristics and expected usage of each firewall interface.
 - The design goals for each interface's rule set (i.e., a logical design).
 - The specific rules to implement that design, by interface.
 - Explanation and documentation on each exception to that design.
- Change control logs will be maintained with the Firewall Logical Specifications (Confidential) documentation defining who made a change request, when it was made, when it was implemented, and the rationale for that change.

6. Physical Network Infrastructure

Access Controls

- Certain areas of the facilities will have restricted access. Some of these rooms are numbered, but are otherwise unidentified as to purpose and not specifically marked as secure areas. These restricted access areas are:

IS Network/Server/Computer Rooms	These rooms will be restricted by keypad and/or key access. Those having unescorted access will be limited to <u>authorized IS staff</u>
IS Offices	Access will be restricted by keypad and/or key access.
IS Work Areas	These areas are non-public work areas. Those having unescorted access will be limited to authorized ITS and IS staff. All doors external to these work areas will remain closed and locked at all times and will be restricted by keypad and/or key access.
Network and Phone closets	The network and phone closets across campuses will be restricted by ID card access. When possible, lockable cabinets within these rooms will be used to provide an extra layer of security. Outside vendors needing access to these areas will either be escorted by IT staff and/or Phone room staff.
Electrical closets	Each electrical closet on campus, as well as the main power distribution closet, will be restricted by traditional key access. Those having unescorted access will be limited to IS and ITS staff and directors and

	the Facilities Engineer. Outside vendors needing access to these areas will either be escorted by IT staff, or check in with Campus Facilities to be temporarily issued a metal key, if authorized.
--	---

7. Secure Location of Communications Equipment to Prevent Theft and Tampering

- The entrances to campus labs, offices and classrooms will be accessible to authorized staff via key twenty-four hours a day, 365 days a year. Any external doors to electronic classrooms and/or computer labs will not be unlocked unless an authorized faculty or staff member is present in the room, unless authorized by the CCS IT Security Administrator and/or the Director of Information Systems or authorized designee.
 - IS Network/Server/ Computer Rooms:
 - These rooms will be restricted by keypad and/or key access. Those having unescorted access will be limited to authorized IS staff
 - Network and Phone closets:
 - The network and phone closets across campuses will be restricted by ID card access. When possible, lockable cabinets within these rooms will be used to provide an extra layer of security. Outside vendors needing access to these areas will either be escorted by IT staff and/or Phone room staff.
 - Electrical closets:
 - Each electrical closet on campus, as well as the main power distribution closet, will be restricted by traditional key access. Those having unescorted access will be limited to IS and ITS staff and directors and the Facilities Engineer. Outside vendors needing access to these areas will either be escorted by IT staff, or check in with Campus Facilities to be temporarily issued a metal key, if authorized.

8. Terminal, Remote Job Entry, and network node (bridges, routers, etc.) access security (including Telnet, RLOGIN, GDP, etc

Console and Terminal Access

- Clear text protocols will be avoided and will be completely phased out eventually.
- Physical access to the device must be tightly controlled.
- Remote access to these devices must be restricted to a small number of computers on a secure internal network.
- Login banner must clearly state that systems are monitored, that unauthorized access is not allowed, and must not provide information as to equipment type, OS type, or version. (See the Login Banner standard (TBD)

Dial-in Access and Modems

- Limited modem access will be supported to enable remote support, principally after hours.
- Logins originating from a modem will require an additional Terminal password. This password will be defined and managed in accordance with the CCS Security Standard for Password Management.

Windows System Configuration:

Physical Security:

- All server class computers (based on their function) will be located in a server room that provides: traditional key/and or key card access control, climate control, and some level of appropriate fire suppression.
- Windows workstations located at the user's desk will all be configured to require a user id and password upon login.

Services:

- Most of the common "business" services (such as DNS, Web, Email, and Databases) will have CCS security standards defined specifically for them. The general principal, is to configure the computer with the fewest services possible

MPE System Configuration:

Services:

While many of the "standard" Internet services will run on the HP3000 under MPE, most of those services are not necessary or are incompatible with the purpose of the processor. Minimal network services will be allowed for inbound connections.

- Standard MPE networking protocols will be configured. These include: Remote File Access (RFA), Remote Process Management (RPM), Virtual Terminal (VT), Network File Transfer (NFT), NS Information Request (NSIR).
- Additional protocols are to be configured to support CCS developed Applications. These include: Web Transaction Server (for Student and Personnel services) and Transporter.
- Third party applications or OS options may also perform network functions. These include: SRN Degree Works, By Request (WRQ FFT), and fairly standard printing protocols (Printer, NetPrint, and JetDirect). Additions to this list will need to be reviewed and will initially be treated as exceptions.
- FTP service will not be allowed, as it completely bypasses the computer's security system. Note: This is in reference to FTP acting as a server or listening process accepting login requests, not FTP running as a client connecting from the HP3000 computer to a remote host.
- All other network services (i.e., inbound to the HP3000) will be treated as an exception and must be documented as defined above.

9. Controls to Prevent Unauthorized Programs in to Computer Systems

Audit/Assessment of Firewall (TBD)

- At least annually, the CCS Security Administrators will review the implemented firewall configuration and ACL files against the firewall rule set documentation. The administrator will verify:
 - The ACL matches the documented rules.
 - The rules and exceptions are still valid and consistent with best practices, policy, and business needs.
 - The change control processes are being followed.
 - Develop a plan to address any discrepancies and recommend any improvements to the configuration or rules that seem appropriate.
- An external audit of the firewall implementation and management procedures will be performed every three years, in addition to this internal assessment. (It is envisioned that this would be part of the regular audit from the State Auditors Office).

Windows System Configuration:

- System builds will be performed with a supported version of Microsoft Windows. All security and recommended patch bundles must be applied.
- The computer will be configured so that it is included in the CCS antivirus update scheme.

Windows Virus Protection:

General

- Every network-enabled Windows server and desktop will have antivirus (AV) software installed.
- Real-time virus protection will be enabled for servers, desktops and mailboxes, thereby performing a proactive scan each time a new file or message is introduced onto any of the systems. This real-time protection will be configured so that the user cannot tamper with or disable it.
 - It is understood and accepted that System Administrators will from time to time disable AV software in order to perform certain tasks, such as installing some types of software.
- Full scans of all mailboxes will be performed.
- Scheduled scans on users' desktops will be performed no less than once a week and scheduled during business hours when the computer is expected to be on. These scans can be run in the background to lessen disruption to work.

- Laptops that are not regularly powered up and connected to the network to receive updates will regularly be updated and scanned by Computer Support personnel.
- Each AV "master" server will check for pattern file updates daily. When new pattern files are received, they will be pushed to all other servers and desktops. All of this will be automated.
 - The client will be configured to check its master server at scheduled intervals to see if there is a new pattern file. (This two-way approach -- the server pushes and the client pulls -- provides a simple fail-over mechanism in case one side is not working properly.)
 - The client will be configured to produce a pop-up message if the pattern file is older than 30 days.

Microsoft Exchange Servers

- As many of the latest viruses and worms have relied on email, Microsoft Exchange is also a significant component in controlling virus and worm outbreaks. In addition to the basic scanning described above, additional protection will be provided by having email scanned as it is sent and received (prior to delivery into the CCS recipient's mailbox).
 - All CCS employees must show caution with regards to received email. If a message looks suspicious (the sender, the contents, the subject, whatever), it should be deleted from both the Inbox and the Deleted Items folders.
 - The AV software will also disable unsafe macros (specifically auto-start macros) in attachments.

Maintenance of the Antivirus System

- The master servers will be configured to automatically update the pattern file on a daily basis. On a weekly basis, the pattern file on the master servers will be manually verified to assure it is current.
- Periodically spot-checks of other servers and desktops will be performed, to verify that they have the most recent pattern file.

When a New Virus Is Spreading

- Check the major vendors' Web sites to confirm that there is indeed a new virus. Avoid false alarms due to hoaxes when possible.
- If the rumor of a new virus is true, verify that the site is protected. Inform users in an appropriate manner, depending on the specifics of the incident.
- If the CCS networks or workstations are not currently protected and the threat is significant, a member of the systems administration staff will go into "monitoring mode," checking the pattern file site at least every half hour until it can be downloaded and pushed out to the servers and workstations.
- If the infection risk dictates, the appropriate Systems Administrator or CS technical support supervisor may also choose to protect systems by disconnecting them from the network.

If the Site Becomes Infected

- If hit with an email virus, consideration will be given to taking the email server off the network until the Windows servers are clean. The CCS Systems Administrators and/or the CCS IT Security Administrator have the authority to make this call if no Director or Dean is available.
- As a rule, infected servers will be rebuilt starting with a freshly formatted disk. Upon virus analysis and agreement among the technician responsible for the system, the CCS IT Security Administrator and the Systems Administrator, if the virus is innocuous, the threat of spreading minimal and cleanup easy, then a cleanup will be performed instead of a rebuild.
- As a rule, infected workstations will also be rebuilt starting with a freshly formatted disk. Upon virus analysis—if the virus is innocuous, the threat of spreading minimal and cleanup easy—then a cleanup will be performed instead of a rebuild.

Unix System Configuration:

- There are minimum Unix installations at CCS. Where necessary, security patches will be installed as quickly and safely as possible for all OS and application security vulnerabilities the computer might be exposed to.

- Recommended patches will be regularly installed on the computer unless vendor applications prevent staying current on patches.

11. Network Breach Detection and Incident Response

Indications of a Potential Compromise

- The initial suspicion or identification of a compromised computer system is not always easily apparent. There are a wide range of behaviors that might serve as problem indicators, but in most cases they are not definitive. These factors might include:
 - Unusually poor system performance.
 - Unusually high and unaccounted for network traffic.
 - Unusual open network ports.
 - Unusual running programs.
 - Unusual programs installed on disk.
 - Unusual blue screen, CD drawer opening and closing, mouse moving around screen.
 - Sluggish or non-responsive network access (Web sites do not display quickly or at all).
- While none of these indicators is solid evidence of a compromised computer, any one of them could be the first sign of a problem. If a user notices these types of behaviors for a computer being used, the college or I.S. Help Desk is to be contacted so the behavior can be referred to the appropriate Systems Administrator.

Incident Response

- As no two incidents are alike, each step listed may not apply to each event. Before dropping any step, the responding technical support personnel will be sure it is appropriate to alter the procedures and that the elimination of one step will not jeopardize later steps in the investigation.

General Guidelines

- Notify the appropriate people for the incident. This will include at least the Systems Administrator for the suspected device, the appropriate supervisor, the CCS IT Security Administrator and/or the Director of Information Systems. . It may also include technical support staff, management and others, as necessary. Identify all of the key players as early as possible.
- The Systems Administrator for the suspected device will take the lead in handling the incident and in instructing other staff regarding the immediate response needed. Upon resolution of the incident, a written report will be made to a CCS IT Security Administrator, the Director of Information Systems, and the appropriate administrator.
- Stay in constant communication across teams and with other impacted individuals.
- Avoid restarting the computer, logging on and off, or otherwise inadvertently starting malicious code. Remember, the programs on a compromised computer cannot be trusted.

Stage 1 – Make Initial Assessment

- Ensure incident is not a false alarm.
- Examine all system and security audit logs for unusual activity, absence of logs or gap in logs.
- Look for attack tools (password cracking tools, Trojan horses, etc.)
- Scan network for known compromises.
- Check for unauthorized applications or services configured to start automatically.
- Examine accounts and groups for increased privilege or unauthorized group members.
- Check for unauthorized processes and services.
- Match compromised system performance against baseline system performance.
- Attempt to make a preliminary assessment of the nature, purpose, and extent of the compromise.
- Assign an initial priority level (i.e., high, moderate, low).
- Determine if evidence will need to be preserved for a potential criminal investigation.

- Communicate the incident to appropriate personnel. This may, depending on the nature of the incident, include CCS Management and law enforcement.

Stage 2 – Protect Evidence

- While chain-of-custody may not be essential in most incidents, creating a good system backup will be performed for any significant compromise. Some containment steps (such as Step 3) may be done together with this step.
 - As early as possible in the incident response, back up systems with media never before used.
 - If possible, back up the entire system, including logs and system state.
 - If critical, maintain documented chain-of-custody for evidence collected.
 - Secure evidence and document who collected, how, when, and who had access to it.

Stage 3 – Contain the Damage and Minimize Risk

- Depending on severity and, in accordance with CCS's IT Security Policy, isolate the affected systems by taking them offline. This will be done by physically removing the network connection, isolating the system in a private network, or shutting the system down. Shutting the system down will be the last resort if the system is compromised as it may be difficult to track the root of the problem once it has been restarted.
- Look for evidence of compromise on neighboring systems.
- Change passwords on affected systems

Stage 4 – Identify Type and Severity of Compromise(s)

- Determine the type of attack and how it was accomplished.
- Perform a system and network vulnerability analysis on the system to identify if there are other related or overlooked vulnerabilities to be considered.
- Determine probable intent of attack (specifically directed at CCS, automated attack, information gathering or probing).
- Identify all systems involved in the attack. Repeat containment steps if additional compromised systems are identified.
- Reevaluate and, if necessary, reassign priority level to event.

Stage 5 – Notify External Agencies

- Update the CCS IT Security Administrator, the Director of Information Systems, and appropriate administrators to ensure they have an accurate understanding of the incident and its status.
- After consulting with CCS management, notify legal counsel, who may notify local and/or federal law enforcement, as appropriate.
- Notify other appropriate agencies, such as the CERT Coordinating Center (http://www.cert.org/reporting/incident_form.txt), as appropriate.

Stage 6 – Recover Systems

- Determine whether damaged systems should be recovered with a complete reinstall or from backup.
- Locate and validate most recent non-compromised backups or recovery media.
- Recover the system.
- Validate functionality and match system performance against historical baselines.
- Verify that the vulnerability (ies) that caused the incident are adequately addressed.
- Determine if it is acceptable to bring the computer systems back online.
- Monitor for repeat attack and for possible mis-configuration due to the steps taken during the containment process.

Stage 7 – Compile and Organize Incident Documentation

- Compile all notes and records into a comprehensive security breach activity log.
- Distribute documents to incident participants for review and approval, as appropriate.

- Review cause of breach and improve defense to prevent it and related attacks in the future.
- Prepare report to management and other stakeholders to explain how the event occurred, the cause of the breach, and how it will be prevented in the future, as required by the impact of the incident.

12. Remote Access Services

College Administrative User VPN Access to HP 3000:

- CCS will only give a unique group's authentication to access the HP3000. These users will be currently defined and have security access forms on file for this additional access.

Off-Campus Access:

- A user connects from the home workstation to the VPN server and enters a username and password.

Staff VPN Access to CCS Internal Network:

- Connectivity to the CCS internal network via a VPN is not a "right" conferred on staff with employment, but rather a privilege CCS makes available. With the use of VPN connectivity, CCS staff will recognize the responsibilities assumed when they, in effect, connect a home workstation into the network.

Off-Campus Access:

- The workstation VPN endpoint, via the assigned group membership, will be allowed to connect to the CCS internal network.

Electronic Mail Configuration

Mail Client Software:

- Considering the almost exclusive use of Microsoft Outlook at CCS, the majority of this standard will focus on security concerns of that software. The client is the last in a chain of defenses against email borne attacks. Some of the configuration options specified here can be rigorously enforced, but many rely on the cooperation of the person using the client.
 - Outlook will be maintained with the most recent security patches. The check for level-one attachments, as defined in Microsoft's security bulletin Q235309, may be altered to be more permissive or disabled. Disabling the level-one attachment check places additional responsibility for proper "email hygiene" on the email recipients.
 - The CCS staff will make themselves aware of the dangerous attachment file types as defined by Microsoft.
 - Outlook will be configured to use the Microsoft Internet Explorer "Restricted Zone" to minimize the risks associated with malicious executable content, such as ActiveX controls, Java, and JavaScript.
 - Microsoft Office Macro Protection will be configured to allow execution of signed macros from trusted sources.
 - Current Anti-Virus software will be maintained and used on each computer system
 - Users with administrator rights will use their non-administrator account to access email.

General Mail Architecture and Management:

- Outlook provides the capability to allow a user to grant access to their mailbox to another user. While this may be necessary in a few well-defined cases, CCS staff will be strongly discouraged from using this feature.
- Upon separation, email accounts will be deleted or deactivated for a finite amount of time. In the case of the latter, the mailbox may be copied from the former employee to a new or existing employee upon request of the Vice President of Human Resources.
- Access to the email service will be restricted to Systems Administrators for whom this is a defined part of their duties. The email administrator is, from time to time, required to view messages in the message store to investigate or address mail system failures, perform maintenance, or investigate security incidents. If administrators notice evidence of activities that is either unlawful or in violation of policy, they will be required to bring the matter to the attention of a director. Otherwise, the administrators are expected to keep the information confidential.

13. Wireless Communications

General

- All access to CCS networks through wireless means will require the same compliance for password-controlled access and for appropriate use as does any wired connection.
- Wireless connections are made available to those areas of a campus that are remote and difficult to connect via conventional wiring systems. Wireless connections are available for faculty, staff, administrator and student lab use.
- All wireless users will meet the expectations for appropriate use as described in the CCS Acceptable Use Policy.

Non CCS-owned Workstation

- Currently, CCS does not support wireless connection for student owned laptops. This has been discussed to some degree, but additional security measures and standards will need to be developed and agreed to by CCS Tech Support staff and administration.

14. VPN Methodology

Staff VPN Access to CCS Internal Network

- Connectivity to the CCS internal network via a VPN is not a "right" conferred on staff with employment, but rather a privilege CCS makes available. With the use of VPN connectivity, CCS staff will recognize the responsibilities assumed when they, in effect, connect a home workstation into the network. These include:
 - Connection from outside the college network into the secure CCS network will be through the VPN server
 - The CCS employee's home workstation will have current, high-quality antivirus software installed and running. Further, virus pattern files will be updated and full disk scans performed at least once a week.
 - The CCS employee is expected to install on a home workstation all security patches appropriate for the workstation's software bundles in a timely manner and will stay current with other operating system and application patches.
 - The CCS employee's home workstation is subject to all applicable CCS, CIS, and DIS networking security and acceptable use policies while connected to the CCS network via the VPN.
 - Internet connectivity during a VPN session is provided by CCS.
 - One very common use of VPN connectivity is to access files and data stored at CCS.
 - Staff will use extreme care to assure both the confidentiality and integrity of this data as it is easily transferred to a home workstation's hard disk, even without intending to do so.
 - Whenever possible, this data will not be transferred to the employee's home workstation's hard disk, but will rather be accessed on the CCS storage device (e.g., drive, directory, or folder) where it resides.
 - If data must be copied to the home workstation, it will be carefully protected while it is on that computer and deleted from the home workstation as soon as possible.

15. VPN Solutions must use Industry Standard Protocols

- All connections through VPN will be logged.

16. VPN solution through a CCS Firewall

- VPN solutions that connect to the CCS network through a firewall will be configured by a technical support staff person.
- A user connects from the home workstation to the VPN server and enters a username and password.
- The VPN server will give the user a local IP within the authorized range and connect them to the CCS network resources.

17. VPN Solutions using Smartcards

Not Applicable: Currently CCS does not operate a VPN solution that involves token-based technology.

Amendments

Appendix A -- Change Log

Date	By	Version	Notes
10/20/03	M. Hall	1.0	
10/21/03	D. Hol	2.0	

Appendix B – References

I.E.5A GENERAL ACCESS SECURITY

Introduction

This standard defines specific procedural and configuration elements for allowing general access to computing resources under control of CCS IT units. This standard should be reviewed, at minimum, on an annual basis.

Scope

This standard defines the steps needed to develop, document, and implement a security program component for access security controls over networks, servers and workstations. CCS units do not ordinarily deploy stand-alone workstations and we define client/server PCs as an internetworked computer. This definition was reviewed with the state auditor's office and found acceptable. This standard will document the access security practices at CCS as they relate to both technology categories. *Hardened passwords* will be used whenever technically and operationally feasible. Appropriate user training should be considered regarding the physical protection of hardened passwords that may be more difficult to remember. For those systems for which it would be technically infeasible, or which would require modification to meet this requirement as defined below, agencies must document the system, and the limitation involved.

Standard

1. Access Security Controls

A. Mainframe (HP3000)

This section will document the current security program in-place to safeguard the "mainframe" computing resources of the Community Colleges of Spokane (CCS's HP3000).

Physical Security:

- The HP3000 is located in an always locked, environmentally controlled computer room (raised floor).
- The building is locked during non-business hours
- The ISD department is locked at all-times and access is controlled by a digital lock (provides logging of entry) as well as department staff.
- Once inside the ISD area there is a "fire wall" with a locked door to the data distribution area.
- The computer room is then accessed from the data distribution area via a combination door lock (not logged)
- The computer room is served by the building fire alarm system; there is no fire suppression system.
- The under-floor is wired to sound an alarm if water is detected.
- All distributed media is accessible only by ISD staff and the staff person(s) designated by the various user areas (key access)
- The ISD computer room is not identifiable from the "street".
- The HP3000 is protected from "dirty" electrical power by both a Transient Voltage Surge Suppression (TVSS) device and 18KVA UPS device. In addition the computer room facility can be supplied (the circuits and devices are in place) with electricity by a portable generator.
- The HP3000 computer system is fully backed-up every evening/early morning during the week; all weekend work is backed up Monday night.
- Non-ISD staff can gain access only with ISD staff cooperation. The one exception is that facilities people (custodians and other building maintenance staff) have access at all times to all spaces. This access is controlled by the Facilities department and is outside of our control.

Dial-up Access:

- Dial-up access is provided via a single in-coming phone line.
- The dial-up number is not published anywhere.
- All logons are logged.
- The dial-up connection is audible and will be detected.
- The dial-up port is configured to not allow console access via dial-up nor can the system be “rebooted” remotely.
- Once a dial-up connection is established the system and application security measures come into play; document in the following sections.

System Logon Access:

- System access requires successful logon via a third-party security system (Security-3000, provided by Vesoft Inc). Sec-3000 is the premiere security enforcement tool in the HP3000 environment.
- Operating System prompt access is only available to a limited number of ISD staff the support staff from the CIS. All other users logon and are directly placed in a menu system that enforces Application Access authentication steps (documented in the next section).
- Current password rules being enforced systematically by Security-3000 on CCS’s HP3000 “mainframe” are:
- Passwords must be at least 5-characters in length (Sec-3000 is case insensitive)
- Passwords must be changed every 60-days (10-days of expiration notice)
- Passwords can not be reused for 180 days
- Users will be deactivated after 3-failed login attempts
- Security-3000 provides a “BadPassword” utility to reject too commonly used words
- All logons that have “SM” (System Manager) rights also require an user/account password (these passwords have no systematically enforced rules) but are well regulated by the HP3000 System Administrator.
- All “streams” (batch job initiation) are logged
- All “logons” are logged. Plus a daily report of logon failures are reviewed by the HP3000 System Administrator to see if there are any signs of intrusion attempts.
- Users deactivated by Security-3000 can only be reactivated by HP3000 System Administration staff and then only after the users identity is satisfactorily authenticated to the Admin staff person.\
- Dial-up access can not acquire the “Console” (device specific operator/admin rights)

Application Access:

- User access authentication to gain access to our administrative system is documented in agonizing detail in our “Security” manual see Appendices.
- Please note that we have an issue with using SCAN access codes as application logon passwords that needs to be addressed to comply with state standards (TBD)

B. Client Server

Individual User Accounts

- All individuals using the CCS networks or computing resources will have an authorized account and password to access the systems. This includes all full-time and part-time faculty, and staff.
- Individual user accounts are requested from the IT authority for the employee unit, by the supervisor or designee, of the individual to be issued the user account.
- The username and temporary password will be provided to the requesting authority, for relay to the applicable individual.
- Individual user accounts will not be shared among two or more individuals.
- Individuals will be issued one (1) individual user account for access to all CCS network resources, including e-mail systems.
- Individual user accounts will have access set according to the *least privilege principle*.

- In the case of staff termination or separation, the employee supervisor is responsible for contacting the unit IT authority, and ensuring the user account is disabled or deleted.

Multi-user Accounts (*Generic User Accounts*)

- When the use of *individual* user accounts is not technically or operationally feasible, a user account will be created for use by multiple users. Examples: Student work-study users, accounts to gain access to systems in student labs, training areas, and multi-user teaching facilities.
- A person responsible for the appropriate use of each multi-user account will be identified and documented. The responsible person must be a full-time or part-time faculty or staff employee.
- The multi-user username and password will be provided to the person responsible for the use of the account, and for supervision of the facility where the account is used.
- Multi-user accounts will be limited to use on appropriate systems, by logon restriction, system policy, or other measure to ensure the multi-user account is used in the intended facility, on appropriate systems, for the intended purpose.
- Use of multi-user accounts should be restricted to the operating hours of the facility where the account is used.
- If possible account restrictions must be systematically imposed.
- Multi-user Accounts will have access set according to the *least privilege principle*.

Service Accounts

- Service accounts will be created for applications and services which require them
- Service accounts will be limited to use on appropriate systems, by logon restriction, system policy, or other measure to ensure the service account is used on appropriate systems, for the intended service.
- Service Accounts will have access set according to the *least privilege principle*.
- Service accounts should be restricted from logging on interactively.
- Service accounts should be segregated by the security needs of the system.

Administrator Accounts

- If possible built-in administrator accounts will be used to perform administrative functions.
- Administrator equivalent accounts will only be created for specific operational or technical purposes.
- Built-in administrator accounts will not be used as service accounts. If a service account with administrative rights is required, an administrator equivalent account will be created for the service to use.

Other Accounts

- Built-in guest accounts will be disabled.

C. Security Groups

Administrative security groups

- Individual user accounts will not be members of *domain administrator* security groups. This applies even if the individual user has responsibility for domain administration functions. The administrator account, rather than the user account will be used for those functions.
- User accounts should not be members of *local administrator* security groups, unless required for a specific technical or operational purpose, and no other alternative exists.

Other security groups

- Membership in other security groups will be set for user accounts and service accounts according to the *least privilege principle*.

2. Passwords

A. Mainframe Passwords

The HP3000 logon security is currently not configured to meet the “hardened” password requirements and is unlikely to be able to systematically enforce all the criteria specified (TBD). Current password rules being enforced systematically by Security-3000 on CCS’s HP3000 “mainframe” are:

- Passwords must be at least 5-characters in length (sec-3000 is case insensitive)
- Passwords must be changed every 60-days (10-days of expiration notice)
- Passwords can not be reused for 180 days
- Users will be deactivated after 3-failed login attempts
- Security-3000 provides a “BadPassword” utility to reject too commonly used words
- All logons that have “SM” (System Manager) rights also require an user/account password (these passwords have no systematically enforced rules) but are well regulated by the HP3000 System Administrator
- All “streams” (batch job initiation) are logged
- All “logons” are logged. Plus a daily report of logon failures are reviewed by the HP3000 System Administrator to see if there are any signs of intrusion attempts.
- Users deactivated by Security-3000 can only be reactivated by HP3000 System Administration staff and then only after the users identity is satisfactorily authenticated to the Admin staff person
- Dial-up access regardless of “logon” can not acquire the “Console” (device specific operator/admin rights)

B. Client Server

Individual User Passwords

Note: CCS intends to implement the DIS standard for hardened passwords with the exception of those units that have Macintosh computers installed on campus. There are technical limitations that do not allow us to support the DIS standard. Please note the following explanation:

The Microsoft UAM for Macintosh has a limitation regarding the length of a password that can be changed by a user using a Macintosh and the Microsoft UAM. Passwords set or changed using the Microsoft UAM which are longer than 7 characters fail when a subsequent attempt is made to logon to a Windows computer (as in attach to a server).

If the password policy on a Microsoft network is set to require a minimum password length of 8 characters, users on Macintosh clients using the Microsoft UAM will not be able to successfully change their password.

Therefore, in a mixed Macintosh and Windows environment, the minimum password length must be set to 7 or less, and Mac users must be counseled not to attempt to use a password longer than 7 characters.

We can demonstrate this problem if you want to see it for yourself. Our current policy is as follows.

Minimum password length = 5 characters. Macintosh users are advised to make passwords at least 5 characters long, but not longer than 77.

- If possible user passwords should be a minimum of 8 characters long .
- User passwords must not be shared between two or more individuals.
- User passwords must be changed a minimum of every 120 days.
- If possible user level passwords should conform to *hardened password*, or *strong password* specifications.

Administrator Passwords

- Administrator passwords must conform to *hardened password*, or *strong password* specifications.
- Administrator passwords must be changed a minimum of every 120 days.
- Administrator or equivalent passwords which are compromised will be changed immediately.
- The same password will not be used on more than one administrator, or administrator equivalent account, or service account.

- Administrator passwords will not be used on other non-administrative accounts or service accounts.

Service Account Passwords

- If possible service account passwords must conform to hardened password, or strong password specifications.
- The same password will not be used on more than one service account.
- Service account passwords which are compromised will be changed immediately.

Multi-user Passwords

- Multi-user passwords will be changed upon request, or when misuse has occurred.
- Users of Multi-user passwords can not change the passwords. Only a system administrator or account operator can change the password on a multi-user account.

Temporary Passwords

- Temporary passwords can be used to gain initial access to a system by a new user.
- Temporary passwords can only be used once.
- The same temporary password should not be issued for use on more than one user account.

Training

- New users should complete a computing orientation, including general access security information, prior to receiving a user account.
- All faculty and staff should complete recurring training on password selection and management, and general data security procedures.

3. Additional Requirements

A. Dial-up Lines

- Limited modem access will be supported to enable remote support, principally after hours.
- Logins originating from a modem will require an additional terminal password. This password will be defined and managed in accordance with the CCS IT Security Standard on Password Management.
- Dial-up access must be authorized on a per-user, or remote access policy basis.
- Remote access clients must not be allowed to connect without authentication.

B. Lock-out Mechanisms

Mainframe

MPE System configuration:

- No more than nine consecutive incorrect login attempts (password attempts) will lock an account. A Systems Administrator will be the only one who can unlock it. Appropriate warning banners will be displayed at login, per the standards defined in the CCS IT Security Standard on Login Banners.

Password Management

- An automatic “lock-out” mechanism will be in place and will be activated after a maximum of five (5) unsuccessful authentication attempts.

Client Server

- Lock out mechanisms should be used to disable account logon after 5 unsuccessful logon attempts.
- Lockout mechanisms will not be used on built-in administrator accounts.

C. Protecting Scan Codes

- It has been the policy of CCS since we started issuing SCAN Authorization codes and SCAN Plus cards that all information pertaining to the codes and cards be kept in a secure location, i.e., locked file cabinet.
- We have also informed employees at the time of issue that the SCAN Authorization codes are for their exclusive use and are not to be shared with other employees.

D. Recording Telecom Access

Mainframe

- The Security 3000 log report is reviewed on a daily basis by the system administrator.
- System logging will be enabled for at least the following events:
 - Interactive and batch logins and logouts.
 - Password changes.
 - System startup, shutdown, and power failure.
 - System logging configuration and management.
 - Hardware diagnostic messages.
- Security issues will be reported to the Computer Services Manager or Director of I.S.

Client/Server

- Compile all notes and records into a comprehensive security breach activity log.
- Review cause of breach and improve defense to prevent it and related attacks in the future.
- Prepare report to management and other stakeholders to explain how the event occurred, the cause of the breach, and how it will be prevented in the future, as required by the impact of the incident.

E. Monitoring Vendor Access

Vendor Access to CCS Systems

- Vendors may, in the performance of their contractual obligations for support services, require access to computer systems managed and maintained by CCS. As a general principle, this access will only be granted as required, will be extremely restrictive, and will be carefully monitored.
- Generally, the vendor will not be given system administrator (or equivalent) privileges. Any access granted to the computer system(s) will provide the vendor's support person the least security privilege required to accomplish any task(s).
- Vendor access will be for a defined and short duration, usually the length of time required to address the specific support incident. After the completion of the task, access will be disabled.
- If a vendor is given access to "standard" accounts (with a password that is shared among support staff) on a computer system, that password will be changed after the vendor completes the work. If the account is especially sensitive, and/or the access requirements are extended in time, the password will be changed more frequently.
- Software installations and/or upgrades to be installed by a vendor will be clearly documented and reviewed by the appropriate Systems Administrator responsible for the resource prior to granting access. This review will occur early in the planning phase, but no later than prior to the coordinating the access to perform the work. If necessary, the CCS IT Security Administrator and/or the Dean of Information Resources will be brought into the planning process.

Terms

Multi-user Account, Generic User Account

- An account name and password combination, known or made known and used by many, for access to specific systems. Example: Systems installed in public areas of a library, or student computing centers.

Least privilege principle

- States that an account may only have the access roles required to perform specific required functions of the user or service, and no more.

Hardened password, strong password

- A password at least 8 characters in length and containing 3 of 5 complexities (uppercase letters, lowercase letters, numeric characters, special characters, non-ASCII characters), and not containing any portion of the username, or the user's full name.

Domain Administrator Privilege, Rights

- Right to administer a network domain, or network-wide objects and resources, including user accounts, computer accounts, services and security access control lists.

Local Administrator Privilege, Rights

- Right to administer objects and resources on a specific computer system or device, including local user accounts, services and security access control lists.

Limitations

- Macintosh clients using operating system version 9 or earlier, and using the Microsoft User Authentication Module (UAM) can not create or change hardened or strong user passwords as defined in this document.
- Macintosh clients using operating system version 9 or earlier, and using the Apple User Authentication Module (UAM) can not create or change hardened or strong user passwords as defined in this document.
- Macintosh servers using operating system version 9 or earlier can not create or change hardened or strong administrator passwords as defined in this document.
- Adjunct faculty not using campus-based computers, and retrieving e-mail from home computers using the POP3 protocol, cannot change their user password when it expires.
- Suitable opportunities to train new and existing users do not exist.

Amendments

Appendix A -- Change Log

Date	By	Version	Notes
10/19/03	T. Davenport	1.0	
10/20/03	R. Larse	2.0	
10/21/03	D. Hol	3.0	

Appendix B – References

- CCS HP 3000 Application Security Manual

I.E.5B INTERNET ACCESS SECURITY

Introduction

This standard describes the risks and security considerations for the use of the Internet for access to applications and data. The risks involved in pursuing e-government applications require that appropriate authentication and access control determines a party's right to the data.

Scope

This standard will focus on a risk assessment for all Internet based applications run by CCS staff and students based on applications developed by CIS, Information Systems (referred to as the district office), SCC, SFCC and the IEL. In addition a number of access security attributes will be examined and documented for each of the application groups outlined below.

Standard

1. *Web Admissions (provided by the CIS):*

CCS uses a Web-based application, Web Admissions, which has been developed by CIS for use by the 34 Washington State community and technical colleges. Web Admissions, is a fairly stand-alone Cold Fusion application which is implemented as a single shared instance of IIS on Windows 2000 at the CIS for all colleges.

1. **Information is public** - Much of the information presented, collected, or managed by CCS is considered sensitive. Some information, like employee earnings history might be considered public record. Other information, such as student records, is protected by FERPA and is considered confidential.
2. **Documented Risk Issues** -
 - a. *The potential impact of viewing data by unauthorized intruders* – If a person were able to gain unauthorized access, this would capture admissions data submitted by a student. This data could then be used in various illegal acts, deleted, or modified. As there is no significant financial data available via this application, and each application provides independent audit ability, damage would likely be limited to disclosure of personal information
 - b. *The potential impact of unauthorized viewing of data by otherwise legitimate users* – The viewing of data by a legitimate user who is not authorized to view the data could result in the misuse of the data and would be a violation of the FERPA law and college policy.
 - c. *The potential impact of the use of the information assets for other than authorized purposes* – Again, the potential impact of using the information assets would be for the selling or disclosure of student admissions information.
 - d. *The potential impact of unauthorized deletion, modification, or disclosure of information* – The result of unauthorized deletion would result in the student not being admitted to the college. Modification of information would result in misinformation going into admissions data, or being sent to an incorrect location. Disclosure of student data without the student's consent would be a FERPA violation.
 - e. *The potential operational impact if the service becomes unavailable (denial of service attacks)* - Each system provided on the Web is redundant with systems available through traditional terminal access or touch-tone telephone access. Consequently, denial of service does not present a substantial risk since students apply for admissions in person, by mail, or at any college terminal.
 - f. *The potential public confidence impact if the services or data provided by the system are compromised* – The impact on public confidence if the server at CCS was compromised, in and of itself, would probably not be measurable. The real risk associated with loss of public confidence is if the data was

compromised as in “d.” above. Potential new students could not use the Web applications admission which would result in loss of student enrollments.

- g. *The importance of non-repudiation (inability of a user to deny the initiation of a transaction) to the transactions support by the system* – Non-repudiation is not currently an issue with the types of transaction now being performed via Web-based admission applications.
 - h. *The impact of an intrusive registration and authentication process on the potential user base of the application* – If access to CCS’s Web application form required an intrusive registration and authentication process, the result would be a delay in student admissions and an increase in staff workload. This could result in the potential loss of students wanting to apply for admissions to CCS.
 - i. *The application impact on the potential user base to one-time and ongoing authentication costs* – There are no one-time and/or ongoing authentication costs; therefore, there is no impact by CCS’s Web admissions application on the end user.
3. **Assessed User Base** – The user-base of the Web-based admissions application process that CIS provides to CCS is potential students. Single sign-on is not seen as a significant aid to this application.
 4. **Selected Identity Confidence Level** - Identification and authentication are performed via a traditional user ID and password.
 5. **Use Transact** – CCS and CIS do not use Transact for any application. Identification and authentication are performed via a traditional user ID and password.
 6. **Request for Mechanism** – The users request and create their own "account" the first time they use the application. As this is simply a Web implementation of a paper-based admissions process, identification is really a part of the (manual) audit of the user-entered admissions form.
 7. **Initial Identification** – Within the application, the users are fully trusted to identify themselves. As this is simply a Web implementation of a paper-based admissions process, verification of identity is really a part of the (manual) audit of the user entered admissions form
 8. **User Agreement** – There is no user agreement within this application.
 9. **Issuance Procedures** – The user is issued an account as the first step in using the application.
 10. **Revocation** – The only means of revocation once the admissions form is submitted is for the user to request an authorized CCS support person to manually deactivate the user’s account.
 11. **Suspension** – The only means of suspension once the admissions form is submitted is for the user to request an authorized CCS support person to manually deactivate the user’s account.
 12. **Renewal** – The user may renew the account by creating a new one.
 13. **Protection of Mechanism** – A user-created User-ID and Password protects the account. All of the user’s data is maintained in a secured database.
 14. **Obligations and Liabilities** – As stated in “1.” above, CCS is obligated to protect the confidentiality of the data as delineated in the FERPA law.
 15. **Validation Process** – Authentication is performed via a user-supplied User-ID and Password pair.
 16. **System Configuration** – The Web server and hosting operating system are configured in compliance with the CCS IT Security Standards on Windows Base System Configuration and Windows Server Configuration.
 17. **Network Configuration** – The associated network devices are configured in compliance with the CCS IT Security Standard on Network Device Configuration.
 18. **Firewall Configuration** - The firewall is configured in compliance with the CCS IT Security Standards on Firewall Change Management and Firewall Logical Specification (Confidential).
 19. **Intrusive Detection** – Intrusion into the servers supporting the Web admission form is monitored and addressed in compliance with the CCS IT Security Standard on Intrusion Detection and Incident Response.
 20. **Audit Procedures** – Each application (submitted by a user) is manually audited by CCS’s Admissions Office to assure that the information is correct and truthful to the extent possible.

2. Web Transaction Server (WTS) (provided by the CIS)

CCS uses a Web-based application, Web Transaction Server (WTS), which has been developed by CIS for use by the 34 Washington State community colleges. The Web Transaction Server is a fairly stand-alone Cold Fusion application which is implemented as a single shared instance of IIS on Windows 2000 at the CIS for all colleges.

1. **Information is public** - Much of the information presented, collected, or managed by CCS is considered sensitive. Some information, i.e., employee earnings history, might be considered public record. Other information, such as student records, is protected by FERPA and is considered confidential.
2. **Documented Risk Issues** -
 - a. The potential impact of viewing data by unauthorized intruders – If persons were able to gain unauthorized access they would be able to capture student and employee data. This data could then be used in various illegal acts, be deleted, or modified. As there is no significant financial data available via this application and each application, provides independent audit ability, damage would likely be limited to the disclosure of personal information.
 - b. The potential impact of unauthorized viewing of data by otherwise legitimate users – The viewing of data by a legitimate user who is not authorized to view the data could result in the misuse of the data and would be a violation of FERPA and college policy.
 - c. The potential impact of the use of the information assets for other than authorized purposes – Again, the potential impact of using the information assets would be for the selling or disclosure of student and employee information.
 - d. The potential impact of unauthorized deletion, modification, or disclosure of information – The result of unauthorized deletion would result in the student no longer being in our database. Modification of information would result in misinformation going into the student or employee records. Disclosure of student data without the student’s consent would be a FERPA violation. Disclosure of employee data is a violation of college policy.
 - e. The potential operational impact if the service becomes unavailable (denial of service attacks) - Each system provided on the Web is redundant with systems available through traditional terminal access or touch-tone telephone access; therefore, denial of service does not present a substantial risk.
 - f. The potential public confidence impact if the services or data provided by the system are compromised – The impact on public confidence if the servers at CCS were compromised, in and of itself, would probably not be measurable. The real risk associated with loss of public confidence is if the data was compromised as in “d.” above. Students and employees would feel less secure that CCS can protect their personal information and/or even that the information is accurate.
 - g. The importance of non-repudiation (inability of a user to deny the initiation of a transaction) to the transactions support by the system – Non-repudiation is not currently an issue with the types of transaction we are now being performed via Web-based applications.
 - h. The impact of an intrusive registration and authentication process on the potential user base of the application – If access to CCS’s WTS required an intrusive registration and authentication process the result would be a delay in student registration and other processes and an increased workload for staff. This item does not seem applicable to our situation.
 - i. The application impact on the potential user base to one time and ongoing authentication costs – There are no one time and/or ongoing authentications costs; therefore, there is no impact. This item does not seem applicable to our situation.

If a person were able to gain unauthorized access to data at level 0, confidential data could be viewed. At level 2, confidential information could be changed and/or stolen. At level 3 confidential data could be viewed, stolen for misuse, deleted or modified. As there is no significant financial data available via these applications, and each application provides independent audit ability, any damage would likely be limited to disclosure of personal information.

3. **Assessed User Base** – The user base of the Web-based applications the CIS provides to CCS includes several classes of users: a) registered students, and staff, b) Faculty, and staff, and c) Employees, and staff. Within the context of the WTS application, the user does have single sign-on. While a broader level of single sign-on might be beneficial, especially in the case of employees, the CCS and the CIS are outside the boundaries of Transact Washington. It should be noted, however, that with the scheduled re-hosting of these applications, the whole authentication architecture will be reviewed.
4. **Selected Identity Confidence Level** - Identification and authentication are performed via a traditional user ID and password
5. **Use Transact** – CCS and CIS do not use Transact for any application. Identification and authentication are performed via a traditional user ID and password.
6. **Request for Mechanism** – Accounts for users are created automatically (when user is a student, faculty, or staff) and their login information is mailed to them.
7. **Initial Identification** – The users have previously identified themselves to the college (as an employee or student).
8. **User Agreement** – There is no user agreement within this application.
9. **Issuance Procedures** – The account login information is issued to new users at periodic intervals (per CCS’s defined schedule) and mailed to the account holder.
10. **Revocation** – The only means of revocation is for CCS to change the user’s PIN.
11. **Suspension** – The two means of suspension are 1) CCS puts a block (unusual action flag) on the user's account, preventing the user from updating data (e.g., registering), and, 2) CCS changes the user's PIN, preventing all user access.
12. **Renewal** – The concept of renewal does not really fit with these applications. Student accounts last forever (to access transcripts for example). If a PIN is forgotten, CCS can manually reset it.
13. **Protection of Mechanism** – A user created User-ID and Password protects the account. All of the user’s data is maintained in a secured database.
14. **Obligations and Liabilities** – As stated in “1.” above, CCS is obligated to protect the confidentiality of the data as delineated by FERPA.
15. **Validation Process** – Authentication is performed via a user-supplied User-ID and Password pair.
16. **System Configuration** – The Web server and hosting operating system are configured in compliance with the CCS IT Security Standards on Windows Base System Configuration and Windows Server Configuration.
17. **Network Configuration** – The associated network devices are configured in compliance with the CCS IT Security Standard on Network Device Configuration.
18. **Firewall Configuration** - The firewall is configured in compliance with the CCS IT Security Standards on Firewall Change Management and Firewall Logical Specification.
19. **Intrusive Detection** – Intrusion into the servers supporting the Web admission form is monitored and addressed in compliance with the CCS IT Security Standard on Intrusion Detection and Incident Response.
20. **Audit Procedures** – Various exceptions and transaction reports are available to CCS to assist in assuring the appropriate use of the WTS applications.

3. CCS Public Web Sites (Dist, Iel, Scc, Sfcc)

1. **Information is Public** – All information presented by the CCS public Web sites is intended for public dissemination.
2. **Documented Risk Issues** –
 - a. The potential impact of viewing data by unauthorized intruders – The only risk of unauthorized viewing of public Web site data is related to those responsible for posting information to the sites intentionally or inadvertently placing sensitive information on those sites.
 - b. The potential impact of unauthorized viewing of data by otherwise legitimate users – There is no adverse impact of unauthorized viewing of public Web site data by legitimate users unless those responsible for posting information to the sites intentionally or inadvertently place sensitive information on public sites.
 - c. The potential impact of the use of the information assets for other than authorized purposes – Because the data posted to CCS's public Web sites is intended for use by the general public, there are essentially no unauthorized purposes possible for which the information asset may be used. If the public Web servers were to be hacked, there is a potential for the sites to be used for other than authorized purposes.
 - d. The potential impact of unauthorized deletion, modification, or disclosure of information – The impact of unauthorized deletion or modification of the information contained in the CCS public Web sites, whether intentional or not, is very significant, and could cause considerable loss and harm to CCS. Disclosure of the information contained in the CCS public Web sites has no risk as it is intended for public dissemination.
 - e. The potential operational impact if the service becomes unavailable (denial of service attacks) – If the services offered by the CCS public Web sites become unavailable through denial of services attacks, the operational impact is significant. This could result in loss of revenue, dissatisfaction of those to whom CCS provides services, interruption of productive work, and a loss of institutional reputation.
 - f. The potential public confidence impact if the services or data provided by the system are compromised – If the services or data provided by the CCS Web sites are compromised, there will be a significant impact in the level of confidence the public can place on the information provided through the Web. This could also result in loss of revenue, dissatisfaction of those to whom CCS provides services, interruption of productive work, and a loss of institutional reputation.
 - g. The importance of non-repudiation (inability of a user to deny the initiation of a transaction) to the transactions support by the system – Non-repudiation does not apply to the type of transactions provided by the CCS public Web sites as the sites are open to the public and do not require any authentication. The only transactions taking place are the requests by browser software for pages identified by URL and the response by the Web servers to broadcast that information for display by the browser.
 - h. The impact of an intrusive registration and authentication process on the potential user base of the application – If access by the community to the CCS public Web sites was required to have an intrusive registration and authentication process, the user base would be a drastically reduced percentage of the potential user base. It would, in fact, limit use of the sites to virtually none.
 - i. The application impact on the potential user base to one-time and ongoing authentication costs – There are no one-time and/or ongoing authentications costs, therefore there is no impact by the CCS public Web sites on the potential user base of those resources at this time.

Mitigation of Risk – All documented risks identified in relation to CCS public Web sites are mitigated by the approval processes identified in the CCS IT Security Standards on Web Servers and the CCS policy on Acceptable Use. In addition, safeguards addressed in numerous standards limit outside access to CCS Web servers. The CCS IT Security Standard on Intrusion Detection and Incident Response addresses prevention and response to the wrongful seizure or unlawful exercise of authority over the legitimate use of the asset. (TBD)

Some areas documented above identify a significant risk of considerable loss and harm to CCS. However, the use of the Web provides significant communication and access to information. It is such an important part of fulfilling the educational and administrative missions of the college that whatever risks exist in the use of these resources is minor in comparison with their positive business impact.

3. **Assessed User Base** – Because they are fully accessible to the public, the user base expected to utilize the CCS public Web sites is unlimited, both in numbers and in diversity. There is no authentication of any type required. Authentication is not seen as a possibility in the future, nor would authentication be considered a significant security enhancement of the sites. Web sites at CCS which require authentication, such as the Intranet, etc., are not considered publicly accessible and do not fall within the parameters of the systems being addressed.
4. **Selected Identity Confidence Level** – The user base of the CCS public Web sites have not been identified as being unique, nor is there an authentication process or mechanism associated with the system. Therefore, it appears that identifying confidence level processes does not apply to this system.
5. **Use Transact** – The use of Transact does not apply to the CCS public Web sites.
6. **Request for Mechanism** – Because no accounts are necessary to access the CCS public Web sites, no request mechanism is required.
7. **Initial Identification** – The CCS public Web sites do not utilize initial identification processes for users.
8. **User Agreement** – There are no user agreements associated with the CCS public Web sites.
9. **Issuance Procedures** – Because no accounts are necessary to access the CCS public Web sites, no authentication mechanism issuance or acceptance procedures are required.
10. **Revocation, Suspension, Renewal** – Because no accounts are associated with access to the CCS public Web sites, no authentication mechanism revocation, suspension, or renewal procedures are required.
11. **Protection of Mechanism** – Because no authentication mechanism is in place for the CCS public Web sites, no protection procedures for such mechanisms are required.
12. **Obligations and Liabilities** – CCS has the obligation to ensure that data placed on the CCS public Web sites is appropriate for public dissemination and is liable for the disclosure of protected data insofar as federal, state, and local sanctions exist protecting such data.
13. **Mechanism Validation Process** – Because no authentication mechanism is required for the CCS public Web sites, no validation of such mechanisms is required.
14. **System Configuration** – The Web servers and hosting operating system for all CCS public Web sites are configured in compliance with the CCS IT Security Standards on Windows Base System Configuration, Windows Server Configuration, Macintosh Base System Configuration, and Macintosh Server Configuration.
15. **Network Configuration** – The network devices associated with the CCS public Web sites are configured in compliance with the CCS IT Security Standard on Network Device Configuration.
16. **Firewall Configuration** – The firewall protecting the servers supporting the CCS public Web sites is configured in compliance with the CCS IT Security Standard on Firewall Change Management.
17. **Intrusion Detection** – Intrusion into the servers supporting the CCS public Web sites is monitored and addressed in compliance with the CCS IT Security Standard on Intrusion Detection and Incident Response.
18. **Audit Procedures** – Each CCS public Web site is evaluated, approved, and periodically audited for compliance with the CCS IT Security Standard on Web Space Usage.

4. District Web Applications

1. **Information is Public** – Some CCS District application data is intended for and is available to the general public (e.g. Staff Directory). Other application data is intended for use by the CCS as an institution and is considered the “private” information of the staff, student or potential student and is protected as such. Each application is designed to offer the minimum level of access based on the authentication credentials of the application user(s). Most authentications are based on SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
2. **Documented Risk Issues** –
 - a. The potential impact of viewing data by unauthorized intruders – If persons were able to gain unauthorized access, they could possibly interfere with student and staff access to CCS online application. A less likely risk would be the potential capture of private information (ID, address, birth date, etc.). Damage would likely be limited to an interruption in access and the disclosure of personal information. The applications with monetary consequences (e.g. Travel, Timesheets and Leave Forms) are audited by appropriate personnel in the Finance offices of CCS.
 - b. The potential impact of unauthorized viewing of data by otherwise legitimate users – The viewing of data by a legitimate user who is not authorized to view it could result in the misuse of the data. Viewing the data by an unauthorized but legitimate viewer would be a violation of the FERPA law and college policy.
 - c. The potential impact of the use of the information assets for other than authorized purposes – Again, the potential impact of using the information assets would be the disclosure of private information and the potential interruption in access to online application functions.
 - d. The potential impact of unauthorized deletion, modification, or disclosure of information – The result of unauthorized deletion or modification could result in lost or “corrupted” data. Most likely would be a mere nuisance for the affected individuals and support staff, but should not result in direct monetary loss. Disclosure of private data without the appropriate consent would result in the violation of the FERPA law and is addressed by state and national statutes.
 - e. The potential operational impact if the service becomes unavailable (denial of service attacks) – If the services offered by the CCS web based applications become unavailable through denial of services attacks, the operational impact is significant. This could result in loss of revenue, dissatisfaction of those to whom CCS provides services, interruption of productive work, and a loss of institutional reputation.
 - f. The potential public confidence impact if the services or data provided by the system are compromised – If the services or data provided by the CCS based applications is compromised, there will be a significant impact in the level of confidence that our online students and staff can place on the information provided. This could also result in loss of revenue, dissatisfaction of those to whom CCS provides services, interruption of productive work, and a loss of institutional reputation.
 - g. The importance of non-repudiation (inability of a user to deny the initiation of a transaction) to the transactions support by the system – Non-repudiation could be a factor with Travel and Time reporting functions. However, due to the level of human involvement at various steps of the processing it would be unlikely to more severe than causing some confusion.
 - h. The impact of an intrusive registration and authentication process on the potential user base of the application – If access to CCS web applications required a more intrusive registration and authentication process the result would be a delay in accessing the online tools. It would also increase staff workload. This would result in the potential loss of student enrollments in CCS classes due to dissatisfaction, or unnecessary staff stress leading to a disruptive level of staff turnover.
 - i. The application impact on the potential user base to one-time and ongoing authentication costs – There are no one-time and/or ongoing authentications costs at this time. (TBD – What the ????)

Mitigation of Risk – The processes identified in the CCS IT Security Standard on Windows Server Configuration mitigate many of the documented risks identified in relation to CCS Web Applications. In addition, safeguards are addressed in numerous standards limit outside access to the CCS application server. The CCS IT Security Standard on Intrusion Detection and Incident Response addresses prevention and response to the usurping of the legitimate use of the asset. (TBD)

Some areas documented above identify a significant risk of considerable loss and harm to CCS. However, the use of the Web for online applications provide significant communication and access to information, and is such an important part of fulfilling the educational and administrative missions of the college. Whatever risks exist in the use of these resources is minor in comparison with their positive business impact.

3. **Assessed User Base** – The user-base of the CCS District web application processes would be new and returning SCC/SFCC/IEL students, faculty, staff and in some cases the general public.
4. **Selected Identity Confidence Level** – Identification and authentication is performed mostly via a traditional user ID and password authentication using SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
5. **Use Transact** – The use of Transact does not apply to the CCS District web applications.
6. **Request for Mechanism** – Where required is provided via the assignment of SID and PIN to students and staff. Applications available to the general public do not require authentication and should be considered public information being made available via a database driven application not unlike a static public information web page.
7. **Initial Identification** – Identification and authentication is performed mostly via a traditional user ID and password authentication using SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
8. **User Agreement** – There is no user agreement beyond FERPA requirements of those staff that work with student information.
9. **Issuance Procedures** – Where required is provided via the assignment of SID and PIN to students and staff.
10. **Revocation, Suspension, Renewal** – The only means of revocation once the SID and PIN is created is for an authorized CCS support person to manually deactivate the user’s account.
11. **Renewal** – Not an issue at this time.
12. **Protection of Mechanism** – A user-maintained Password (PIN) protects the account. All of the application data is maintained in a secured database.
13. **Obligations and Liabilities** – As stated in “1.” above, CCS is obligated to protect the confidentiality of student data as delineated in the FERPA law.
14. **Validation Process** – Identification and authentication is performed mostly via a traditional user ID and password authentication using SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
15. **System Configuration** – The CCS Application server and hosting operating system is configured in compliance with CCS IT Security Standards on Windows Base System Configuration and Windows Server Configuration. This is basically adhering to the industries “best practices”.
16. **Network Configuration** – The associated network devices are configured in compliance with the BCC IT Security Standard on Network Device Configuration.
17. **Firewall Configuration** - The firewall is configured in compliance with the CCS IT Security Standards on Firewall Change Management and Firewall Logical Specification (Confidential). (TBD)
18. **Intrusion Detection** – (TBD)

19. **Audit Procedures** – Currently no “formal” audit procedures (similar to the HP3K annual security audit) are implemented for web based applications. (TBD)

5. SCC Web Applications

1. **Information is Public** – Some SCC application data is intended for and is available to the general public (e.g. public information on the SCC web site). Other application data is intended for use by the SCC as an institution and is considered the “private” information of the staff, student or potential student and is protected as such. Each application is designed to offer the minimum level of access based on the authentication credentials of the application user(s). Most authentications are based on SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
2. **Documented Risk Issues** –
 - a. The potential impact of viewing data by unauthorized intruders – If persons were able to gain unauthorized access, they could possibly interfere with student and staff access to SCC online application. A less likely risk would be the potential capture of private information (ID, address, birth date, etc.). Damage would likely be limited to an interruption in access and the disclosure of personal information.
 - b. The potential impact of unauthorized viewing of data by otherwise legitimate users – The viewing of data by a legitimate user who is not authorized to view it could result in the misuse of the data. Viewing the data by an unauthorized but legitimate viewer would be a violation of the FERPA law and college policy.
 - c. The potential impact of the use of the information assets for other than authorized purposes – Again, the potential impact of using the information assets would be the disclosure of private information and the potential interruption in access to online application functions.
 - d. The potential impact of unauthorized deletion, modification, or disclosure of information – The result of unauthorized deletion or modification could result in lost or “corrupted” data. Most likely would be a mere nuisance for the affected individuals and support staff, but should not result in direct monetary loss. Disclosure of private data without the appropriate consent would result in the violation of the FERPA law and is addressed by state and national statutes.
 - e. The potential operational impact if the service becomes unavailable (denial of service attacks) – If the services offered by the SCC web based applications become unavailable through denial of services attacks, the operational impact is significant. This could result in loss of revenue, dissatisfaction of those to whom SCC provides services, interruption of productive work, and a loss of institutional reputation.
 - f. The potential public confidence impact if the services or data provided by the system are compromised – If the services or data provided by the SCC based applications is compromised, there will be a significant impact in the level of confidence that our online students and staff can place on the information provided. This could also result in loss of revenue, dissatisfaction of those to whom SCC provides services, interruption of productive work, and a loss of institutional reputation.
 - g. The importance of non-repudiation (inability of a user to deny the initiation of a transaction) to the transactions support by the system – Non-repudiation in general is probably not a significant issue within the SCC provided applications.
 - h. The impact of an intrusive registration and authentication process on the potential user base of the application – If access to SCC web application required a more intrusive registration and authentication process the result would be a delay in accessing the online tools. It would also increase staff workload. This would result in the potential loss of student enrollments in SCC classes due to dissatisfaction, or unnecessary staff stress leading to a disruptive level of staff turnover.
 - i. The application impact on the potential user base to one-time and ongoing authentication costs – There are no one-time and/or ongoing authentications costs at this time. (TBD)

Mitigation of Risk – The processes identified in the CCS IT Security Standard on Windows Server Configuration mitigate many of the documented risks identified in relation to SCC Web Applications. In addition, safeguards are addressed in numerous standards limit outside access to the SCC application

server. The CCS IT Security Standard on Intrusion Detection and Incident Response addresses prevention and response to the usurping of the legitimate use of the asset. (TBD)

Some areas documented above identify a significant risk of considerable loss and harm to SCC/CCS. However, the use of the Web for online applications provide significant communication and access to information, and is such an important part of fulfilling the educational and administrative missions of the college. Whatever risks exist in the use of these resources is minor in comparison with their positive business impact.

3. **Assessed User Base** – The user-base of the SCC web application processes would be new and returning SCC/SFCC/IEL students, faculty, and staff and in some cases the general public.
4. **Selected Identity Confidence Level** – Identification and authentication is performed mostly via a traditional user ID and password authentication using SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
5. **Use Transact** – The use of Transact does not apply to the SCC web applications.
6. **Request for Mechanism** – Where required is provided via the assignment of SID and PIN to students and staff. Applications available to the general public do not require authentication and should be considered public information being made available via a database driven application not unlike a static public information web page.
7. **Initial Identification** – Identification and authentication is performed mostly via a traditional user ID and password authentication using SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
8. **User Agreement** – There is no user agreement beyond FERPA requirements of those staff that work with student information.
9. **Issuance Procedures** – Where required is provided via the assignment of SID and PIN to students and staff.
10. **Revocation, Suspension, Renewal** – The only means of revocation once the SID and PIN is created is for an authorized SCC support person to manually deactivate the user’s account.
11. **Renewal** – Not an issue at this time.
12. **Protection of Mechanism** – A user-maintained Password (PIN) protects the account. All of the application data is maintained in a secured database.
13. **Obligations and Liabilities** – As stated in “1.” above, SCC is obligated to protect the confidentiality of student data as delineated in the FERPA law and other state and national statutes. Confidentiality of staff information is covered by the same or similar rules and regulations.
14. **Validation Process** – Identification and authentication is performed mostly via a traditional user ID and password authentication using SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
15. **System Configuration** – The SCC Application server and hosting operating system is configured in compliance with SCC IT Security Standards on Windows Base System Configuration and Windows Server Configuration. This is basically adhering to the industries “best practices”.
16. **Network Configuration** – The associated network devices are configured in compliance with the BCC IT Security Standard on Network Device Configuration.
17. **Firewall Configuration** - The firewall is configured in compliance with the SCC IT Security Standards on Firewall Change Management and Firewall Logical Specification (Confidential). (TBD)
18. **Intrusion Detection** – (TBD).
19. **Audit Procedures** – Currently no “formal” audit procedures (similar to the HP3K annual security audit) are implemented for web based applications. (TBD)

6. SFCC Web Applications

1. **Information is Public** – Some SFCC application data is intended for and is available to the general public (e.g. public information on the SFCC web site). Other application data is intended for use by SFCC as an institution and is considered the “private” information of the staff, student or potential student and is protected as such. Each application is designed to offer the minimum level of access based on the authentication credentials of the application user(s). Most authentications are based on NT User/User groups, in some cases authentication is based on SID or User-Id paired with a PIN or password.
2. **Documented Risk Issues** –
 - a. The potential impact of viewing data by unauthorized intruders – If persons were able to gain unauthorized access, they could possibly interfere with student and staff access to SFCC online application. A less likely risk would be the potential capture of private information (ID, address, birth date, etc.). Damage would likely be limited to an interruption in access and the disclosure of personal information.
 - b. The potential impact of unauthorized viewing of data by otherwise legitimate users – The viewing of data by a legitimate user who is not authorized to view it could result in the misuse of the data. Viewing the data by an unauthorized but legitimate viewer would be a violation of the FERPA law and college policy.
 - c. The potential impact of the use of the information assets for other than authorized purposes – Again, the potential impact of using the information assets would be the disclosure of private information and the potential interruption in access to online application functions.
 - d. The potential impact of unauthorized deletion, modification, or disclosure of information – The result of unauthorized deletion or modification could result in lost or “corrupted” data. Most likely would be a mere nuisance for the affected individuals and support staff, but should not result in direct monetary loss. Disclosure of private data without the appropriate consent would result in the violation of the FERPA law and is addressed by state and national statutes.
 - e. The potential operational impact if the service becomes unavailable (denial of service attacks) – If the services offered by the SFCC web based applications become unavailable through denial of services attacks, the operational impact is significant. This could result in loss of revenue, dissatisfaction of those to whom SFCC provides services, interruption of productive work, and a loss of institutional reputation.
 - f. The potential public confidence impact if the services or data provided by the system are compromised – If the services or data provided by the SFCC based applications is compromised, there will be a significant impact in the level of confidence that our online students and staff can place on the information provided. This could also result in loss of revenue, dissatisfaction of those to whom SFCC provides services, interruption of productive work, and a loss of institutional reputation.
 - g. The importance of non-repudiation (inability of a user to deny the initiation of a transaction) to the transactions support by the system – Non-repudiation in general is probably not a significant issue within the SCC provided applications.
 - h. The impact of an intrusive registration and authentication process on the potential user base of the application – If access to SFCC web application required a more intrusive registration and authentication process the result would be a delay in accessing the online tools. It would also increase staff workload. This would result in the potential loss of student enrollments in SFCC classes due to dissatisfaction, or unnecessary staff stress leading to a disruptive level of staff turnover.
 - i. The application impact on the potential user base to one-time and ongoing authentication costs – There are no one-time and/or ongoing authentications costs at this time. (TBD)

Mitigation of Risk – The processes identified in the CCS IT Security Standard on Windows Server Configuration mitigate many of the documented risks identified in relation to SCC Web Applications. In addition, safeguards are addressed in numerous standards limit outside access to the SCC application

server. The CCS IT Security Standard on Intrusion Detection and Incident Response addresses prevention and response to the usurping of the legitimate use of the asset. (TBD)

Some areas documented above identify a significant risk of considerable loss and harm to SFCC/CCS. However, the use of the Web for online applications provide significant communication and access to information, and is such an important part of fulfilling the educational and administrative missions of the college. Whatever risks exist in the use of these resources is minor in comparison with their positive business impact.

3. **Assessed User Base** – The user-base of the SFCC web application processes would be new and returning SCC/SFCC/IEL students, faculty, and staff and in some cases the general public.
4. **Selected Identity Confidence Level** – Identification and authentication is performed mostly via a traditional user ID and password authentication using SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
5. **Use Transact** – The use of Transact does not apply to the SFCC web applications.
6. **Request for Mechanism** – Where required is provided via the assignment of SID and PIN to students and staff. Applications available to the general public do not require authentication and should be considered public information being made available via a database driven application not unlike a static public information web page.
7. **Initial Identification** – Identification and authentication is performed mostly via a traditional user ID and password authentication using SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
8. **User Agreement** – There is no user agreement beyond FERPA requirements of those staff that work with student information.
9. **Issuance Procedures** – Where required is provided via the assignment of SID and PIN to students and staff.
10. **Revocation, Suspension, Renewal** – The only means of revocation once the SID and PIN is created is for an authorized SFCC support person to manually deactivate the user’s account.
11. **Renewal** – Not an issue at this time.
12. **Protection of Mechanism** – A user-maintained Password (PIN) protects the account. All of the application data is maintained in a secured database.
13. **Obligations and Liabilities** – As stated in “1.” above, SFCC is obligated to protect the confidentiality of student data as delineated in the FERPA law and other state and national statutes. Confidentiality of staff information is covered by the same or similar rules and regulations.
14. **Validation Process** – Identification and authentication is performed mostly via a traditional user ID and password authentication using SID or User-Id paired with a PIN or password, in some cases authentication is NT User/User group based.
15. **System Configuration** – The SFCC Application server and hosting operating system is configured in compliance with SFCC IT Security Standards on Windows Base System Configuration and Windows Server Configuration. This is basically adhering to the industries “best practices”.
16. **Network Configuration** – The associated network devices are configured in compliance with the BCC IT Security Standard on Network Device Configuration.
17. **Firewall Configuration** - The firewall is configured in compliance with the SFCC IT Security Standards on Firewall Change Management and Firewall Logical Specification (Confidential). (TBD)
18. **Intrusion Detection** – (TBD).
19. **Audit Procedures** – Currently no “formal” audit procedures (similar to the HP3K annual security audit) are implemented for web based applications. (TBD)

Amendments

Appendix A -- Change Log

Date	By	Version	Notes
10/19/03	T. Davenport	1.0	
10/21/03	D. Hol	3.0	

Appendix B – References

I.F SECURITY TRAINING

Introduction

This standard documents the various elements of the IT Security Training program for all CCS staff, faculty and administration.

Scope

The scope of this training standard will cover the access to, misuse or loss of IT hardware, software, data and facilities. It will also outline the users responsibilities for protecting IT assets, compliance with software license agreements, appropriate Internet use, virus protection and reproduction of copyright material.

Standard

1. Training Aims

- CCS recognizes the high degree of trust it places in its IT staff. This makes the hiring process and probationary period of a new employee critical for assessing the trustworthiness and capabilities of all new IT employees. Careful IT employee screening and review practices per CCS Personnel and CCS Security Standards will be followed.

2. Training Activities

Employee Security Awareness Training (TBD)

- Each staff member will undergo an initial IT Security Awareness Program within three months of being hired.
- Sufficient time will be made available for staff to periodically participate in Security Awareness Programs.
- A CCS IT Security Administrator or an authorized designee will be responsible for administering the CCS IT Security Awareness Program, for documenting employee participation in the program, and for maintaining records of training.

Policy and Standards Awareness

- At least annually, CCS staff will be required to review the CCS IT security policies and standards. Sufficient time will be made available for staff to do this.

Security Training (TBD)

- The CCS IT Security Administrator or an authorized designee will maintain a resource list of security courses, programs, and conferences available to the staff since training will be part of the annual evaluation of all IT employees.

New Employee Orientation

1. A new hire will be given a basic orientation covering the following procedures, policies, and standards as well as the location of the full collection of documents for future review and reference:
 - a. Emergency and Public Safety Procedures
 - i. Emergency Preparedness Plan
 - ii. Medical and First Aid Information
 - iii. Fire Procedures
 - b. State Policies
 - i. Conflict of Interest Policy
 - ii. Drug Policy

- iii. Ethical Conduct Executive Order: Standards of Ethical Conduct
- iv. Sexual Harassment Policy
- v. Whistleblower Program
- c. Acceptable Use Policies
 - i. CCS Acceptable Use Policy
 - ii. CCS IT Security Policy
- d. CCS IT Security Standards (TBD)
 - i. Overview of CCS IT Security Program
 - ii. Personnel Security
 - iii. Physical Security
 - iv. Security Strategy
 - v. Data Security
 - vi. Network Security
 - vii. Access Security

Written copies of these procedures, policies and standards will be provided to new employees . After their review of the documents, new employees will be presented a statement for signature acknowledging that they have read and understand their responsibility for compliance with these policies. At the discretion of the Human Resources or the IT Administrator additional policies may also be included in the initial orientation.

Ongoing Training

- It is the responsibility of each employee to review annually the various procedures, policies, and standards that pertain to ongoing employment with CCS, including those listed in the New Employee Orientation section above. (Also, see the CCS IT Security Standard on Employee Training). These documents will be provided by the immediate supervisor as needed.

Physical Security

Fire Suppression

- Designated staff will receive periodic training on the use of the fire suppression equipment.

Flood/Water Protection

- Designated staff will receive periodic training on responding to a flood situation. This training may be in the form of reviewing documentation instead of formal training.

Climate Control

- Designated staff will receive periodic training on responding to HVAC/DDC failures. This training may be in the form of reviewing documentation instead of formal training.

Electrical Power and Backup Power

- Designated IR support staff will receive periodic training on responding to power failures. This training may be in the form of reviewing documentation instead of formal training.

Evacuation Planning and Building Safety

- All designated work areas will be equipped with an emergency first aid kit, and all staff members will be trained in its use. This training may be in the form of reviewing documentation instead of formal training.

3. Training Schedule (TBD)

- At this time, an IT Security Training program doesn't exist, but one will be developed in the near future.
- The training materials and review will be included in new employee orientation and will become part of the required annual training classes for all CCS
- This training material will also be made available on an on-line presentation that will log the users participation.

4. Administrator for agency IT Security Training

- The CCS IT Security Administrator or an authorized designee will be responsible for administering the CCS Security Awareness Program, for documenting employee participation in the program, and for maintaining records of training.

- The CCS IT Security Administrator or an authorized designee will maintain a resource list of security courses, programs, and conferences available to the staff since training will be part of the annual evaluation of all IT employees.

5. Address regularly occurring training activities

- Each staff member will undergo an initial IT Security Awareness Program within three months of being hired.
- Sufficient time will be made available for staff to periodically participate in Security Awareness Programs.
- At least annually, CCS staff will be required to review the CCS IT security policies and standards. Sufficient time will be made available for staff to do this.
- It is the responsibility of each employee to review annually the various procedures, policies, and standards that pertain to ongoing employment with CCS, including those listed in the New Employee Orientation section above. (Also, see the CCS IT Security Standard on Employee Training). These documents will be provided by the immediate supervisor as needed.

Amendments

Appendix A -- Change Log

Date	By	Version	Notes
10/22/03	D. Hol	1.0	

Appendix B – References

I.G SECURITY PROGRAM MAINTENANCE

Introduction

This standard outlines how CCS will maintain their IT Security Program. This plan will require that agencies review, evaluate, and update their IT security policies, standards, and guidelines annually or more frequently whenever its business, computer, or telecommunications environments undergo change.

Scope

The scope of this maintenance program will include, Physical Facilities; Computer Hardware/software; Telecommunications Networks; Application Systems; Internet Based Information Systems and impacts related to organizational or budget changes.

Standard

1. Plan to maintain the IT security program

A CCS IT Security Administrators and the Director of Information Systems are responsible for maintaining this set of security standards.

Each standard will be reviewed at least annually. If changes to CCS's computing environment or the more general state of computing (best practices, risk, vulnerability or threat) occur, appropriate standards will be modified.

2. IT Security Program review process

- Review, evaluation, updates and/or changes to the CCS IT Security program and its supporting documents, policies and procedures will generally come as a result of changes within the CCS computing environment, mandates from CIS, mandates from government, or changes to the type or level of risk associated with the environment in which CCS works. Additionally, they may be triggered by any applicable modifications to the physical facilities, computer hardware/software, telecommunications networks, applications systems, Internet-based information systems, or any impact that is related to organizational and/or budget changes.
- Changes to the security processes, procedures and practices established within the CCS IT Security program will be made and approved by the Director of Information Systems and the CCS IT Security Administrators, or authorized designee.
- As IT security policies and standards are revised, all CCS employees will be notified via a broadcast email where appropriate. Where a change in standard or policy has a direct impact on faculty, staff or administration, the review process will include appropriate committees at each CCS unit.
- At that time, employees will have three weeks to review and comment on a revised standard. Comment may be provided directly to a CCS IT Security Administrator and/or the Director of Information Systems in an e-mail, in a one-on-one format, or in a large group discussion format. This assures that college employees are aware of proposed changes and will have an opportunity to influence the direction of changes to the standards. (On rare occasions, mandates or extreme risk levels may dictate a shorter review period or even no review period. At those times, the process will be adjusted to best meet the stated principle.)
- A document change history will be maintained for each security standard. Change notes will be kept at a summary level but should be clear, concise and meaningful.
- After CCS employees have provided their input on proposed IT policy and standard changes, the CCS IT System Administrator principally responsible for the impacted area will finalize the new or revised policies and standards. Employees will be notified via a broadcast e-mail message that the standard has been approved and how to access the finalized version.

3. Changes that will require review

- Review, evaluation, updates and/or changes to the CCS IT Security program and its supporting documents, policies and procedures will generally come as a result of changes within the CCS computing environment, mandates from CIS, mandates from government, or changes to the type or level of risk associated with the environment in which CCS works. Additionally, they may be triggered by any applicable modifications to the physical facilities, computer hardware/software, telecommunications networks, applications systems, Internet-based information systems, or any impact that is related to organizational and/or budget changes.

4. Annual certification to the ISB

- The CEO and Presidents of CCS, after consulting with the Director of Information Systems and the CCS IT Security Administrators, will provide annual certification to the Information Services Board that CCS's IT Security Program has been developed, implemented, tested and its processes, procedures, policies and practices updated as needed.

5. Agencies assigned responsibility for maintaining their security program

CCS Security Strategy

The CCS IT Security Program, in its standards and policies, has assigned responsibility for IT security and for the installation, monitoring, and enforcement of the security rules and procedures to individuals, groups, and units on campus with appropriate training and background to administer these vital technology functions.

IT Security Administrator Position

Each unit of CCS (SCC, SFCC, IEL and the District Office) will maintain an IT Security Administrator position that is assigned primary oversight of the agency security and is responsible for maintenance and implementation of the CCS IT Security Program. These positions will generally be the supervisor/manager of the technical/computer support department and the Director of Information Systems. CCS security concerns and responsibilities cross internal organizational boundaries and as such, the CCS IT Security Administrator will:

1. Require strong support from management and staff to formulate and implement appropriate security.
2. Require a fairly broad background in areas of development practices, systems administration and operational practices, and networking, as well as current trends in security.
3. Work to negotiate a balance between risk, risk mitigation, and business needs.
4. Work to integrate secure practices into business practices to assure greater levels of acceptance by the campus staff and users.
5. Have authority to install, monitor, and enforce security rules and procedures.

6. Change management process for the IT Security Standards

A document change history will be maintained for each security standard and will be listed at the end of each document. Change notes will be kept at a summary level but should be clear, concise and meaningful.

7. Distribution Procedures

As IT security policies and standards are revised, all CCS employees will be notified via a broadcast email for those standards that directly impact end users. If a change in standards impacts the technology support staff, then distribution will be made according to the procedures outlined in section 2 of this document.

Amendments

Appendix A -- Change Log

Date	By	Version	Notes
10/22/03	D. Hol	1.0	

Appendix B – References

II. INTERNET BROWSER/SERVER CONFIG AND USE

Introduction

This standard describes the security standards for using the Internet and running state web-enabled applications over the Internet.

Scope

The Internet provides a number of services including E-mail, file transfer, remote login, interactive conferences, news groups and the World Wide Web. The first section of this standard describes the security standards for using the Internet and running state web-enabled applications over the Internet.

The second section of this standard addresses web browsers. Web browsers provide a user interface to navigate through the Internet by interpreting, formatting, and presenting the documents to users. Browsers, E-mail clients and other desktop tools may also introduce vulnerabilities to an agency.

The third section of this document addresses web server security. Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. There are many areas of Web servers to secure: the underlying operating system, the Web server software, server scripts and other associated components.

Standard

1. *Internet Use and Connectivity:*

- Units and individuals are prohibited from establishing permanent or sustained Internet connections via an Internet Service Provider (ISP) from any CCS-networked workstation which bypasses the CCS firewall. This prohibition will be strictly enforced, as it provides an unmonitored entry path from the Internet into the CCS network, which can lead to unintended security risks.
- Transmitting non-encrypted confidential information, as defined by the CCS policy on Access to Public Records and by the federal Family Education Rights and Privacy Act (FERPA) is strictly prohibited. The following are a couple of considerations that must be taken into account:
 - SQL Server
 - Data stored on disk will be secured commensurate with its level of confidentiality or value. Some data that is labeled confidential might, for example, require encryption and storage only within a database.
 - Consideration will be given to additional security that might be appropriate for confidential data, such as credit card numbers and a Personal Identification Number (PIN); this might include encryption of specific columns.
 - Data File Transfers
 - External Transfers
When transferring production data to a business partner who is not a member of the Washington Community Technical Colleges (WCTC) institution, care must be taken to ensure that the integrity and confidentiality of the data is maintained in transit. Any data transferred across a public network, must be encrypted in transit using an industry standard, strong encryption algorithm
 - Email Transfers
Any files being transferred will most likely be downloaded to a workstation and manipulated in some manner prior to attaching to an e-mail; therefore, care must be taken to protect the integrity and confidentiality of this data after it leaves the application server.
 - Web-based Transfer
 - The data will be transferred over a Secured Socket Layer (SSL) encrypted link.
 - Care will be taken to protect the integrity and confidentiality of this data after it leaves the application server.

- Secure Shell (SSH) and File Transfer Protocol (FTP)
 - FTP data will be encrypted and signed with pretty-good-privacy (PGP). (PGP will be used throughout this document to mean any of the following: Commercial PGP, OpenPGP, or GNU GPG).

2. Minimum Web Client Security Requirements

The following is CCS's documented plan for the use of web browsers and e-mail clients:

- All software used to access the Internet must be approved by a CCS tech support staff member and must incorporate all available/appropriate security patches.
- During the initial "build" all drive partitions, account policies, group policies, event log and auditing settings, security options, user rights, file permissions, services, and registry settings will be configured and applied in accordance with current best IT practices, as determined by the Systems Administrator of the affected system, in consultation with other CCS staff, as necessary. These decisions will apply to the business and educational application of the systems within the context of all appropriate and applicable CCS IT Security Standards, including this standard. All services not necessary to support the business use of the computer will be disabled.
- The initial system build will be performed with the computer system either disconnected from the network, if possible, or using a secure network connection. If necessary, it will be attached to "production" networks for installation, but it will not be used on any CCS network in a production capacity until it has been fully built, patched, and security hardened.
- System builds will be performed with a supported version of Microsoft Windows. All security and recommended patch bundles will be applied.
- Upgrades to new operating systems and application versions will be based on business need. Decisions to upgrade the standard campus operating system for administrative systems will be made by the appropriate CCS Information Technology authority.
- Security patches for OS and application security vulnerabilities will be installed as quickly and safely as possible after their release.
 - Recommended patches will be regularly installed on the computers and servers.
- All outbound browser traffic will use appropriate technology to prevent disclosure of IP addresses.
- Files received from the Internet are checked for viruses.
 - Appropriate anti-virus (AV) software as defined by the appropriate CCS Information Technology authority will be installed on all workstations and configured to ensure that files received from the Internet are checked for viruses.
 - Real-time virus protection will be enabled for all desktops and mailboxes, thereby performing a proactive scan each time a new file or message is introduced onto any of the systems.
 - Scheduled scans on users' desktops will be performed daily.

3. Web Server Security Requirements

All CCS Web servers must adhere to the following standards of operation and maintenance unless specific exemptions are document and approved by the appropriate CCS Information Technology authority.

Web Content Review

- Web content, for this section, will refer only to that content that the CCS publishes as documentation and information to its users, its business partners, and the public. This content is often "static" pages, and retrieval of documentation that has been archived in a Web- accessible repository.
- Public Web servers will not be used to host sensitive information intended to be accessed only by internal users. In other words, an Intranet and an Internet Web server may not be run on the same computer.
- Providing and managing the actual web content is a cooperative and collaborative effort that includes staff from all departments at the CCS, all of whom are expected to be aware of and sensitive to the following issues with regards to the information published on the CCS web sites. CCS's Webmasters will have ultimate responsibility for managing content on all CCS web sites. This will include such tasks as:
 - Identifying what content should be published to a Web site.
 - Reviewing the content for possible negative ramifications for publishing.
 - Identifying who should be responsible for creating and maintaining the content.
 - Reviewing the information for sensitivity and distribution control.

- Determining the appropriate access and security controls.
- Periodically reviewing the Web site for sensitive information that may be stored (hidden) in the server side scripting source code (e.g., ASP, PHP) or form.

Web Server Software

- The following standards apply to Web Server software Campus users are forbidden from downloading, installing, or running any Web server software without prior approval from the CCS IT Security Administrator and the Director of Information Systems.
- CCS Technology Support units are responsible only for the content or services provided by their departments. Any other content placed on CCS-provided Web server space is the responsibility of the individual or department to whom the space is assigned.

Remote Control of Web Servers

- All remote control of Web servers, including administrator operations and/or supervisor-level logons, will be done using properly secured sessions utilizing passwords in compliance with the CCS IT Security Standard on Password Management.

Web Servers Not To Be Used as a Repository

- Web servers that are accessible to the public will not serve as a repository for confidential data. However, a public Web server can act as a proxy for access to confidential data located on secure servers.

Amendments

Appendix A -- Change Log

Date	By	Version	Notes
9/9/03	T. Davenport	1.0	
10/22/03	D. Hol	2.0	

Appendix B – References

III. STANDARDS FOR DIGITAL GOVERNMENT (INTERNET) APPLICATION SUBMITTAL

Introduction

The CIS and the WCTC are outside the DIS firewall and the Digital Government Framework, as we understand it, is not directly available to us. The web-based applications developed by the CIS and CCS are, however, built on a common framework of their own that has been documented and is periodically reviewed.

For this reason, CCS has determined that this standard is not applicable to our IT environment.