



# El Paso Community College Information Security Risk Assessment Survey

## Executive Summary

Texas Administrative Code, 1 TAC §§202.70-202.77, establishes minimum standards for the protection of information resources entrusted to Texas state agencies. It is the policy of the State of Texas that:

*"Information resources residing in the various agencies of state government are strategic and vital assets belonging to the people of Texas. These assets must be available and protected commensurate with the value of the assets. Measures shall be taken to protect these assets against accidental or unauthorized access, disclosure, modification or destruction, as well as to assure the availability, integrity, utility, authenticity and confidentiality of information. Access to state information resources must be appropriately managed."*

Current advances in information technology have contributed to a rise in the accessibility of information, ease of use, productivity and efficiency. However, there are significant risks involved with this type of advancement. Security threats and breaches have increased and crimes are committed with more malice.

The Texas Department of Information Resources developed guidelines (Practices for Protecting Information Resources Assets, March 2003) "to assist agencies and institutions of higher education to achieve the goal of acceptable information resources risk management and to meet the state's standards for information security." These guidelines recommend the identification of critical assets and the performance of security risk assessments in order to locate and document vulnerabilities.

The Information Security Office of the El Paso Community College is charged with recommending policies and establishing procedures and practices, in cooperation with owners and custodians, necessary to ensure the protection of the IT resources of the District. One such practice is a security vulnerability assessment of the computing infrastructure in order to determine the current state of computing resources. The vulnerability assessment attempts to identify threats that could affect the confidentiality, integrity, or availability of College information resources. Results of the assessment along with recommendations for improving security practices will be distributed to departments, and, as required by information security standards, a final summary report will be prepared for approval by EPCC's President.

As a tool in conducting the vulnerability assessment, the following survey is being distributed to network managers and system administrators who are responsible for providing management of critical systems and applications at EPCC. The survey is a compilation of risks that include the SANS (Sys-Admin, Audit, Networks, Security organization) list of the twenty most critical internet security vulnerabilities, security guidelines established by the Texas Department of Information, and also considers compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Family Education Rights and Privacy Act (FERPA), and the Gramm-Leach-Bliley Act (GLBA).

We expect that the results of this survey will provide a valuable self-assessment of the current state of the computing security environment in each individual department. By identifying all critical information assets, areas vulnerable to potential compromise, and commensurate protective measures, it will be possible to minimize the risks associated with rapid advancement in information technology.

Sincerely,

Fabiola Rubio  
Vice President for Information Technology  
and Chief Information Officer  
El Paso Community College

Effective: 10-11-2004

## El Paso Community College Information Security Risk Assessment

### Purpose

- Identify potential threats, known vulnerabilities and mitigation recommendations that exist in the El Paso Community College information system architecture. [The quality of the assessment will be directly related to the degree of cooperation and participation that the agency provides to the assessment team.]
- Fulfill the requirement of 1TAC202.72(a): A security risk analysis of information resources shall be performed and documented. The security risk analysis shall be updated based on the inherent risk. The inherent risk and frequency of the security risk analysis will be ranked.

### Objectives

- The outcome of the analysis will be a list of threats and vulnerabilities (flaws or omissions in controls) that may affect the confidentiality, integrity, and availability, and/or accountability of resources that are essential to critical resources
- To perform and document a security risk analysis based on threat and vulnerability assessments
- To provide a snapshot of EPCC status regarding security risks and compliance issues
- To provide a basis for selecting the most appropriate and cost-efficient protection measures
- To provide information on the likelihood of a threat and its occurrence and the impact(s) on information resources
- To provide due diligence to ensure reasonable steps are taken to prevent loss of resources
- To provide the foundation of all risk management programs
- To identify areas for reducing weaknesses before and simultaneously with recovery planning
- To help create IT Security awareness throughout the El Paso County Community College District

### Goals

- Identify Critical Resource Elements (Resources)
- Conduct Risk Assessments
- Complete the Security Risk Analysis

### Applicable Policies, Laws and Standards

- El Paso Community College
  - EPCC Procedure for Information Computer Security Procedure Number 2.05.01.30  
<http://www.epcc.edu/infosec/procedure02050130.html>
  - EPCC Procedure for our Acceptable Use Policy for Information Resources Number 2.05.01  
<http://www.epcc.edu/infosec/procedure020501.html>
- State of Texas
  - Texas Administrative Code: Information Security Standards, Title 1, Part 10, Chapter 202  
[http://info.sos.state.tx.us/pls/pub/readtac\\$ext.ViewTAC?tac\\_view=4&ti=1&pt=10&ch=202&rl=Y](http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202&rl=Y)
  - Practices for Protecting Information Resources, September 2003, Texas Department of Information Resources  
<http://www.dir.state.tx.us/IRAPC/practices/index.htm>
- U.S.
  - Gramm-Leach Bliley Act (Financial Record Privacy)  
<http://www.ftc.gov/privacy/glbact/glbsub1.htm>
  - Family Education Rights and Privacy Act (Protection of Education/Student Records)  
<http://www4.law.cornell.edu/uscode/20/1232g.html>
  - Health Insurance Portability and Accountability Act (Privacy of Health Information)  
<http://www.hipaa.org/>

## Departmental Information and Critical Resource Elements

**Please complete one security assessment survey for each resource considered critical to the business operations of your department.** This survey has been developed for managers and administrators of computing resources. In addition, faculty or staff who have been identified by the Chief Information Officer as system administrators who manage systems or applications that are critical to specialized business functions or coursework (those who are not directly supported by their college or department's network manager) are also strongly encouraged to complete the assessment.

Fill in the most accurate assessment of the current status of the critical resource. If the critical resource is a computer system that is made up of more than one element, base your responses on the most appropriate element, or the system as a whole, where applicable.

### Departmental Information

Please provide contact information for your department.

College/Department:	
Evaluator(s) and Title(s):	
Primary Contact e-mail:	
Primary Contact Telephone:	
Evaluation Date:	

### Identify Critical Resource Elements

Computing resources can be comprised of single elements or as members of major systems. Identify the elements that make-up the critical resource. Circle (or fill in) all that apply.

- Data
- Personnel
- Hardware
- Software
- Facilities
- Other : \_\_\_\_\_

### Data Resources

Identify (circle or fill in) any confidential, sensitive, or proprietary data or other information that are stored on the critical resource.

- student records
- health care information
- financial records
- employee records
- personal information
- university or departmental proprietary information
- computer system logs
- emergency procedures/plans
- archives
- other: \_\_\_\_\_

**Personnel Resources**

List the names of personnel who have system access, administrative permissions, or other special privileged access to the critical resource. Include emergency support personnel. If additional forms are needed, see Appendix A.

Name	Function (primary support, emergency support, etc.)	Telephone	Supervisor

**Hardware and Equipment Resources**

Complete this section if the critical resource is identified as hardware (communications equipment /devices, UPS systems, mini and microcomputers, disk and tape drives, printers, terminals, fax machines, modems, power supplies, etc.). If additional forms are needed, see Appendix B.

Describe Hardware/ Equipment:	
IP(s): Static IP or "DHCP"	
Vendor:	
System Administrator(s):	
Number of Workstation Installations attached to system (if applicable):	
Describe systems which are interdependent upon the critical resource for service or operation	
Physical Location (bldg, room)	
Other functions located in the same room (include any functions which are managed by other departments if applicable)	
Room Manager	

**Software Resources**

Complete this section if the critical resource is software (operating systems, databases, web and non-web applications, mail servers, firewalls, other security software, file maintenance software, communications systems software, etc.). If additional forms are needed, see Appendix C.

Name of Software/Application:	
Type/Role (see above)	
Commercial or Developed In-House	
Vendor:	
Version:	
System Administrator (s):	
Applications that restrict access to the software resource, if applicable (i.e. firewall, etc.)	

**Security Levels**

Based on the description of security requirements found in the Security Level Key, identify the level of protection required to maintain confidentiality, availability and integrity of the resource(s). Use the chart below as a guide to describe the overall security level requirements of the resource(s) identified in "Identify Critical Resource Elements".

**Security Level Required** (high, medium, low): \_\_\_\_\_

Security Requirement	Description of Resource	Impact Potential	Safeguard Implementation Schedule	Assessment Interval
High	Information resources that involve large dollar amounts or significantly important transactions;  Systems or resources that store confidential or sensitive data that is protected by FERPA, HIPAA, GLBA or other federal and state laws, i.e. social security numbers, credit card numbers, student records, personal financial records, personnel records, health information, social security numbers, etc.  Impacts a large number of people or interconnected systems.	Disastrous, catastrophic, or major loss will result if security is compromised;  Unauthorized disclosure or modification of confidential, sensitive or proprietary information would cause real damage to the university or parties involved, or could result in fraud, errors, loss of public confidence or legal action;  Business operations would be hindered, or an impact on public health or safety would occur if the transactions were not processed timely and accurately.	Immediate	Annual
Medium	Information resources that transact or control a moderate or low dollar value;  Impacts a moderate proportion of the customer base.	Very Serious damage will result if security is compromised;  Disruption in business operations; Diminished capacity of business operations; Potential for embarrassment or problems for the parties involved if released.	Implement safeguards in the near future	Biennial
Low	Information resources that publish generally available public information;  Resources that result in a relatively small impact on the population.	Moderately Serious damage will result if security is compromised;  Business operations will not be disrupted if the resource is compromised.	Attention and consideration should be implemented as a good business practice	Biennial

## Instructions for Completing the Survey

Use the Implementation Level Key as a guide to identify the current implementation level for the controls listed in each category of the survey. Fill in the most accurate assessment of the current status of the critical resource. If the critical resource is a computer system that is made up of more than one element, base your responses on the most appropriate element, or the system as a whole, where applicable. After each question, there is a comment field and an initial field. The comment field can be used to note the reference to supporting documentation that is attached to the questionnaire or is obtainable for that question. The initial field can be used when a risk based decision is made concerning not to implement a control or if the control is not applicable for the system.

Survey statements are based on Texas Administrative Code: Information Security Standards, Title 1, Part 10, Chapter 202; Health Insurance Portability and Accountability Act (HIPAA); Family Education Rights and Privacy Act (FERPA); Gramm-Leach-Bliley Act (GLBA); EPCC Information Resources Security Policy 3.6; EPCC Computer Use Policy 3.10; Texas Department of Information Resources Practices for Protecting Information Resources 2003, and SANS Top Twenty Internet Security Vulnerabilities.

**Please complete one survey for each critical resource and return the completed form(s) to the Office of the Chief Information Officer, c/o Richard Buller within three week from the date of receipt.**

If you have any questions, please contact Richard Buller, [rbuller@epcc.edu](mailto:rbuller@epcc.edu), 915 831-6312.

<b>Implementation Level Key</b>	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

### Information Security Risk Assessment Survey

#### Security Policy for the Identified Resource

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	The security policy is known by all individuals who have the responsibility for implementing the policy.		
2	A security plan has been developed based on identified threats.		

#### Management and Staff Responsibilities

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	Security roles are defined for data owners.		
2	Security roles are defined for data custodians.		
3	Security roles are defined for system users.		
4	Security roles are defined for security contacts.		
5	Security roles are defined for system administrator(s).		
6	Security roles are defined for managers/supervisors.		
7	System administrators attend FERPA training prior to receiving access to student data.		

#### Personnel Security

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	A background check is performed on new employees.		
2	There is an orientation course on best security practices for new employees.		
3	Employees are required to sign nondisclosure agreements.		
4	A policy of segregation of duties has been established and documented.		
5	Security sensitive positions are defined.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

**Training and Awareness**

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	Administrators and users are aware of confidentiality policies that prohibit the disclosure of protected information (as required by FERPA, GLBA, and HIPAA).		
2	Users are aware that they must protect confidential and sensitive data (student, employee or university information) in printed or electronically displayed form.		
3	Live or current confidential or sensitive information is not used during training.		
4	Users are aware of procedures for backing up files.		
5	Users are instructed to log off computers when away from their workstations for prolonged periods.		
6	Users are aware of methods for selecting and managing secure passwords.		
7	Workstations utilize password-protected screensavers.		
8	Users are aware that sharing accounts is prohibited.		
9	Users are aware that workstations must run virus protection software.		
10	Users are aware of social engineering techniques.		
11	Users are aware that circumventing a security control is a violation of the Computer Use Policy.		
12	Users are aware that they must comply with all reasonable requests and instructions from a computer system administrator.		
13	Users are aware that unauthorized use of a university computer resource is a violation of the Acceptable Use Procedure.		
14	Users are aware of procedures for reporting security incidents.		
15	Users are aware that they must comply with the College computer use and security policies.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

**Physical Security**

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	Physical security policies and procedures are in place for the critical resource.		
2	Physical security policies and procedures are enforced.		
3	Reviews of physical security measures are conducted annually as well as when facilities or security procedures are significantly modified.		
4	Physical access to computer facilities is controlled and restricted to authorized individuals.		
5	Terminals or workstations logged into a current job session are not left unattended except where security measures have been taken to prevent unauthorized access.		
6	Physical security measures are in place for portable devices (laptops, PDA's, etc.)		
7	Physical security measures are commensurate with the sensitivity or confidentiality of protected data stored on the critical system.		
8	Portable devices (laptops, PDA's, etc.) are stored securely when not in use.		
9	Areas housing critical resources are locked at all times.		
10	An alarm system is in place and logs all access.		
11	Visitors are required to wear badges.		
12	Procedures are in place for locking the room in which the critical system is housed.		
13	A card key system is in use in addition to locking doors.		
14	A keypad/combination lock system is used.		
15	Media and printed documents containing confidential or sensitive information are stored securely when not in use.		
16	Data files are encrypted.		
17	The critical resource is housed in a separate room.		
18	Doors automatically lock.		
19	Locks are keyed off master.		
20	The area housing the critical resource is monitored.		
21	Logs of visitor and employee entrance into and exit from the area are maintained.		
22	Visitors are escorted.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>Physical Security continued</b>		
23	Removable media (CD-ROMS, floppy disks, zip disks, etc.) are protected from unauthorized access (i.e. stored in a locked drawer) and unauthorized removal.		
24	Keys, access cards, identification are removed when staff, contractors or vendors when responsibilities change, when termination occurs or when access is longer needed.		
25	Emergency procedures are documented and tested at least annually.		
26	Physical access to protected data is restricted to staff who are responsible for the security and maintenance of the data.		

**Media Sanitizing/Disposal/Retention/Storage**

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	Policies and procedures are in place for proper sanitizing and disposal of sensitive material on floppy disks, CDs, etc.		
2	An authority is assigned to ensure that media containing sensitive material is sanitized before disposal.		
3	Media is properly stored for retention.		
4	Media and documented materials are protected from unauthorized access, theft, unauthorized copying, modification, installation of software, or destruction.		
5	Media is securely stored.		

**Software License Compliance**

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	Licenses are available or obtainable for all software running on the critical resource.		
2	Commercial or licensed software and other copyrighted digital materials are protected from unauthorized duplication.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

**Network and System Administration**

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>Network Security</b>		
1	Methods for approved access to network services are documented.		
2	A firewall is configured and in place.		
3	Services that are accessible by external users are documented.		
4	An intrusion detection system (IDS) or other monitoring techniques are in place.		
5	The IDS knowledge base is configured by the system administrator.		
6	Individuals allowed to access the system externally are documented.		
7	The network architecture is hidden from untrusted external users.		
	<b>Management</b>		
1	The names and contact information for system administrators are documented.		
2	System administration is contracted to non-EPCC sources		
3	Backup personnel have been identified to respond to emergencies.		
4	System administrators are provided security training prior to administering the system.		
5	System administrators and privileged users manage the system within specified guidelines and adhere to the System Administrator Code of Ethics (see EPCC IT Code of Ethics)		
	<b>Maintenance</b>		
1	Maintenance policies and procedures are in place.		
2	Only trusted personnel are allowed to perform maintenance functions.		
3	Sensitive data are removed from equipment before the equipment is sent out for repair or surplus.		
4	Procedures are in place to ensure that returned equipment has not been tampered with.		
5	Maintenance records are kept to indicate what was done, when, and by whom.		
6	Modems are disconnected after a specific period of inactivity or when no longer needed.		
7	Hard drives are properly erased prior to computer re-assignment or surplus.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>Security Plans</b>		
1	A system security plan is documented for this system and all interconnected systems.		
2	The security plan is periodically reviewed and monitored for effectiveness for dealing with threats, vulnerabilities and weaknesses.		
	<b>Virus Protection</b>		
1	Virus protection software and procedures are in use on the system.		
2	Virus information is distributed to system administrators and users.		
3	System administrators and users know whom to contact when a virus infection occurs.		
4	Removable storage media is scanned for viruses and other malicious code prior to use.		
5	Software is scanned for viruses prior to installation.		
	<b>Identification/Authentication</b>		
1	Each user of the information resource is assigned a unique identifier except for situations where risk analysis demonstrates there is no need for individual accountability of users		
2	A user's access authorization is appropriately modified or removed when the user's employment or job responsibilities change.		
3	Information resources systems contain authentication controls that comply with documented security risk management decisions		
4	Authentication procedures are in place.		
	<b>Passwords</b>		
1	Unique passwords are assigned for each user.		
2	Passwords include UPPER and lowercase alphanumeric characters.		
3	Passwords include symbols and special characters (non-alpha-numeric).		
4	Passwords include at least one number.		
5	Passwords are a minimum of 8 characters.		
6	Restrictions are in place to prevent usage of EPCC ID, account name, or login name as a password.		
7	Restrictions are in place to prevent usage of an E-mail address as a password.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>Passwords continued</b>		
8	Restrictions are in place to prevent usage of passwords that do not include UPPER and lowercase alphanumeric characters		
9	Restrictions are in place to prevent usage of passwords that are inclusive of single or multiple combinations of words that can be found in any dictionary, including foreign language dictionaries		
10	Restrictions are in place to prevent usage of passwords that contain numerical (digit) substitutions for characters (e.g. h3lp, adm1n, pa\$\$w0rd, etc.)		
11	Restrictions are in place to prevent usage of passwords composed of numbers only.		
12	Restrictions are in place to prevent usage of null passwords.		
13	Restrictions are in place to prevent usage of any previously used password.		
14	Accounts are locked after a specified number of failed password attempts.		
15	Aging requirements are in place to enforce password changes no less than every 120 days.		
16	Individuals with system administrator privileges are required to change passwords at more frequent intervals than end-users.		
17	System administrator or other system accounts do not contain default passwords.		
18	A procedure is in place for forgotten passwords.		
	<b>Account Management</b>		
1	Procedures for establishment, modification, deletion, and monitoring of active and inactive accounts are in place.		
2	The names of individuals with root access to the system are documented.		
3	Justification is required before remote access is permitted.		
4	Accounts that can be accessed remotely are documented.		
5	Administrator or other system accounts do not contain default names.		
6	Access to sensitive or confidential data is restricted to individuals who have completed FERPA training and to those who have been advised of protection requirements for financial and employee records.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>Account Management continued</b>		
7	Unsuccessful logon attempts indicate the cause of the failure.		
8	Accounts are locked after a set number of unsuccessful logon attempts.		
9	Logs of unsuccessful logon attempts are maintained.		
10	Modem access is terminated when an employee transfers or terminates employment.		
11	Guest accounts are disabled.		
12	Access to shared resources is restricted.		
13	Access privileges for computer users do not exceed the requirements of the role established for their use of the system.		
14	Access privileges for each user of the system are regularly reviewed.		
	<b>User Access</b>		
1	All administrators and users of the system have attended FERPA training if student information is stored in the system.		
2	Access privileges to data files is strictly controlled and users are limited to view only what is required for their specific job function.		
3	Access privileges to applications are strictly controlled, and user access is limited to only that which is required for their specific job function.		
4	A pre-defined number of unsuccessful login attempts results in suspension of the user's account.		
5	User accounts are logged off automatically after periods of non/inactive use.		
6	Users are restricted from accessing the operating system or other application/system resources not required in the performance of their job duties.		
7	Privileges that allow modifications to data are strictly controlled.		
8	User access is limited to specific time intervals.		
9	Access privileges for all users and administrators of the system are documented.		
10	User workstations are positioned to prevent access by customers or staff who are not authorized to use the workstation.		
11	Data displayed on computer screens is not visible to persons who do not have approved access.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented
	Control/Statement			Current Implementation Level (0-5)	Action/Comment	
	<b>System Security</b>					
1	The system is regularly patched for vulnerabilities.					
2	Unneeded ports are closed to prevent unauthorized access.					
4	Trained system administrators are assigned to manage the critical system.					
5	Recommended procedures for remediating SQL Injection have been applied.					
6	Recommended procedures for remediating data validation checks/errors have been applied.					
7	Recommended procedures for remediating the potential for buffer overflows have been applied.					
8	The current system configuration is documented, including systems that are interconnected.					
9	Configuration changes are protected from unauthorized access, use, or disclosure.					
10	Default configurations and applications are patched prior to installation.					
11	Steps are taken to secure the system/application immediately after (or prior to) installation or upgrades.					
12	Intrusion detection software or other monitoring techniques are in use.					
13	Ghosted image installations are reviewed and updated periodically for vulnerabilities.					
14	Remote access methods for accessing the system have been tested for security.					
15	End-of-day logoff is required.					
16	Sessions automatically timeout.					
17	Password protected screensavers are used to lock the screen.					
	<b>SANS Internet Security Vulnerabilities for Unix Systems</b>					
1	Procedures for remediating vulnerabilities associated with BIND domain name system have been applied as recommended by SANS.					
2	Procedures for remediating vulnerabilities associated with remote procedure calls have been applied as recommended by SANS.					
3	Procedures for remediating vulnerabilities associated with apache web server have been applied as recommended by SANS.					

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>SANS Internet Security Vulnerabilities for Unix Systems continued</b>		
4	Procedures for remediating vulnerabilities associated with general UNIX authentication accounts with no passwords or weak passwords have been applied as recommended by SANS.		
5	Procedures for remediating vulnerabilities associated with clear text services have been applied as recommended by SANS.		
6	Procedures for remediating vulnerabilities associated with sendmail have been applied as recommended by SANS.		
7	Procedures for remediating vulnerabilities associated with simple network management protocol (SNMP) have been applied as recommended by SANS.		
8	Procedures for remediating vulnerabilities associated with SSH have been applied as recommended by SANS.		
9	Procedures for remediating vulnerabilities associated with misconfiguration of enterprise services (NIS/NFS) have been applied as recommended by SANS.		
10	Procedures for remediating vulnerabilities associated with SSL have been applied as recommended by SANS.		
	<b>SANS Internet Vulnerabilities for Windows Systems</b>		
1	Procedures for remediating vulnerabilities associated with Internet Information Services (IIS) have been applied as recommended by SANS.		
2	Procedures for remediating vulnerabilities associated with Microsoft SQL Server (MSSQL) have been applied as recommended by SANS.		
3	Procedures for remediating vulnerabilities associated with windows authentication have been applied as recommended by SANS.		
4	Procedures for remediating vulnerabilities associated with Internet Explorer have been applied as recommended by SANS.		
5	Procedures for remediating vulnerabilities associated with windows remote access services have been applied as recommended by SANS.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>SANS Internet Vulnerabilities for Windows Systems continued</b>		
6	Procedures for remediating vulnerabilities associated with Microsoft data access components have been applied as recommended by SANS.		
7	Procedures for remediating vulnerabilities associated with windows scripting host have been applied as recommended by SANS.		
8	Procedures for remediating vulnerabilities associated with Microsoft Outlook and Outlook Express have been applied as recommended by SANS.		
9	Procedures for remediating vulnerabilities associated with windows peer-to-peer file sharing have been applied as recommended by SANS.		
10	Procedures for remediating vulnerabilities associated with simple network management protocol (SNMP) have been applied as recommended by SANS.		
	<b>Auditing</b>		
1	Appropriate audit trails are maintained to provide accountability for updates made to mission critical information, hardware and software and for all changes to automated security or access rules.		
2	A sufficient history of transactions is maintained to permit an audit of the information resources system by logging and tracing the activities of individuals through the system.		
3	A configuration control function or the equivalent is in place.		
4	System resources are documented.		
5	Contents of audit logs are protected from unauthorized access, modification, and/or deletion.		
6	A retention policy for audit logs is in place.		
7	Audit logs are stored and saved properly.		
8	Configuration changes are documented.		
	<b>Encryption</b>		
1	Encryption for storage and transmission of information is based on documented security risk management decisions.		
2	Unsecured methods are not used to transmit protected data (i.e. via unencrypted e-mail or unencrypted web applications).		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>Data Protection</b>		
1	Confidential information is accessible only to authorized users.		
2	Information containing confidential data is identified, documented and protected from unauthorized access, modification or destruction.		
3	Information resources shared or assigned to more than one agency are protected in accordance with conditions imposed by the providing agency.		
4	Data stored on portable devices (laptops, PDA's, etc.) are encrypted.		
5	Printed copies of protected data are secured (i.e. not left in plain sight).		
	<b>System Identification/Logon Banner</b>		
1	System identification/logon banners are in use.		
2	System identification/logon banners include the statement "Unauthorized use is prohibited".		
3	System identification/logon banners include the statement "Usage may be subject to security testing and monitoring".		
4	System identification/logon banners include the statement "Misuse is subject to criminal prosecution".		
5	System identification/logon banners include the statement "No expectation of privacy except as otherwise provided by applicable privacy laws".		

**Systems Development and Acquisition**

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	Test functions are kept physically or logically separate from production functions.		
2	Procedures are in place for testing and approving systems prior to placement into production status.		
3	Copies of production data are not used for testing unless all university employees and independent contractors involved in testing have been authorized to access the data.		
4	Information security audit controls are included in all phases of system development lifecycle or acquisition		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>Systems Development and Acquisition continued</b>		
5	Security related changes are approved by the data owner prior to implementation.		
6	Only authorized individuals are allowed to move and install computer equipment.		

**Incident Response**

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	A computer security incident response capability is established within the department or college.		
2	Security incidents are reported regularly to designated security contacts.		
3	Security incidents are promptly investigated and documented.		
4	Violators of computer security are disciplined appropriately per established policies for faculty, staff, and students.		

**Business Continuity Planning**

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	A business continuity plan has been documented.		
2	The business continuity plan has been distributed to key personnel.		
3	A copy of the business continuity plan is stored off site in a secure location.		
4	The business continuity plan addresses natural and manmade disasters as well as power outages.		
5	The business continuity plan is regularly reviewed.		
6	The business continuity plan identifies and prioritizes the resources that are most important to protect in an emergency.		
7	The business continuity plan includes a security risk assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.		
8	A business impact analysis has been conducted to assess the potential impacts of a loss of business functionality due to an interruption of computing or infrastructure support services.		

Implementation Level Key	0	1	2	3	4	5
	Not Applicable	Not Implemented	Minimally Implemented	Partially Implemented	Mostly Implemented	Fully Implemented

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
	<b>Business Continuity Planning continued</b>		
9	The business impact analysis addresses maximum tolerable downtime for time-critical support services (i.e. personnel, facilities, technology platforms, software, information resources security utilities, data networks and equipment, voice networks and equipment, vital electronic records and/or data).		
10	A disaster recovery plan is documented.		
11	The disaster recovery plan identifies recovery resources and a source for each.		
12	The disaster recovery plan contains step-by-step instructions for implementing the plan.		
13	The disaster recovery plan includes procedures for implementation of manual operations.		
14	An individual has been assigned to maintain the disaster recovery and business continuity plan to ensure currency.		
15	The business continuity and disaster recovery plans are tested annually.		
16	An uninterrupted power source (UPS) is in place to increase the possibility of an orderly shutdown without loss of data.		

**Backup Operations**

	Control/Statement	Current Implementation Level (0-5)	Action/Comment
1	Critical data are backed up on a scheduled basis (daily or weekly as appropriate).		
2	Backup media and data are stored off site in a secure, environmentally safe, locked facility accessible only to authorized agency representatives.		
3	Backup policies and procedures are in place.		
4	System and user backups are performed regularly.		
5	The names of individuals authorized to perform backups is documented.		
6	Backup media is tested regularly for restorability/recoverability of files.		
7	Policies and procedures are in place for archived data.		
8	Contracted service organizations agree to abide by designated security and confidentiality policies.		



**El Paso Community College  
Information Security  
Risk Assessment Survey**

**EPCC Information Security Risk Assessment Survey  
Appendix A**

**Personnel Resources**

List the names of personnel who have system access, administrative permissions, or other special privileged access to the critical resource. Include emergency support personnel.

Name	Function (primary support, emergency support, etc.)	Telephone	Supervisor



# El Paso Community College Information Security Risk Assessment Survey

## Appendix B

### Hardware and Equipment Resources

Complete this section if the critical resource is identified as hardware (communications equipment /devices, UPS systems, mini and microcomputers, disk and tape drives, printers, terminals, fax machines, modems, power supplies, etc.).

Describe Hardware/ Equipment:	
IP(s): Assigned static or "DHCP"	
Vendor:	
Version:	
System Administrator(s):	
Number of Workstation Installations attached to system (if applicable):	
Describe systems which are interdependent upon the critical resource for service or operation	
Physical Location (bldg, room)	
Other functions located in the same room (include any functions which are managed by other departments if applicable)	
Room Manager	

Describe Hardware/ Equipment:	
IP(s): Assigned static or "DHCP"	
Vendor:	
Version:	
System Administrator(s):	
Number of Workstation Installations attached to system (if applicable):	
Describe systems which are interdependent upon the critical resource for service or operation.	
Physical Location (bldg, room)	
Other functions located in the same room (include any functions which are managed by other departments if applicable)	
Room Manager	



# El Paso Community College Information Security Risk Assessment Survey

## Appendix C

### Software Resources

Complete this section if the critical resource is software (operating systems, databases, web and non-web applications, mail servers, firewalls, other security software, file maintenance software, communications systems software, etc.).

Name of Software/Application:	
Type/Role (see above)	
Commercial or Developed In-House	
Vendor:	
Version:	
System Administrator (s):	
Applications that restrict access to the software resource, if applicable (i.e. firewall, etc.)	

Name of Software/Application:	
Type/Role (see above)	
Commercial or Developed In-House	
Vendor:	
Version:	
System Administrator (s):	
Applications that restrict access to the software resource, if applicable (i.e. firewall, etc.)	