

**1. IA Partnerships:** Extending IA beyond the normal boundaries of the College/Institution and bringing current IA practitioners into the IA Center. Provide evidence of partnerships in IA education with 4-year schools, other Community Colleges, Two-Year Technical schools, K-12 schools, Industry Schools, Government Schools, Federal/State Agencies, Business, Industry or Non-profit organizations. Evidence must be in the form of an articulation agreement, Memorandum of Agreement, letters of endorsement, etc. between the schools. Articulation Agreements must be specific to IA programs. Partnership(s) may include: Shared curriculum and resources (IA teaching materials provided); shared faculty (faculty on curriculum committee for more than one institution); and reciprocity of credits.

**Overall Point Value: 10 minimum/20 maximum**

a. Shared Curriculum (e.g., IA teaching materials provided to technical schools, universities, community colleges, K-12 schools, etc.)

**Point Value: Up to 5 points**

**SUBMISSION:**

Rose State College and the other CSEC (Cyber Security Education Consortium) partners have adopted an academic degree or certificate program in Information Assurance (IA) and Digital Forensics (DF). The charter members of CSEC participate and develop workshops for all participating institutions and other state and federal agencies. Curriculum is shared with all members of the CSEC institutions. Leveraging partnerships with other universities, two-year colleges, and career and technology centers, opportunities to provide education and training throughout Oklahoma and other neighboring states is possible with Rose State College and the CSEC's partnerships. A link to our consortium page showing all member schools can be located at:

<http://www.cseconline.org>

Rose State College through CSEC has been able to reach out to not only Oklahoma schools but to schools in the Colorado, Missouri, Kansas, Arkansas, Tennessee, Texas and Louisiana areas.

The following institutions are partners in the operation of CSEC:

Oklahoma Career and Technology Education System  
Oklahoma City Community College  
Oklahoma State University - Information Technology Center  
University of Tulsa  
Butler Community College  
Johnson County Community College  
Manhattan Area Technical College  
Dodge City Community College  
Hutchinson Community College  
Kansas City Kansas Community College  
Collins College  
Richlands College  
Tarrant County College  
Pulaski Technical College  
Northwest Arkansas Community College  
Arkansas State University  
University of Arkansas Community College Batesville

Jackson State Community College  
Columbia State Community College  
Jackson State Community College  
Columbia State Community College  
Dyersburg State Community College  
Walters State Community College  
Northeast State Community College  
Nashville State Community College  
Southwest Tennessee Community College  
Pellissippi State Technical Community College  
Roane State Community College  
Cleveland State Community College  
Volunteer State Community College  
Arapahoe Community College  
Pueblo Community College  
Bossier Parish Community College  
Louisiana Technical College - Shreveport  
Sowela Technical Community College  
Louisiana Technical College - Sullivan  
Metropolitan Community College

Information Assurance and Digital Forensic Curriculum  
Memorandum of Agreement)

1. Oklahoma State University Institute of Technology
2. Mid-Del Career Tech

b. Shared Faculty (e.g., Faculty on curriculum development committee for more than one institution)

**Point Value: Up to 5 points**

**SUBMISSION:**

Rose State College along with CSEC has a curriculum work group that meets quarterly. This work group is responsible for the development, update and dissemination of CSEC-sponsored curriculum as well as training faculty from other institutions:

1. Robert Hamilton, Oklahoma Career Technology Education System
2. Dr. Tom Pigg, Jackson State Community College
3. Brett Weber, Rose State College
4. Ken Dewey, Rose State College
5. Eileen Dewey, Rose State College
6. Sujeet Sheno, Tulsa University

Rose State College is currently the lead curriculum developer for Digital Forensics and Mobile Communications. Rose State also is assisting another consortium member with their development of Secure Coding development.

c. Use of distance education technology and techniques to deliver IA courses. (Distance education includes live/delayed broadcasts, videotapes/CDs, lectures, and web-based IA courses.)

**Point Value: Up to 5 points**  
**SUBMISSION:**

Rose State College uses Desire To Learn (d2l) for all classes, on campus or distance, (visit <http://d2l.rose.edu>). Rose State also utilizes video lectures in the form of podcasts (visit Rose State Colleges 's iTunes University at: <https://deimos.apple.com/WebObjects/Core.woa/Browse/rose.edu>). Individual faculty also utilize their own faculty pages to deliver distance learning lectures (visit Professor Dewey's page at: <http://www.rose.edu/faculty/kdewey/rose/podcasts>)

Rose State College just introduced a new virtualization system allowing for distance learning opportunities for all colleges belonging to the CSEC partnership. A presentation showing the capabilities is available here: <http://cae2y.rose.edu/RSC-CSEC-Virtualization-April-2010.pdf>

d. Evidence the program is providing students with access to IA practitioners (Example: guest lecturers working in IA industry, government, faculty exchange program with industry and/or government, etc.)

**Point Value: Up to 5 points**  
**SUBMISSION:**

Rose State College supports many clubs. Students in the IA field established the Cyber Security club in 2006. The Cyber Security club provides many opportunities for students to get together and prepare for collegiate competitions as well as a forum for technical and business leaders to demonstrate products to our students. The Cyber Security club also participates in service-learning projects, giving students another avenue to get much needed hands-on training in the field of cyber security. The Rose State College Cyber Security Club was named the Club of the Year for 2010.

Rose State College has lecturers that present at our monthly meetings. Industry lecturers are brought in to cover current topics important to Cyber Security, IA and Digital Forensics. Rose State also assists in the delivery of IA courses to fellow consortium institutions. Lectures are also given on Information Assurance and Identity theft to numerous state and local organizations. During 2009, 6 lectures and 3 full classes were conducted.

Some of the most recent lecturers for the academic year of 2009-2010 include:

1. Tiffany Smith from the Midwest City Police Department Criminal Investigations Unit. She spoke on Forensics, crime scene analysis and numerous other topics.
2. Charles Thigpen from the United States Postal Investigation Unit. He spoke about postal security inspections and how they work to fight cyber crime.
3. Sean Satterlee (former NSA) is the Cyber Security Investigator for the Chickasaw Nation and will be speaking about security in gaming

institutions. He will also be giving a talk on Exploiting the Critical Space: The Art of Espionage.

4. Sujeet Shenoi (Tulsa University Cyber Corps Director) spoke on training Cyber McGyvers.

Internship opportunities are also given to our students during their last semesters here at Rose State College prior to graduation. The two biggest sponsors of these internships are:

1. FAA - The FAA at the Mike Monroney Aeronautical Center currently employs 7 of our students in either Internship or full time positions.
2. DISA - DISA Currently employs 2 Rose State College students, 1 in an internship position and 1 full time.
3. Dell - Dell currently employs 4 Rose State College students, 1 in an internship position and 3 full time.

Students are also encouraged to join and participate in the Oklahoma chapter of Infraguard (visit <http://www.infraguardok.org>)

---

**2. IA Student Development:** The program provides development opportunities for students that lead to a two year associate's degree or a certificate in an IA discipline.  
**Overall Point Value: 14 minimum/28 maximum**

a. Evidence of IA degrees/areas of study/track or certificates (For example: List of IA Associates degrees and/or certificates in IA curriculum as listed on the institution's website or catalog, list of all IA program courses with their descriptions).

**Point Value: 5 points**

**SUBMISSION:**

To understand the scope of student opportunities enjoyed by Rose State College students, it is important to understand the uniqueness of its setting. With 27,000 civilian and military personnel, Tinker Air Force Base is the largest air depot installation in the United States and the largest employer of the state of Oklahoma. Many of these employees and their dependents are Rose State College students. As Rose State College is located less than a mile from the gates, Rose State College has a long-standing relationship with the Base. Beginning in 1971, the College has been the preferred location for Tinker AFB training workshops. In 2009, the College hosted 14,000 individuals in credit and non-credit training in the Professional Education and Training Center. Approximately 90% of the training was Tinker AFB and related.

Rose State College had developed many courses which incorporate into the two-year associates degree and several CNSS certificates. Faculty members associated with CSEC have worked across several states to standardize

programs in the area of Cyber Security, Information Assurance and Digital Forensics.

1. Degrees:

Networking A.A.S. at RSC

(visit [http://www.rose.edu/students/degreeprog/BS\\_09-10/NETWORKING\\_2009-2010.pdf](http://www.rose.edu/students/degreeprog/BS_09-10/NETWORKING_2009-2010.pdf))

2. CyberSecurity A.A.S. at RSC

(visit [http://www.rose.edu/students/degreeprog/BS\\_09-10/NETWORKING - CYBERSECURITY OPTION\\_2009-2010.pdf](http://www.rose.edu/students/degreeprog/BS_09-10/NETWORKING - CYBERSECURITY OPTION_2009-2010.pdf))

3. Computer Information Technology A.A.S. at RSC

(visit [http://www.rose.edu/students/degreeprog/BS\\_09-10/COMPUTER INFORMATION TECHNOLOGY\\_2009-2010.pdf](http://www.rose.edu/students/degreeprog/BS_09-10/COMPUTER INFORMATION TECHNOLOGY_2009-2010.pdf))

Certificates: (visit <http://cybersecurity.rose.edu/infosecert.asp>)

1. NSTISSI 4011 - Information System Security Professional

2. CNSS 4012 - Senior System Managers

3. CNSS 4013 - System Administrators

4. CNSS 4014 - Information System Security Officer

5. CNSS 4015 - System Certifier

6. CNSS 4016 - Risk Analyst

The following is a link to course descriptions within the Network and Cyber Security degree plan:

<http://www.cybersecurity.rose.edu/Courses.asp>

**b. Evidence of Copies of Articulation/Transfer agreements with 4 yr institutions offering a concentration or IA degrees/areas of study/track or certificates.**

**Point Value: 5 points**

**SUBMISSION:**

The following Four-year Institutions have the most successful transfer agreement with Rose State College:

Oklahoma State University - Information Technology in Okmulgee

- Degree in Information Assurance and Forensics

- (visit <http://cae2y.rose.edu/OSUITAgreement.pdf>)

South Western Oklahoma State University

- Degree in Computer Science or Information Systems

- (visit <http://cae2y.rose.edu/SWOSUAgreement.pdf>)

In addition to the acceptance of associate in science and associate in arts transfer degree programs, Rose State College has entered into specific articulation agreements for specific programs such as Cyber Security, Applied Technology, Technical Supervision and Management, and others. Four-year institutions with which Rose State College holds articulation agreements include the College of Liberal Studies at the University of Oklahoma the

University of Central Oklahoma, East Central University, Northeastern Oklahoma State University, and others.

<http://www.okhighered.org/student-center/transfer-stdnts/course-transfer.shtml>

c. Articulation agreements with high schools to facilitate awareness and training for faculty/administration/students.

**Point Value: 2 points per school / 6 pts maximum**

**SUBMISSION:**

Rose State College works with area schools to facilitate awareness and training for faculty and students. Rose State College offers a 'Ticket to Rose' program for all area high school students in the Choctaw and Mid-Del area. Students completing certain programs at the technology center will obtain college credit toward the appropriate associate in applied science degree awarded by Rose State College.

Actual Articulation Agreement documents can be found on:

<http://cae2y.rose.edu/StudentDevelopment.asp>

1. Ticket to Rose (Free Scholarship for all Mid-Del High School students)
2. Mid-Del Technology Center (page 10)
3. Eastern Oklahoma County Technology Center (page 10)
4. Metro Technology Center (page 10)
5. Moore Norman Technology Center (page 10)
6. Gordon Cooper Technology Center (page 10)
7. Mid-Del Technology Center College Alliance Page

Rose State College also hosts workshops on Identity Theft, Risk Management and Forensic Toolkit training to local schools and other two-year institutions during in-service training. Schools that have participated in these training activities include:

1. Harrah Public Schools – Identity Theft and Risk Management
2. Mid-Del Schools – Identity Theft and Risk Management
3. Oklahoma City Community College – Access Data Certified Examiner Training
4. Pueblo Community College – Access Data Certified Examiner Training
5. Redlands Community College – Access Data Certified Examiner Training
6. Collins County Community College – Access Data Certified Examiner Training
7. Jacksonville Community College – Access Data Certified Examiner Training

d. Participation in Cyber/IA competitions.

**Point Value: 2 points per each / 6 pts maximum**

**SUBMISSION:**

1. Rose State College students participate in the DC3 challenge
2. Rose State hosted Cyber Defense competition 2007
3. Rose State hosted Cyber Defense competition 2008
4. Rose State hosted Cyber Defense competition 2009

Current competitions hosted by or assisted by the Rose State IA Program:

1. Cyber Security Invitational Competition – hosted by OSU-IT, Rose State Cyber Security students served as mentors to the technology students entered in the competition.
2. Skills USA – Rose State Cyber Security students mentored students in the area of Micro Hardware and Operating Systems and also in the area of Networking.

e. Courses containing “Hands-on” training or Lab training.

**Point Value: 2 points per course / 6 pts maximum**

**SUBMISSION:**

All the classes taught in the Rose State Cyber Security program utilize a “hands-on” portion and some type of lab training. The percentage of lab training has recently increased with the implementation of the virtualization infrastructure.

Courses that have a lab component:

1. [CIT 2323 Network Security](#)
2. [CIT 2563 Computer Security](#)
3. [CIT 2553 Computer and Networking Forensics](#)
4. [CIT 1503 Intro to Networks](#)
5. [CIT 1523 Micro Hardware and Operating Systems](#)
6. [CIT 2513 Secure Electronic Commerce](#)
7. [CIT 2603 Secure Auditing and Penetration Testing](#)

---

**3. IA as multidisciplinary subject:** The academic program demonstrates that IA is treated as a multidisciplinary subject with elements of IA knowledge incorporated into various disciplines.

**Overall Point Value: 10 minimim/15 maximum**

a. Evidence that IA is taught as modules in existing non-IA courses and that non-technical/non-IA students are being introduced to IA (For example: Non-technical/non-IA students are being introduced to IA concepts; e.g. business courses teaching Information Security modules, health courses – HIPAA regulations)

**Point Value: 5 points**

**SUBMISSION:**

The state of Oklahoma requires computer literacy which includes a module on basic Information Assurance (IA) which includes password protection, online

security, and backup/recovery. Other programs such as Rose State's Health Science courses also cover IA modules.

1. Health Science requires courses in the Health Science Health Information Technology area. Students are taught the basic confidentiality and 19 identifiers that have to be removed for a record to be considered "de-identified" by HIPAA. In our HSHI 1222 Directed Practice I, the mandatory orientation includes a HIPAA video tape and faculty confidentiality presentation before students can go on-site for clinicals. Likewise, our affiliation contracts require students to have HIPAA training before going out to participate in their clinical. Finally, on top of all that, the O. U. Medical Center requires their own HIPAA presentation before students can go to clinicals on-site there. In HSHI 2102 Health Information in Alternate Care Settings: Students learn that HIPAA is applicable in virtually all healthcare settings. In HSHI 1112 Legal Aspects of Health Information: Students learn about the privacy requirements under HIPAA. In HSHI 2332 Health Information Seminar: Students learn more about the securing requirements under HIPAA.
2. Radiography program students have a course component in the first semester of their professional curriculum which covers HIPAA and Confidentiality issues in the health care arena and work place. There are certain clinical education sites ( Norman Regional and the OUHSC) which require each student and faculty representing the college must go through their institutions HIPAA/Confidentiality training. Students may bring medical images from the clinical education sites to the campus for educational purposes. They must de-identify these images before leaving the medical facility. Students must also keep a log of the types of clinical exams they have been involved in each day. No names or medical record numbers are recorded on these logs, only the very specific exam (accession) number.
3. Paralegal Studies require courses that discuss federal and state statutes that cover certain acts such as Sarbanes Oxley, Gramm-Leach-Bliley Act, Patriot Act and issues in CyberLaw.
4. Business Administration requires courses that cover business law, business ethics and law and banking.
5. Management requires courses that cover E-Business Management and Law.

b. Evidence IA programs (certificate and/or degree programs) require non-technical courses of study; e.g. ethics, policy, and business.

**Point Value: 5 points**

**SUBMISSION:**

All Networking/Cyber Security A.A.S. degree students at Rose State are require to take several non-technical courses:



1. 6 credit hours in Communications, Literature (English Composition 1, English Composition 2 or Technical Report Writing).
2. 3 credit hours in College Algebra
3. 3 credit hours in Economics (Personal Finance, Micro or Macro Economics)
4. 3 credit hours in History (US History to 1877 or US History since 1877)
5. 3 credit hours in Political Science (American Federal Government)

c. Availability of non-credit/credit professional development courses in IA (e.g. First responders, K-12 teachers)

**Point Value: 5 points**

**SUBMISSION:**

As a member of CSEC, Rose State has assisted in the training of the Office of State Finance which includes First Responders and over 100 other state employees. This yearly seminar includes things like IA, Risk Assessment, Incident Response, Security Administration, National Cyber Incident Response, Security Audits, Table Tops.

Rose State is currently working with local High Schools to offer a seminar on Cyber Security and IA at local schools.

Other non-credit/credit professional development courses in IA that are available include:

- [Criminal Justice](http://www.rose.edu/students/degreeprog/SS_09-10/CRIMINAL%20JUSTICE,%20CRIMINAL%20JUSTICE%20OPTION,%20AA%20%20%202009-2010.pdf)  
([http://www.rose.edu/students/degreeprog/SS\\_09-10/CRIMINAL%20JUSTICE,%20CRIMINAL%20JUSTICE%20OPTION,%20AA%20%20%202009-2010.pdf](http://www.rose.edu/students/degreeprog/SS_09-10/CRIMINAL%20JUSTICE,%20CRIMINAL%20JUSTICE%20OPTION,%20AA%20%20%202009-2010.pdf))
- [Technical Supervision and Management](http://www.rose.edu/students/degreeprog/BS_09-10/TECHNICAL%20SUPERVISION%20AND%20MANAGEMENT%202009-2010.pdf)  
([http://www.rose.edu/students/degreeprog/BS\\_09-10/TECHNICAL%20SUPERVISION%20AND%20MANAGEMENT%202009-2010.pdf](http://www.rose.edu/students/degreeprog/BS_09-10/TECHNICAL%20SUPERVISION%20AND%20MANAGEMENT%202009-2010.pdf))

Rose State College also offers non-credit course in the Small Business Development Center and through the Continuing Education and Community Services

---

**4. IA Outreach:** The academic program must demonstrate a strong collaboration with business, industry, government, and the local community.

**Overall Point Value: 4 minimum/10 maximum**

a. Evidence provided in the form of a Strategic Plan and/or general IA Awareness Program description (example: flyers, letters from sponsors, etc), and/or workshop accomplishments. (For example: sponsorship of workshops for K-12, senior citizen groups, community colleges, technical schools, state homeland security, first responders, industry, etc.)

**Point Value: Up to 10 points**

**SUBMISSION:**

1. Rose State along with its CSEC partners put on the 5<sup>th</sup> Annual Oklahoma Cyber Security Seminar. This is a free 2 day seminar arranged by the Oklahoma Office of State Finance. This workshop is for state workings, first responders, and other technical employees of the Oklahoma state government.  
Agenda can be found at:  
(<http://cae2y.rose.edu/5thAnnualCyberSecuritySeminarAgenda.pdf>)
2. Rose State College faculty and students held an Identity theft seminar for Harrah Public Schools. Training was provided during in-service to faculty, staff, and select students on ways to protect their identity.
3. Rose State College faculty spoke on current cyber trends to a local organization, Tinker Business Industrial Park. Current issues affecting participants including Cyber Security, Identity Theft, Social Engineering were discussed.
4. Rose State College faculty spoke to the Mid Del Leadership Council on 2 separate occasions in the 2009-2010 calendar years. The Leadership Class is made of local business partners, civic leaders. A link showing the 2010 class graduates can be found at:  
[http://eastword.net/article/04-22-2010/Leadership\\_2010\\_class\\_graduates.aspx](http://eastword.net/article/04-22-2010/Leadership_2010_class_graduates.aspx)
5. Rose State College faculty and Cyber Security club members presented to numerous Student Success classes about Identity Theft and social engineering. These Success classes are made up of high risk students that are in danger of failing or are on academic probation. Faculty and students are asked to present each semester for numerous sections of this class as it fits perfectly into their curriculum.
6. Rose State College faculty and Cyber Security club members presented to numerous personal finance courses. These courses are a general education requirement for numerous programs at Rose State and the topic of Identity Theft is taught as numerous students are just now becoming adults and starting to open accounts, purchase online among other activities that could make them easy targets.
7. Rose State College faculty spoke at the Mid-Del Rotary on the subject of Cyber Security, Identity Theft, and Social Engineering.
8. Rose State College faculty spoke to the Del City Rotary on the subject of Cyber Security, Identity Theft, and Social Engineering.
9. Rose State College faculty spoke to the Non-Traditional Students Organization at Rose State College. This club is made up of primarily adult students the topics of Identity Theft and Social Engineering were requested as they are current topics affecting many students.
10. Rose State College faculty spoke to the local school news paper on the topics of Identity Theft and Social Engineering. The paper did an article about it. An article can be found at:  
<http://www.rose.edu/commfriend/15street/2-26-10.pdf>

**5. IA Faculty:** Faculty assigned specifically to teach and/or develop IA courses/curricula/modules.

**Overall Point Value: 11 minimum/15 maximum**

a. Identify by name faculty member with overall responsibility for the IA instructional program. Provide evidence, i.e. verification letter and/or job description.

**Point Value: 5 points (required)**

**SUBMISSION:**

Kenneth Dewey

Director/Professor Rose State College Cyber Security Program / Information Assurance Program

Professor Dewey is in charge of curriculum, classes, and faculty pertaining to the Rose State College Cyber Security Program

b. Identify by name additional IA faculty members teaching IA courses within the department that sponsors IA programs.

**Point Value: 1 pt per name / up to 5 maximum**

1. Kenneth Dewey
2. Eileen Dewey
3. Terry Byers
4. Arlene Haynes
5. Brett Weber
6. Satish Singhal
7. Calvin Smith (Adjunct)
8. Donna Shoemaker (Adjunct)
9. William Richards (Adjunct)
10. Christopher Yates (Adjunct)

c. Provide evidence in the form of curriculum vitae supporting the faculty member's qualifications to teach IA. At least one IA faculty member will be expected to be professionally certified with at least one of the IA certifications listed under DOD Directive 8570, such as CISSP, CPP, CISA, CISM, GIAC, etc. or a minimum of 9 hrs of graduate coursework and/or appropriate experience in a related field could be considered in lieu of a professional certification.

*Note: Can be same individual as 5a.*

*CISSP: Certified Information System Security Professional*

*CPP: Certified Protection Professional*

*CISA: Certified Information Systems Auditor*

*CISM: Certified Information System Security Manager*

*GIAC: Global Information Assurance Certification*

**Point Value: 5 points (required)**

**SUBMISSION:**

Kenneth C. Dewey

MS, MA, BS

CISSP, ACE, MCSE, ACE, Security+, A+, Net+, iNet+, CNA, CNSS 4011-4016

Director / Professor Rose State Cyber Security and Information Assurance Programs

Professor Dewey has also completed 46 hours of course work towards a Ph.D. in Information Assurance from Nova Southeastern University.

---

**6. Practice of IA encouraged throughout the Institution:** The academic program demonstrates how the institution encourages the practice of IA, not merely that IA is taught.

**Overall Point Value: 8 pts minimum/20 maximum**

a. Provide a link to the institution IA security plan and/or policies

**Point Value: Up to 5 points**

**SUBMISSION:**

The Rose State College IA Practices page can be found here:

<http://cae2y.rose.edu/IAPractices.asp>

Usage policies and samples are included in section c below.

b. Institution designated Information System Security Officer or equivalent. Provide name, position and job description for person or persons responsible for information security.

**Point Value: 5 points**

**SUBMISSION:**

Ms. Isabelle Billen is Director, Information Systems/Institutional Research, and is in charge of all user security related to the PeopleSoft ERP system. Core Duties: Develop and coordinate institutional research projects, develop institutional reports for state and federal reporting agencies, provide support to the institutional outcomes assessment program, and plan, organize, and schedule enterprise-wide applications and/or systems analysis projects. Oversees applications programming activities. Supervises work of employees engaged in developing, maintaining, and modifying programs use in the enterprise-wide applications. Manage and coordinate user security templates and settings in PeopleSoft.

Mr. Bradley Johnston is the Network Engineer, and shares responsibility for primary network infrastructure security.

Core Duties: Assists the Coordinator of Technical Services with network or security project planning, implementation, and upgrade; maintains and configures switches, routers, and firewalls; maintains network security infrastructure and software for the campus and all of its computer subsystems; maintains documentation for TCP/IP and network infrastructure settings and system diagrams; and troubleshoots network related problems.

Mr. James Johnston is ERP Systems Administrator, and shares responsibility for PeopleSoft ERP system hardware and primary network infrastructure security.

Core Duties: Primarily responsible for managing the Rose State College PeopleSoft servers and ERP-related equipment and software. Manage and support PeopleSoft servers, including upgrades and patches as needed. Support two-tier connectivity between ERP clients and servers. Manage and support the Cisco network load balancing systems connected to the ERP environment. Manage and maintain ERP-associated backup systems. Ensure proper and secure configuration of the PeopleSoft ERP hardware.

c. Provide evidence of the implementation of the institution IA security plan to encourage IA awareness throughout the campus. (Example: Students and faculty/staff are required to take computer based training or on-line tutorials; a security banner statement present on institution computers; security related help screens are available; institution-wide seminars are held on the

importance of IA, etc- 2pts awarded per item)

**Point Value: 2 minimum / 10 maximum**

**SUBMISSION:**

The Rose State College IA Practices page can be found here:  
<http://cae2y.rose.edu/IAPractices.asp>

Banners are used on all student computers reminding them about IA security and other topics along same lines. Banners are changed frequently.

The current banner says: Remember to always logoff when done and not to share personal information with anyone. Think Information Security!

A security training and awareness program is currently being updated via an Information Systems Policies and Procedures Committee on campus. The committee is hoping to have this completed by summer 2010.

The current Computer Use Policy states:

#### Computer and Network Use

The College provides computers, software, peripherals, and network services for use by RSC students, faculty, and staff to support academic and administrative functions. Personal use of these resources for other purposes is permitted when it does not consume a significant amount of these resources (to be determined by the network administrator), does not interfere with the performance of the user's job or other college responsibilities, and is otherwise in compliance with this policy.

These resources may not be used for personal commercial purposes or for personal financial or other gain. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

#### User guidelines:

1. Network logons are automatically created for each student upon enrollment. Faculty and staff (part-time or regular) may obtain a network logon upon request of the immediate supervisor. Students, faculty, and staff are responsible for any access code assigned to them, which includes not sharing any network or computer system logons and passwords. An access code includes any form of information used to authenticate, secure, or control electronic information technology resources.

Examples include network logon Ids, passwords, keys, and door codes.

2. Copyrighted software must only be used in accordance with its license or purchase agreement and must not be copied or altered except as permitted by law or by the software licensing agreement. ITS staff will install college-approved software on college-owned computers. Upon request, ITS staff will install personal software as long as it is licensed.

3. Inappropriate conduct that will not be tolerated includes, but is not limited to:

- Unauthorized access, alteration or destruction of another user's data, programs, electronic mail, or voice mail.

- Attempts to obtain unauthorized access to either local or remote computer systems or networks.

- Attempts to circumvent established security procedures or to obtain access privileges to which the user is not entitled.

- Obscene, offensive, threatening, harassing, or intimidating material entered into the computer and sent by electronic means.

- Intentional viewing of pictures of an erotic or sexual nature when such images can be viewed by others who are offended by them; and, mailing, printing, or copying obscene materials.

- Knowingly running, installing, or giving to another a program or data file which could be classified as or contain a computer virus, worm, or Trojan horse.

- Activities that embarrass, denigrate, or libel an individual or organization.

- Activities that imply College endorsement of any commercial products other than those approved by the appropriate Executive Council member.