Center for Information Assurance and Security Education
Security Plans

Policy Summary

A branch of the School of Information Systems and Applied Technology

College of Applied Sciences and Arts

Southern Illinois University Carbondale

National Centers of Academic Excellence

The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA Education (CAE/IAE) and CAE-Research (CAE-R) programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various disciplines. Designation as a CAE/IAE or CAE-R is valid for five academic years, after which the school must successfully reapply in order to retain its CAE designation.

Students attending these designated schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.

CAE/IAEs and CAE-Rs receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation's information systems.

Security Plans

As part of Criterion 3: University Encourages the Practice of IA in the requirements for CAE/IAE, Southern Illinois University Carbondale School of Information Systems and Applied Technology (ISAT) has developed a set of security policies that cover all aspects of security handling associated with assets and risks of the School. The intent of these policies is to summarize the involved entities and encourage best practices in Information Assurance.

Below is a list of the School security policies and a brief summary. These policies are not mandatory, but a definition of encouraged practices for faculty, staff, and students of ISAT.

Audit Policy	Encourage IA and outline internal audit practices to determine security benchmarks.
Clean Desk Policy	List of procedures for protecting information through simple, everyday office management tasks.
Data Backup Policy	Highlight of areas of information management where risk of data loss are not always considered.
Incident Response Policy	Procedures for reporting security incidents.
Information Asset Management Policy	Guidelines for ensuring secure information management.
Infrastructure Change Policy	Procedures for maintaining a stable environment and notifying the appropriate entities of changes.
Physical Security Policy	Steps for ensuring the security of physical assets.
Smart Browsing Policy	Guidelines for safe internet browsing.

References

NSA. (2010). *Criteria for Measurement for CAE/IAE*. Retrieved from National Security Agency: http://www.nsa.gov/ia/academic_outreach/nat_cae/cae_iae_program_criteria.shtml

NSA. (2010). *National Centers of Academic Excellence*. Retrieved from National Security Agency: http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml