POLICY PURPOSE:
This policy provides direction and support for managing the acquisition, development and maintenance of CSU information systems.

POLICY STATEMENT:
CSUN will integrate information security requirements into the software life cycle of information systems that contain protected data. The security requirements must identify controls that are needed to ensure confidentiality, integrity, and availability. These controls must be appropriate, cost-effective, and mitigate risks that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of the protected data.

RESOURCES AND REFERENCE MATERIALS:

500-14 Application Service Providers Security Requirement
Application Development Standard
Data Classification Standard
Patch Management Guideline

FURTHER INFORMATION:
Vice President for Information Technology and CIO

APPROVED BY THE PRESIDENT