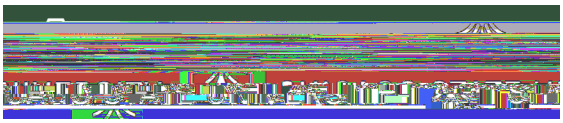


- include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

is the most senior University employee responsible for the security program and its operation.

is a major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

is the individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.

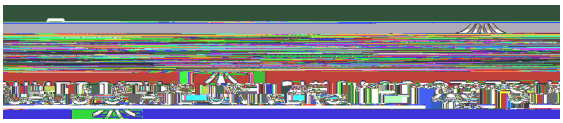
University's Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.

is a college, department, school, program, research center, business service center, or other operating Unit of the University.

is any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.

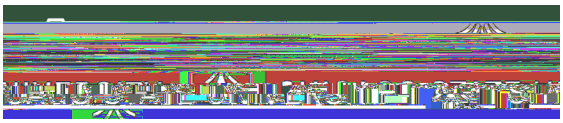
are University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University, and third-party contractors engaged by the University and their agents and employees.

is someone officially attached or connected to the College who is not a student or employee (e.g., contractors, vendors, interns, temporary staffing, volunteers.)



A security incident will be considered “high” if any of the following characteristics are present:

I. Threatens to impact (or does impact) systems critical to the University’s ability to function normally. This includes but is not limited to email, courseware, human resources, financials, internet connectivity, or portions of the campus network
II. Poses a serious threat of financial risk or legal liability
III. Threatens to expose (or does expose) “Confidential” data as defined by the Data Classification & Handling Policy
IV. Threatens to propagate to or attack other networks, or organizations internal or external to the University
V. Terroristic threatg62 ЭDC 2-0.0(t)(s)13 (e ()5 (o)-find (r)4 ( )1(T)ЭDC 011d (fi)4 (nd qTd( )Tum)8(i)Tc 01p



Policy Exceptions and Maintenance

Waivers from certain and specific policy provisions may be sought following the CSU Waiver Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted.

Enforcement

This Security Incident Response Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between CSU policies, they must be brought to the attention of CSU for immediate reconciliation.

Failure to report an information security incident may subject the user to disciplinary action including, but not limited, to suspension of the user's access to electronic information resources. Users also should be aware of other possible consequences under University policies and federal, state, or local laws, particularly those related to computer crime and copyright violation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

References