The University employs a variety of technical, physical, and administrative controls in an effort to maintain the confidentiality, integrity, and availability of information assets. However, the University cannot guarantee the confidentiality of all electronic data for the following reasons:

- End users may accidentally set improper permissions for access to their data stores
- Unauthorized access to data may occur due to compromised system security, compromised account credentials, or by the actions of a malicious employee
- Unencrypted electronic data is vulnerable to interception and inspection during transmission
- Data exfiltration by malware is commonplace
- Data may need to be accessed in the course of information system diagnostics or maintenance
- Data may need to be inspected in the course of an investigation into alleged policy violations or violations of the law
- The University may be compelled to disclose specific data to University police and/or other law enforcement agencies
- The University may need to access data post employee separation for the purposes of business continuity
- The University may, upon request, provide data to the next of kin of a deceased University community member

Information Resources’ staff does not routinely inspect the contents of electronic data or transmissions; specific work functions that are exceptions to this are described below.

**Inspection of Network Traffic and Server Logs**

As part of a comprehensive information security program, the Information Security Office employs programs that collect and/or analyze network traffic and information system logs exclusively for the following purposes:

- To detect unauthorized access to information systems
- To detect reconnaissance activities performed by malicious parties
- To detect and quarantine computing devices that have become infected with malware
- To identify and disable compromised accounts
- To detect and alert on security policy violations
- To provide the level of forensic readiness required by the Computer Security Incident Response Team
- To provide accountability as required by law
In addition, the Office of Network Infrastructure collects statistics related to the utilization of network services and applications for the purposes of capacity planning and performance engineering.

**Inspection of Data Stores**

As part of our data loss prevention program, the Information Security Office employs programs that scan and detect restricted data in our desktop environments and central file stores (Royal Drive). These scans are conducted exclusively for the purpose of locating and securing restricted data appropriately in the University’s systems.

No member of the Information Resources staff outside of the Computer Security Incident Response Team (CSIRT) is authorized to access individual data stores without first obtaining the explicit permission of the account owner. Inspection of data by CSIRT members will be guided by the principles stated above, and is restricted in scope to what is required by the investigative procedures published in the CSIRT Operational Standards manual.

Exceptions to this inspection policy may be granted when required by extenuating circumstances provided that requests for exceptions are formally documented, submitted to the Information Security Office, and approved by the Chief Information Officer in consultation with the appropriate Vice Presidents and Deans.

Approved by Jerome DeSanto, VP Planning & CIO

May 9, 2012
Revised June 2013