OM 9.2.3 - Misuse and Abuse of IT Resources

Scope
All Clarkson University units and employees.

Reason for Policy
Students, granting agencies, donors and other groups providing sources of funding that support information technology resources at Clarkson University expect that these assets will be used in a lawful manner and in support of instructional, research and service missions sanctioned by the University.

Policy Statement

Reporting
Reports of apparent misuse or abuse of Clarkson University information technology resources are to be made to the Office of the Chief Information Officer (CIO).

Suspension or termination of access
Service managers, system administrators, and security and network engineers may temporarily suspend or block access to an account when it reasonably appears necessary to do so in order to protect the integrity, security, and functionality of University or other computing resources, or to protect the University from liability.

The technician responsible for a particular service may disable access unilaterally if processes in an assigned account are causing or reasonably appear likely to cause damage to systems or data or serious service degradation for other users. Except when prohibited by law, inappropriate, or impractical, the technician will notify the involved individual prior to disabling the computer account. Where prior notification is not permitted, appropriate, or practical, the technician will make all efforts to notify the involved individual afterward in a timely manner. Unless other policies are invoked, access will be restored as soon as possible after the removal of the threat.

Technical Investigation
The Office of the CIO will coordinate technical investigation and computer forensics for complaints of misuse or abuse of University information technology resources. All investigations will comply with applicable law, and University policies and procedures.

Disciplinary Process
Reports of misuse or abuse are normally resolved through established University disciplinary policies and procedures applicable to the relevant user. The University may also refer suspected violations of applicable law on the part of any individual to appropriate law enforcement agencies. University Counsel, and other law enforcement officials as appropriate, shall address misuse or abuse of Clarkson University resources by persons not affiliated with the University.

Consultation
The Chief Information Officer (CIOs) is available to provide consultation or advice related to technology use or misuse to any University, campus, or unit administrators or individual personnel.

Definitions

*Information technology resources*—all University owned and operated computers, software, hardware, and infrastructure. It further includes all University services and programs such as email, course management systems, and web pages. It also includes:

1. Data and other files, including electronic mail, stored in or located or residing on (temporarily or otherwise) University-owned centrally-maintained systems, departmentally-maintained systems, and University-owned systems or computers.
2. University data and other files stored off campus in systems owned or operated by other entities. These systems may be subject to their own terms and conditions related to privacy and other matters.
3. Data communicated over University networks.

History

March 2018