OM 9.1.0 - Information Security

[ Scope ] [ Reason for Policy ] [ Policy Statement ] [ History ]

About This Policy

Effective Date: January 1, 2018
Last Updated: January 26, 2018
Responsible University Office: Office of Information Technology
Responsible University Administrator: Chief Information Officer
Policy Contact: Office of Information Technology
helpdesk@clarkson.edu

Scope

All Clarkson University units and employees.

Reason for Policy

To protect information that is non-public in nature, including personal information about individuals, institutional information, financial information and intellectual property, the University has established this Information Security Plan. This Plan is intended to incorporate compliance with all relevant laws and regulations and applies to all areas of the University and all third party contractors having access to University owned data, including IaaS /PaaS/SaaS providers, food services and the book store. Referenced laws and other regulation include but are not limited to:

Graham-Leach-Blilly Act (GLBA / 16 CFR 314)

The specific rules of GLBA addressed in the Plan are:

1. 16 CFR 314.4.a: “Designate an employee or employees to coordinate your information security program.”
   a. Clarkson designates this as the Director of Network Services and Information Security.
2. 16 CFR 314.4.b: “Identify reasonable foreseeable internal or external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including: (1) employee training and management; (2) information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) detecting, preventing and responding to attacks, intrusions, or other system failures.”
   a. This risk assessment is covered by OM 9.1.10 - Risk Assessment
3. 16 CFR 314.4.c: “Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguard’s key controls, systems, and procedures.”
   a. These safeguards are defined in sections 9.1.1-9.1.9 of the Operations Manual.
4. 16 CFR 314.4.d: “Oversee service providers, by: (1) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) requiring your service providers by contract to implement and maintain such safeguards.”
5. 16 CFR 314.4.e: “Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.”
   a. The Policy section of this page addresses review of the overall Information Security policy set of the University, including OM 9.1.5.4 - User Training

DMCA –

In accordance with the Digital Millennium Copyright Act, Clarkson University has designated an agent to receive notifications of alleged copyright infringement occurring on the Clarkson University computer network. Clarkson University’s response to notices of alleged infringement that comply with the DMCA [Title 17, United States Code, Section 512(c)(3)(A)] will include removal of or blocked access to the material named in the infringement notification. All other procedures outlined in the Copyright Policy will be followed.

NYS Information Security Breach and Notification Act (NYSISBNA) –
In accordance with the requirements set forth in the NYSISBNA, the University will disclose any breach of the security of a system containing private information following discovery or notification of the breach to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. In accordance with the NYSISBNA, the required notification may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. If such a determination has been made, then notification shall take place after such law enforcement agency determines that such notification does not compromise such investigation. Additionally, notification of the breach will be made to the New York State Consumer Protection Board, NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC), and the New York State Attorney General using the methods outlined by the NYS Office of CSCIC at this website: http://www.cscic.state.ny.us/security/securitybreach/index.htm.

Family Educational Rights and Privacy Act (FERPA) –

The Family Educational Rights and Privacy Act (FERPA) (20 USC 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. This law gives parents certain rights with respect to their children’s education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are “eligible students.” The rights of eligible students are outlined as part of the Clarkson University Student Regulations (VIII-I).

Technology, Education and Copyright Harmonization Act (TEACH) –

TEACH says that is is not copyright infringement for teachers and students at an accredited, nonprofit education institution to transmit performances and displays of copyrighted works as part of a course if certain conditions are met. If these conditions are not met or cannot be met, use of the material will have to qualify as fair use or permission from the copyright holder(s) must be obtained. The guidelines for University compliance in this aspect are outlined as part of the Copyright Policy.

Policy Statement

The implementation of the Information Security Program is divided across a number of area-specific policies. These polices as a group form the basis for the Program and are linked here.

- OM 9.1.1 - Physical Security
- OM 9.1.2 - Network Security
- OM 9.1.3 - Application Security
- OM 9.1.4 - Device Security
- OM 9.1.5 - User Account Security
- OM 9.1.6 - Data Security
- OM 9.1.7 - Outsourcing IT Services
- OM 9.1.8 - Incident Response Plan
- OM 9.1.10 - Risk Assessment
- OM 9.1.11 - Automated Controls Auditing

OM 9.1.0 - Information Security section of the University Operations Manual will be reviewed at least annually by the Office of Information Technology and changes made as needed based on current threats, regulation and industry mandates.

History

March 9, 2018
April 28, 2017
February 26, 2018 - formatting update