OM 9.1.8 - Incident Response Plan

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

Scope
All Clarkson University units and employees.

Reason for Policy
The need to respond to a data-security related incident is nearly inevitable for most organizations. This policy provides the requirements around such a plan.

Policy Statement
The Office of Information Technology will create and maintain an Incident Response Plan that includes the following information, guidance and directives:

- Roles, responsibilities and communication strategies for use in the event of a compromise
- Specific Incident Response procedures
- Data Backup processes
- Mechanism for consistent analysis of reporting requirements
- Coverage and responses for all critical system components
- Reference or inclusion of incident response procedures from various payment brands (PCI specific)
- Designates specific personnel responsible and available for responding to alerts on a 24/7 basis
- Indicates what automated security system alerts are to be included as a part of the IRP.

The IRP is to be reviewed at least annually. During this review, the IRP will be modified according to updated industry developments, legal and regulatory changes and best-practice lessons learned from prior incidents.

Additionally, any staff involved with security incident response are to be provided training appropriate to their IR role. This training should be reviewed and refreshed at least bi-annually.