

College Procedure: 701.16 – Incident Recovery Plan, Communications

Policy Reference: 701 – IT Security
Responsible Department: Information Technologies
Approval Authority: Cabinet
Procedure Owner: Vice President, Information Technologies
Effective Date: 08/21/2019

Version Number: 1
Legal Counsel Reviewed (yes/no): No
Scope: College-wide

Reason for Procedure

As part of an effective security program having a recovery plan and communication plan is important.

The Procedure

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. Restoration activities are coordinated with internal and external parties (e.g. Coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

References

NIST SECURITY FRAMEWORK

Revision Log

Table 1 Revision Log

Version Number	Date Approved	Approved by	Description of Change
1	08/21/2019	Cabinet	Procedure template