Gordon State College

Incident Response Collaborative Model

419 College Drive,
Barnesville, GA 30204
(800) 282-6504 or
(678) 359-5555

1. Event or Incident Requiring Collaboration

Critical incidents that require collaboration are incidents involving loss, damage, misuse of information assets, or improper dissemination of information. These incidents can be characterized as having an adverse impact on the College's reputation, financial position, information systems security posture, or health and safety of faculty, staff and students. Examples of incidents requiring collaboration:

- Unauthorized access to sensitive or confidential information (e.g., SS#, credit card #'s, any security breach involving Personally Identifiable Information)
- Suspected misuse of IS resources resulting in widespread compromise of information security
- Large scale intrusions or system attacks

2. Ad-Hoc Group Convenes via phone or live conference

- Director of IT – **(Point of Contact)**
- VP of Finance and Administration
- Compliance Officer
- Human Resources
- Information Security Officer
- Public Safety
- Public Information
- System Administrator
- President and Cabinet (Ex officio members)

2. Other resources to be considered on a situational basis:

- Unit Head of Affected Area
- Subject Matter Experts
- USG CISO
- USG Internal Audit
- USG Legal Affairs

3. Ad-hoc Group determines the resources necessary to reach a resolution on the incident.

3a Is this incident likely to result in criminal or civil legal action?

If the answer is yes, the path below should be pursued. If no, 3b should be followed.

Scope:
A decision needs to be made to determine the point at which Gordon State College will stop its internal investigation and hand it over to law enforcement and then to which law enforcement agency (e.g., FBI, GBI, Secret Service, and/or local law enforcement).

Review Method:
The standards of evidence for an investigation which is likely to result in criminal prosecution are far higher than those for which administrative action only is expected. For example, prior to any internal investigation of the machines involved, it would likely be appropriate to have law enforcement mirror the drives of machines, then turn the mirrored drives back to Gordon State for its internal investigation.

Investigation:
Coordinate with USG Cybersecurity, USG Internal Audit Office and Law Enforcement.

USG ITS Helpdesk
706-583-2001 / 1-888-875-3697
helpdesk@usg.edu

3b Is this incident unlikely to result in legal action and likely to result in administrative action that is localized within the College?

If yes, the following path should be pursued.

Scope:
A decision needs to be made at what level the investigation will take place and the standard of evidence that will be maintained. A decision will also need to be made regarding the point at which enough evidence has been obtained to satisfy the requirement to take appropriate administrative action.

Review Method:
The standards of evidence for an administrative investigation are less stringent than those which may result in legal actions but are important to maintain nonetheless. This ad hoc group must decide at what level evidence of the investigation should be documented.

Investigation:
As the internal investigation proceeds, the ad-hoc group must be cognizant of situations encountered which may change the examination from administrative to a potential legal investigation and take appropriate steps.

4. Assigning Investigation Oversight:

The ad-hoc group will determine which internal department will take the lead for coordinating the investigation and communicating the results. This designated lead group will:

- Coordinate all efforts related to the investigation
- Determine the custodians of data
- Have responsibility for reporting results and ensuring continuing lines of communication between departments, President, and Cabinet

5. Conducting the Investigation

The department or group with oversight of the investigation has the responsibility to communicate the results of the investigation and ensure, as soon as data on this incident relevant to the position of the Institute is uncovered, it reaches the executive decision makers.

6. Follow up and Reporting

The department or group with oversight of the investigation reconvenes the ad-hoc group at the end of the investigation and reports on

- The outcome of the investigation
- Lessons learned (how the process worked)
- Cost of incident (in hard costs and personnel time devoted to the incident response)
- Discuss methods to prevent future incidents

Board of Regents Ethics and Compliance Hotline:
1-877-516-3466
bor.alertline.com/gcs/welcome

Gordon State Ethics and Compliance Hotline:
1-877-516-3454
gdn.alertline.com/gcs/welcome

Reference:
USG IT Handbook Section 5.3

USG Incident Response and Reporting Standard

09/18/2018