Security Incident Response Flowchart

Communicate. Provide initial notification of the breach to the affected system's proprietor and custodian, the appropriate campus IT security response team, and any other people required by the circumstances. Provide updates as appropriate throughout the incident response process.

Start the log of actions taken. This log must be maintained consistently through the response process.

Secure the area. Electronic evidence can be very perishable and can be easily destroyed, resulting in an inability to determine if restricted information has been compromised, or to prosecute. Visually identify potential evidence, both conventional (physical) and electronic, and determine if perishable evidence exists. Take care not to alter the condition of any electronic device: If it is off, leave it off. If it is on, leave it on. Inventory and evaluate the scene.

Assess the need for forensic information. Surreptitious packet traces and system monitoring utilities can contribute understanding the nature and scope of the incident and can aid a potential criminal investigation. The factors to consider include the potential value of forensic information *vs*. the immediate need to protect and restore University resources and services. Document your decision.

Collect forensic information. Collect the evidence considered to be appropriate in the previous step.

Regain control. Once required forensic information has been collected, regain control of the compromised system. This may include network disconnection, process termination, system shutdown, *etc*.

Analyze the intrusion. Understand and document the nature of the intrusion and its impact on information and process integrity. Determine if restricted information may have been acquired by unauthorized individuals. Determine what address information is available for individuals whose data may have been acquired by unauthorized individuals. Estimate the potential cost, *e.g.*, dollars, reputation, and resources, of the intrusion to the University. (A cost estimate may be required to involve law enforcement.)

Notification?
Is there a possibility notification will be required?

Submit repggrouport. Notify the executive notification team (executive management, legal counsel, public affairs, executive IT leadership, *etc*.), and the Associate Vice President – Information Resources and Communications if there is a possibility that public disclosure will be required. Keep communication open as vulnerabilities are corrected.

Determine if notification is required. Work with the executive notification team to determine whether to make a public disclosure of the incident. This will require ongoing communication with the team that is correcting the vulnerabilities that enabled the incident.

Make public disclosures. Once the nature and scope of the incident are sufficiently understood, public disclosures can be made.

Correct system or application vulnerabilities. Correct the condition that allowed the intrusion to occur. Inform the executive notification team of any new inforamtion that may affect notification.

Restore the service. Once vulnerabilities have been resolved, restore service.