INDIANA UNIVERSITY

IT Incident Response Procedures

International Networks

(office/department)

1. A person who notices an incident
   - Some types of incidents that may warrant action/investigation are: slow or non-responsive systems, new errors/messages, programs constantly crashing, unauthorized access, break-in attempts, inadequate protection controls, or inadvertent disclosure.

2. Step away from the computer. Do not touch it or attempt to login or alter it. Do not power it off. These actions will delete forensic evidence that may be critical to your incident.

3. That person notifies IRNOC NOC (irncnoc@globalnoc.iu.edu) _____
   [appropriate party]

4. If IRNOC NOC (irncnoc@globalnoc.iu.edu) _____ cannot be reached, notify Hans Addleman (addlema@iu.edu) _____
   [appropriate party] *[this person]*
   or Andrew Lee (leea@iu.edu) _____.
   [this person]

5. Hans Addleman _____ will collect information (**without using the system**)
   [person/party]
   If it can be done quickly, such as: scope of the issue, type of compromise, names and IP addresses of machines, approximate date/time of compromise (if known), and usernames of users and system administrators of the machine.

6. Hans Addleman _____ *[person/party]* will then notify:
   - Director Jennifer Schopf / Associate Director Andrew Lee _____ *[management]*
   - The University Information Policy Office (UIPO).
     i. Contact procedures for the UIPO are detailed: https://protect.iu.edu/online-safety/report-incident/sensitive-data-breaches.html

7. The UIPO will work with the department's IT staff to coordinate response and forensic investigation, as necessary. They will use the UIPO sensitive data incident response checklist and toolkit. Details about the incident and response will be documented in their tracking system.

8. Specifically for production services like websites: plan remedial action to restore service, and when. Consider bringing up a new machine to host the site - or posting a "down for maintenance" banner.

9. Incident team will review steps taken in response to attempt to prevent future incidents.