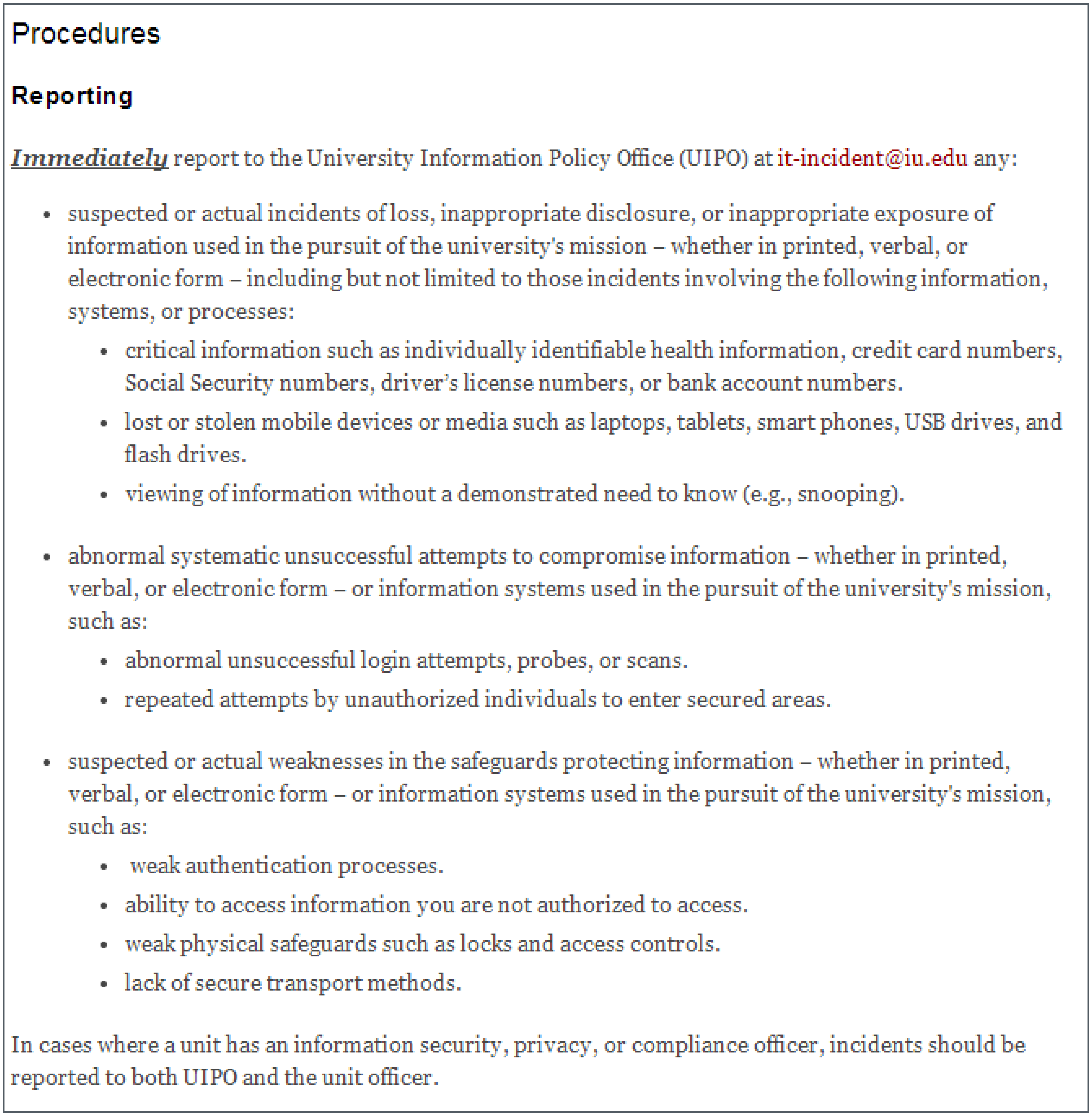
Artifact B: Indiana University Breach Reporting Guidelines



Procedures

Reporting

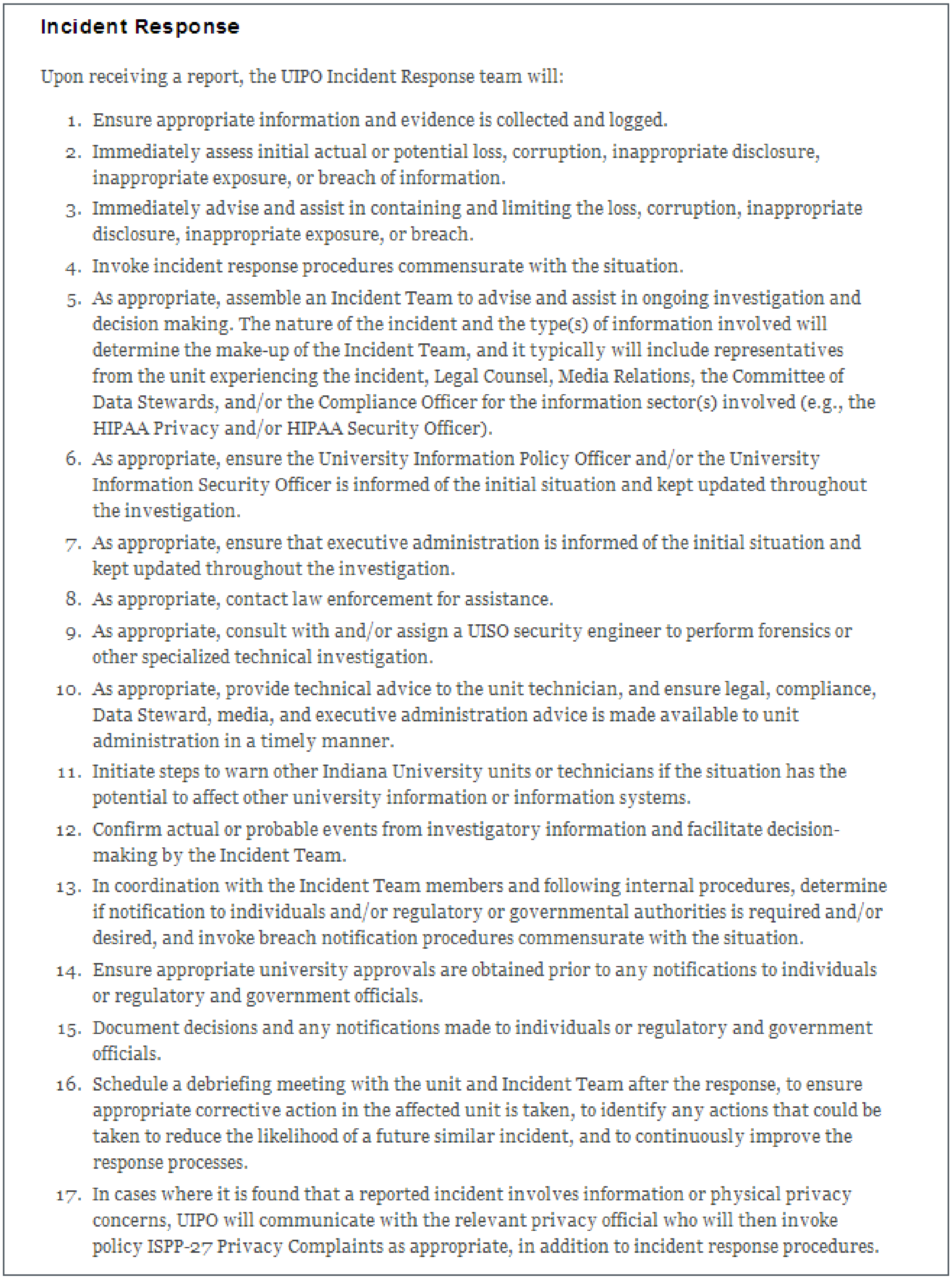
Immediately report to the University Information Policy Office (UIPO) at it-incident@iu.edu any:

- suspected or actual incidents of loss, inappropriate disclosure, or inappropriate exposure of information used in the pursuit of the university's mission – whether in printed, verbal, or electronic form – including but not limited to those incidents involving the following information, systems, or processes:
  - critical information such as individually identifiable health information, credit card numbers, Social Security numbers, driver's license numbers, or bank account numbers.
  - lost or stolen mobile devices or media such as laptops, tablets, smart phones, USB drives, and flash drives.
  - viewing of information without a demonstrated need to know (e.g., snooping).
- abnormal systematic unsuccessful attempts to compromise information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission, such as:
  - abnormal unsuccessful login attempts, probes, or scans.
  - repeated attempts by unauthorized individuals to enter secured areas.
- suspected or actual weaknesses in the safeguards protecting information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission, such as:
  - weak authentication processes.
  - ability to access information you are not authorized to access.
  - weak physical safeguards such as locks and access controls.
  - lack of secure transport methods.

In cases where a unit has an information security, privacy, or compliance officer, incidents should be reported to both UIPO and the unit officer.

Information and Information System Incident Reporting, Management, and Breach Notification, http://policies.iu.edu/policies/categories/information-it/ispp/ISPP-26.shtml.

Artifact C: Indiana University Breach Response Guidelines



Incident Response

Upon receiving a report, the UIPO Incident Response team will:

1. Ensure appropriate information and evidence is collected and logged.
2. Immediately assess initial actual or potential loss, corruption, inappropriate disclosure, inappropriate exposure, or breach of information.
3. Immediately advise and assist in containing and limiting the loss, corruption, inappropriate disclosure, inappropriate exposure, or breach.
4. Invoke incident response procedures commensurate with the situation.
5. As appropriate, assemble an Incident Team to advise and assist in ongoing investigation and decision making. The nature of the incident and the type(s) of information involved will determine the make-up of the Incident Team, and it typically will include representatives from the unit experiencing the incident, Legal Counsel, Media Relations, the Committee of Data Stewards, and/or the Compliance Officer for the information sector(s) involved (e.g., the HIPAA Privacy and/or HIPAA Security Officer).
6. As appropriate, ensure the University Information Policy Officer and/or the University Information Security Officer is informed of the initial situation and kept updated throughout the investigation.
7. As appropriate, ensure that executive administration is informed of the initial situation and kept updated throughout the investigation.
8. As appropriate, contact law enforcement for assistance.
9. As appropriate, consult with and/or assign a UISO security engineer to perform forensics or other specialized technical investigation.
10. As appropriate, provide technical advice to the unit technician, and ensure legal, compliance, Data Steward, media, and executive administration advice is made available to unit administration in a timely manner.
11. Initiate steps to warn other Indiana University units or technicians if the situation has the potential to affect other university information or information systems.
12. Confirm actual or probable events from investigatory information and facilitate decision-making by the Incident Team.
13. In coordination with the Incident Team members and following internal procedures, determine if notification to individuals and/or regulatory or governmental authorities is required and/or desired, and invoke breach notification procedures commensurate with the situation.
14. Ensure appropriate university approvals are obtained prior to any notifications to individuals or regulatory and government officials.
15. Document decisions and any notifications made to individuals or regulatory and government officials.
16. Schedule a debriefing meeting with the unit and Incident Team after the response, to ensure appropriate corrective action in the affected unit is taken, to identify any actions that could be taken to reduce the likelihood of a future similar incident, and to continuously improve the response processes.
17. In cases where it is found that a reported incident involves information or physical privacy concerns, UIPO will communicate with the relevant privacy official who will then invoke policy ISPP-27 Privacy Complaints as appropriate, in addition to incident response procedures.

Information and Information System Incident Reporting, Management, and Breach Notification, http://policies.iu.edu/policies/categories/information-it/ispp/ISPP-26.shtml.