Report an Incident

Are you in a panic because you suspect an incident?

Go to the First Response Checklist for immediate help.

Administrative Policy Statement 2.5 states that UW employees "must report an unforeseen event, a potential or confirmed breach of personal data, or an information security incident promptly to the office responsible for responding to and/or managing the incident."

1. Review the information below.
2. Refer to the First Response Checklist for guidance in handling the incident.
3. Also see the First Response Guide if you are a system administrator or system owner.

SCOPE

This policy applies to:

- All areas of the University
- All workforce members
- All information except United States government classified information
- All mediums for storing or processing information regardless of who owns, operates, or manages the medium

---

To report an incident involving:

1. **Personal data other than Protected Health Information or Human Subjects data:**
   See the UW Privacy Office's Report an Incident web page, contact uwprivacy@uw.edu, or call 206-616-1238.

2. **Human Subject Information and Reportable New Information for Research:**
   See Human Subjects Division Guide to Reporting New Information.

3. **Protected Health Information at Health Sciences Healthcare Components:**
   Contact Health Sciences Administration at 206-543-0702.

4. **Protected Health Information at UW Medicine:**
   Contact UW Medicine Compliance at comply@uw.edu or 206-543-3098 (local) or 855-211-6193 (toll free).

5. **Information security and/or Export Controls (other than Covered Defense Information):**
   Contact the Office of the Chief Information Security Officer (CISO) at ciso@uw.edu or 206-685-0116.

6. **National Security Classified Information and/or Covered Defense Information:**
   Contact the University Facility Security Officer at uwfso@uw.edu.

Each individual with delegated authority for incidents is responsible for developing, maintaining, and following an incident management process as defined in APS 2.5: Information Security and Privacy: Incident Reporting and Management. The Office of the CISO will coordinate with other delegate authorities, if needed, to manage the incident response process.

DO & DON'T

Do

- Report all information security incidents as soon as possible.
- Isolate the affected system to prevent further intrusion, release of data, etc.
- Limit sharing of information to individuals who have responsibility for managing and addressing the incident.
- Be clear about the facts versus assumptions or speculations.
- Document only information that has been substantiated.
- Mark documents as "draft" until finalized.
- Preserve all pertinent systems logs.
- Identify all systems and departments that connect to the affected system.

Don't

- Delete, move, or alter files on the affected system.
- Send any notifications before consulting with the appropriate delegated authorities listed above.
- Communicate that there is a potential or confirmed breach to individuals who are not:
    - Contributing facts or are decision makers.
    - Involved in the incident management process.
    - Impacted by the breach.
- Contact or retaliate against the individual(s) who may have caused the event/incident.
- Conduct your own forensic analysis.

WHAT TO REPORT

Please provide the following data when reporting an incident:

- When did the event occur?
- What type(s) of data are involved?
- How many records are involved?
- Was the data encrypted?
- What system(s), if any, are involved?
- What organization(s) or unit(s) are involved?
- Are there system logs that need to be preserved?
- Is the system deemed critical to operations?
- What was the root cause of the incident (if known)?
- Please provide contact information for your IT support person (if applicable).
- Name(s) of individual(s) at the UW who know or have been informed about the event/incident.