### Purpose:
This policy formalizes the requirements for reporting and responding to information security incidents. Prompt and consistent reporting of information security incidents is necessary to protect and preserve university information resources and data.

### Policy:
All suspected information security incidents must be reported promptly to the appropriate university office or party.

Information Technology will define standard methods for identifying, reporting, and responding to information security incidents.

### Documentation:
All data collected and/or used as part of the Information System Security Incident process and related procedures will be formally documented and securely maintained.

### Scope/Applicability:
This policy applies to all users of information systems or data at the OU Health Sciences Center and University Health Care Components.

### Regulatory Reference:
- HIPAA 45 CFR 164.308(a)(1)(ii)(B)
- 16 CFR Part 314 Standards for Safeguarding Customer Information

### Definitions:
See the Information Security Policy Definitions document for definitions

### Responsible Department:
Information Technology

### Enforcement/Audit:
The university’s Internal Auditing department is responsible for monitoring and enforcement of this policy.

### Related Policies:
- Information Security Incident Reporting Standard

### Procedures:
See Information Security Incident Reporting Standard

### Renewal/Review:
This policy is to be reviewed and updated as needed by IT Information Security Services.