# Information Technology (IT) Security

## University Policy

THE OHIO STATE UNIVERSITY

Applies to: Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and other affiliates who are acting on behalf of the university

| Responsible Office | Office of Technology and Digital Innovation |
|---|---|

## POLICY

Issued:      08/18/2010
Revised:    02/04/2025

The university recognizes that **information security** is vital to accomplishing its mission. Therefore, members of the university community have an individual and shared responsibility to protect the university's **information assets** and comply with applicable laws, regulations, policies, and standards.

### Purpose of the Policy

To set forth requirements for protecting the university's information assets and for reporting and responding to **information security incidents**.

### Definitions

| Term | Definition |
|---|---|
| Data | Information created, collected, maintained, transmitted, or recorded by or for the university to conduct university operations. It includes (a) research data and (b) data used for planning, managing, operating, controlling, or auditing university functions, operations, and mission, but does not include personally created data. Institutional data includes, but is not limited to, information in paper, electronic, audio, and visual formats. |
| Disaster recovery (DR) | The activities and program that allow the university to maintain, resume, or restore mission-critical systems and infrastructure following a disruption of information technology services. |
| Email phishing | Email scams where the attacker attempts to trick an individual into giving them their credentials or access to their system. |
| Incident response team | One or more teams of individuals who investigates an information security incident. |
| Information assets | Infrastructure, information systems, software, or institutional data. |
| Information security | The protection of information assets from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. |
| Information security incident | A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, potential breach, modification, or destruction of information whether accidental or malicious; an interference with information technology operations; or a significant violation of the Responsible Use of University Computing and Network Resources policy. |
| Misuse | Any situation where university information is used in a manner inconsistent with laws, regulations, or university policies. This may include intentional violations or unintentional errors in safeguarding or disseminating information. |
| Reportable breach | An information security incident which requires the university to notify impacted individuals or organizations in accordance with applicable laws, contractual agreements, industry regulations, or university policy. |
| Unit | College or administrative unit. |

Applies to:  Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and other affiliates who are acting on behalf of the university.

## Policy Details

I. Information Security Overview
   A. The university maintains a comprehensive, institution-wide information security program which incorporates cybersecurity, information security risk management, privacy, and disaster recovery.
   B. A key component of protecting the university's information assets is the classification of institutional data into four levels based on the data's sensitivity and regulatory requirements as detailed in the university's [Institutional Data policy](#).

II. Information Security Incident Response Management
   A. The university maintains processes to minimize the impact of information security incidents on the university's information assets. These processes limit the negative consequences to both the university and individuals and improve the university's ability to promptly restore operations affected by such incidents.
   B. The university also maintains processes for potential data breach review. Such processes evaluate information security incidents and consider breach reporting and notification requirements that may be triggered due to contractual obligations and/or laws and regulations.

## PROCEDURE

Issued:       08/18/2010
Revised:     02/04/2025

I. Information Security
   A. Cybersecurity and Risk Management
      1. Digital Security and Trust within the Office of Technology and Digital Innovation (OTDI) maintains the university's cybersecurity risk management framework which manages information security risk to the university's information assets.
      2. The university's [Information Security Standard (ISS)](#) and the [Information Security Control Requirements (ISCR)](#) are key aspects of the framework and set forth the university's minimum security and disaster recovery requirements.
         a. These requirements are adapted from the National Institute of Standards and Technology (NIST) cybersecurity, privacy, and risk management frameworks and incorporate NIST standards related to disaster recovery planning for information systems.
         b. As set forth in the ISCR, units must assign information security roles. Information security roles must include (at a minimum) a unit information security coordinator.
      3. Digital Security and Trust assesses compliance with the framework, identifies risks, and shares assessment outcomes as appropriate with others who have a shared responsibility for information security at the university.
   B. Privacy
      1. Digital Security and Trust maintains the university's privacy program in coordination with partners and units across the university.
      2. The privacy program aims to protect the confidentiality, integrity, and availability of university information through the development and use of privacy procedures and best practices.
   C. Disaster Recovery Program
      1. Digital Security and Trust maintains the university's disaster recovery program in coordination with units and their business continuity plan(s) across the university.
      2. The disaster recovery program assists the university in preparing for, responding to, and recovering from disruptions or disasters that affect the university's information assets to minimize downtime, data loss, and overall impact on operations.
   D. Training
      1. Institutional data users must complete the training outlined in the [Institutional Data policy](#).

Applies to:  Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and other affiliates who are acting on behalf of the university.

2.  Individuals must take appropriate data security and/or privacy training as assigned by the university.

II.  Information Security Incident Response Management
   A.  Duty to report
      1.  All individuals must immediately report information security incidents to their information security coordinator, security@osu.edu, or issecurity@osumc.edu.
      2.  Examples of information security incidents that must be reported include, but are not limited to, **email phishing**, sending data to unintended recipients, and suspected or actual unauthorized access.
   B.  Processes
      1.  The university's chief information security officer or their appointed designees publish information security incident response management procedures as needed to support proper reporting and handling of information security incidents.
      2.  Each unit with institutional data, as defined in the Institutional Data policy, must:
         a.  Maintain an information security incident response plan that complies with the requirements set forth in the Information Security Incident Response Management Process as well as federal and state information security regulations and contractual agreements that apply to the institutional data each unit possesses and
         b.  Notify the Digital Security and Trust **incident response team** of information security incidents as required by the Information Security Incident Response Management Process or as defined in II(A)(1).
   C.  Potential breach review
      1.  The university's Data Incident Response Team (DIRT) evaluates information security incidents and determines whether the information security incidents have resulted in a **reportable breach** that requires notification to impacted individuals, agencies, or organizations in accordance with applicable laws, contractual agreements, industry regulations, or university policy.
      2.  The Health Insurance Portability and Accountability Act (HIPAA) Potential Breach Notification Committee at The Ohio State University Wexner Medical Center evaluates and responds to potential breaches of protected health information across the university in accordance with HIPAA regulations.

III.  Policy Violations
   A.  Data users who violate this policy may be:
      1.  Denied access to university computing resources.
      2.  Subject to corrective or disciplinary action, up to and including termination or dismissal, in accordance with applicable policies or rules for violations of this policy.
      3.  Subject to civil litigation or criminal prosecution depending on the circumstances.
   B.  The university may temporarily suspend or block access to university computing resources prior to the initiation or completion of corrective or disciplinary procedures.
   C.  The university may refer or be required to refer suspected violations of applicable law to appropriate law enforcement agencies.

Applies to:  Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and other affiliates who are acting on behalf of the university.

## Responsibilities

| Position or Office | Responsibilities |
|---|---|
| Chief Information Security Officer or designees | Publish information security incident response management procedures as needed to support proper reporting and handling of information security incidents. |
| Data Incident Response Team (DIRT) | Evaluate information security incidents, determine if a reportable breach has occurred, and facilitate university response as set forth in the policy. |
| Disaster recovery program | Assist the university in preparing for, responding to, and recovering from disruptions or disasters affecting the university's information assets. |
| HIPAA Potential Breach Notification Committee | Evaluates and respond to potential breaches of protected health information in accordance with HIPAA regulations. |
| Incident response teams | Investigate information security incidents and facilitate appropriate response. |
| Individuals to whom this policy applies | 1. Protect the university's information assets and comply with applicable laws, regulations, policies, and standards.<br>2. Complete university required information security and/or privacy training as assigned by the university.<br>3. Report potential information security incidents as set forth in the policy. |
| Office of Technology and Digital Innovation, Digital Security and Trust | 1. Assess compliance with the cybersecurity risk management framework, identify risks, and share assessment outcomes as appropriate.<br>2. Maintain the university's privacy program in coordination with partners and units across university.<br>3. Maintain the university's disaster recovery program in coordination with units and their business continuity plan(s). |
| Privacy program | Develop and use privacy procedures and best practices to protect the confidentiality, integrity, and availability of university information. |
| Units | 1. Assign information security roles including, at a minimum, a unit information security coordinator.<br>2. Coordinate with Digital Security and Trust to maintain the university's privacy program.<br>3. Maintain an information security incident response plan for unit as set forth in the policy.<br>4. Notify OTDI's Digital Security and Trust incident response team of information security incidents as set forth in this policy. |
| University | 1. Notify impacted individuals or organizations of a reportable breach as set forth in the policy.<br>2. Maintain comprehensive, institution-wide information security program.<br>3. Maintain processes to minimize impact of information security incidents on university's information assets.<br>4. Maintain processes for potential data breach review.<br>5. Assign appropriate data security and/or privacy training. |

## Resources

University Policies, policies.osu.edu
   Business Continuity Management, go.osu.edu/bcm-policy
   Disaster Preparedness and University State of Emergency, 6.17, hr.osu.edu/wp-content/uploads/policy617.pdf
   Identity Theft Red Flags, go.osu.edu/itrf-policy
   Institutional Data, go.osu.edu/idp
   Payment Card Compliance, go.osu.edu/payment-card-compliance-policy
   Privacy and Release of Student Education Records, go.osu.edu/student-records-policy
   Protected Health Information and HIPAA, go.osu.edu/phi-hipaa-policy
   Public Records, go.osu.edu/public-records-policy
   Research Data, go.osu.edu/researchdatapolicy
   Responsible Use of University Computing and Network Resources, go.osu.edu/rup
   Whistleblower, 1.40, hr.osu.edu/wp-content/uploads/policy140.pdf

Applies to: Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and other affiliates who are acting on behalf of the university.

Information Security Standards and Requirements
Information Security Control Requirements (ISCR), it.osu.edu/iscrweb
Information Security Incident Response Management Process,
it.osu.edu/system/files/2022/12/osu_information_security_incident_response_management_process.pdf
Information Security Standard (ISS), go.osu.edu/infosec-iss

Additional Guidance
Cybersecurity4You, cybersecurity4you.osu.edu
Business Continuity Governance, busfin.osu.edu/university-business/risk-management/business-continuity-management/business-continuity-governance
Data Governance Program, go.osu.edu/datagovernance
Disaster Recovery Program, it.osu.edu/offerings/cybersecurity/services/disaster-recovery
Ethics Point, ohio-state.ethicspoint.com
HIPAA Privacy and IT Security Contacts, it.osu.edu/privacy/report-privacy-concern
Institutional Data Elements Classification Assignments, go.osu.edu/idp-elements
National Institute of Standards and Technology (NIST) Risk Management Framework, csrc.nist.gov/projects/risk-management/about-rmf
Research Event Reporting, research.osu.edu/research-responsibilities-and-compliance/human-subjects/event-reporting
Ohio State Privacy Principles, privacy.osu.edu
Ohio State Shared Values, osu.edu/shared-values
Patient Health Information and HIPAA Policy Information, wexnermedical.osu.edu/healthcare-professionals/phi-hipaa-policy
Research Health Information, it.osu.edu/security/research-support/research-health-information
Student Analytics Privacy Principles, it.osu.edu/privacy/learn-about-privacy-principles
OSU Records Management, go.osu.edu/records
Youth Privacy Principles, it.osu.edu/privacy/youth-privacy-principles

## Contacts

| Subject | Office | Telephone | E-mail/URL |
|---|---|---|---|
| Policy questions | Office of Technology and Digital Innovation, Digital Security and Trust | (614) 292-1385 | otdi-dst@osu.edu |

## History

| | |
|---|---|
| Interim Issued: | 08/18/2010 |
| Revised: | 03/01/2011 |
| Edited: | 05/13/2011 |
| Edited: | 07/11/2011 |
| Reviewed: | 05/06/2015 |
| Edited: | 06/29/2015 |
| Reviewed: | 05/16/2016 |
| Edited: | 12/16/2021 |
| Revised: | 02/04/2025 |