Information Security

Data Classification

The purpose of our Information Security Policy is to protect the confidentiality, integrity, and availability of Institutional Data, as well as any Information Systems that store, process, or transmit Institutional Data at Marshall University. This classification system ensures that data is handled appropriately based on its sensitivity and associated risks.

Public Data

Data classified as Public poses little or no risk to the University or its agents if disclosed, altered, or destroyed without authorization.

Examples of Data

- Campus Maps
- Event Announcements
- Press Releases
- Public Record Information
- Course Information

Scenario: A university staff member publishes a press release about upcoming campus events. This data is classified as public and can be shared freely without restrictions.

Private Data

Data classified as Private poses a moderate risk to the University or its agents if disclosed, altered, or destroyed without authorization.

Examples of Data

- University budget details
- Procurement information
- Research Proposals
- Internal Audit Reports
- Limited Directory Information

Scenario: A university employee accesses internal audit reports to prepare for a compliance review. The data is treated as private and stored securely using Adobe Acrobat Pro DC or SharePoint.

Restricted Data

Data classified as Restricted poses a significant risk to the University or its agents if disclosed, altered, or destroyed without authorization.

Examples of Data

- Student advising information
- FERPA-protected student information
- HIPAA-protected health information
- Donor details
- Employee personnel information
- Data protected by confidentiality agreements
- Building utilities and life safety information

Scenario: Handling Student Financial Aid Information
A financial aid officer at Marshall University is tasked with processing student loan applications. This involves accessing sensitive data such as students' Social Security numbers, loan amounts, and bank account details.

Use of Policy

Access Control: Accessing the data through a secure SharePoint site, which is restricted to authorized personnel only. Visual cues on the site indicate that it contains restricted information.

Device Encryption: The officer uses a university-issued laptop that is encrypted and password-protected. No data is downloaded to personal devices.

Email Security: When sharing information with another department, the officer uses the "ENCRYPT" feature in email to ensure secure transmission.
Alternatively, they send a secure, access-controlled link.

Physical Security: Any paper copies of loan applications are kept in a locked cabinet and shredded once they are no longer needed.

Compliance: The officer ensures that all actions comply with FERPA regulations, treating all student financial aid data as restricted.

Outlook

Sending an Encrypted Email with your University Account

Step 1: Open a New Email
Launch Outlook.
Click New Email to start composing a message.

Step 2: Go to the Options Tab
In the new message window, click the Options tab in the ribbon at the top.

Step 3: Choose Encryption
Click the Encrypt button (it may appear as a lock icon).

Step 4: Compose and Send
Write your email as usual.
Click Send when you're ready.

Encrypt-Only: Encrypts the message without restricting forwarding.
Do Not Forward: Cannot forward, print or copy.
Confidential: Should remain internal. Can be modified but cannot be copied or printed.
Confidential View Only: read-only access.

Full MUIT UPGA-10 Information Security Policy

Scan above
OR
Click Here

MARSHALL
INFORMATION TECHNOLOGY