GW Office of Ethics, Compliance, and Risk

Report a Concern

Ethics | Compliance | Reporting | Policies | Conflicts of Interest & Commitment | Protection of Minors | About Us

Home ▸ Policies ▸ Find a Policy ▸ Alphabetical Policy Listing ▸ Cybersecurity Risk Policy

Cybersecurity Risk Policy

Policy Summary

Managing cybersecurity risk is critical to maintaining the confidentiality, integrity, and availability of the university's Information Technology Resources ("GW IT Resources"). This policy outlines the George Washington University's ("GW" or "university") responsibilities in assessing and managing cybersecurity risk and Authorized Users' (hereinafter defined) duty to protect GW IT Resources.

Who is Governed by this Policy

- This policy applies to all university students, faculty, staff, and all other individuals and entities including, but not limited to, contractors, temporary employees, sponsored researchers, affiliates, visitors, and volunteers (collectively, "Authorized Users").

Policy

GW Information Technology ("GW IT") will assess the university's cybersecurity risk and manage any identified risk for the purpose of eliminating or minimizing the likelihood and impact of threats and vulnerabilities to the greatest extent practical. GW IT manages and mitigates cybersecurity risk by, among other things, establishing policies and guidance on the use of GW IT Resources, instituting cybersecurity risk standards and procedural controls, and providing security awareness training for Authorized Users.

Any data stored or processed using GW IT Resources falls within the scope of this policy which is governed by the IT Cybersecurity Risk Management Standard. The standard outlines requirements and processes for assessing and managing the cybersecurity risk associated with those GW IT Resources that collect, transmit, store, or process data used to accomplish university operations such as research, teaching, learning, and administrative support.

GW IT is responsible for detecting suspected or known security threats or emerging indications of compromised systems. GW IT accomplishes this by evaluating the content of university systems, network behavior, and third-party technology products and services acquired by the university. GW IT is also responsible for making decisions for network and cybersecurity defensive measures that protect the confidentiality, integrity, and availability of GW IT Resources.

In addition to the responsibilities of GW IT, Authorized Users play an important role in mitigating cybersecurity risk while using GW IT Resources both on campus and when accessing GW IT Resources remotely. Authorized Users are required to:

- Comply with GW's Acceptable Use of IT Resources Policy.
- Comply with GW's Identity and Access Management Policy and Standards.
- Complete assigned security awareness training.
- Understand and observe their responsibilities related to their stewardship of data and services, including compliance with the university's Data Classification and Protection Guide.

- Safeguard the confidentiality, integrity, and availability of the university’s information residing on or connected to GW IT Resources.
- Only use university-managed or approved devices to conduct GW activities, to the greatest extent possible. In circumstances when a non-GW-managed device is used to conduct GW activities, follow the university’s Data Classification and Protection Guide.
- Have all software or hardware to be used on the university network reviewed or assessed by GW IT consistent with the Procure to Pay Purchasing Review Process prior to the acquisition or installation.

In addition, Authorized Users conducting research activities may unintentionally be at greater risk of exposure to malware or other vulnerabilities that may degrade GW IT Resources and put GW research information at risk for fraud, theft, or misappropriation. Accordingly, research activities that involve use of GW IT Resources must be conducted in compliance with university policies, Office of Vice Provost of Research requirements, and applicable laws and regulations. This may include, but is not limited to, agreements and plans that outline data use and protection and obtaining the appropriate security reviews and approvals prior to project initiation.

Enforcement and Penalties

Non-compliance with this policy may result in restriction and possible loss of access to GW IT Resources. Non-compliance may also result in disciplinary action up to and including termination (employees) or suspension/expulsion (students).

Definitions

Authorized Users: All university students, faculty, and staff. It also applies to all other individuals and entities granted use of GW IT Resources, including, but not limited to, contractors, temporary employees, sponsored researchers, affiliates, visitors, and volunteers.

GW IT Resources: Any technology resource or equipment that supports one or more functional objectives of the university. This includes any system, service, or physical facility owned, contracted, or managed by the university to acquire, store, process, transmit, scan, receive, or dispose of data or information (e.g., software, computers, mobile phones, tablets, storage devices necessary for security and surveillance).

Related Information

- Acceptable Use of IT Resources Policy
- GW IT Cybersecurity Risk Management Standards
- Procurement Policy
- Data Classification and Protection Guide
- Privacy of Personal Information Policy
- Privacy of Student Records
- Records Management Policy

Contacts

Contact	Phone Number	Email Address
GW Information Security	202-994-4948	infosec@gwu.edu

Responsible University Official: Vice Provost for Libraries and Information Technology
Responsible Office: GW Information Technology

Origination Date: October 18, 2023
Last Material Change: N/A
Next Scheduled Review: August 2025

To provide feedback on this policy, please contact the Responsible Office(s) listed above or the Office of Ethics, Compliance, and Risk. More information describing university policies is outlined in the University Policy Principles.

Noncompliance with this policy can be reported through this website.

Office of Ethics, Compliance, and Risk

Email the Office

Report a Concern

Call the Office

Our office is part of the

GREEN
OFFICE
NETWORK

Campus Advisories

EO/Nondiscrimination Policy

Website Privacy Notice

Contact GW

Accessibility

Terms of Use

Copyright

Report a Barrier to Accessibility