GCSOM Electronic Resources Security Policy

Policy Number: 600.1010.100 Policy Revision Date: 2020-05-28

Policy Category: Information Technology

Policy Owner: Information Technology

Policy Audience:

Students, Faculty and Staff

1. Definitions:

FERPA: Family Educational Rights and Privacy Act

GLB: Gramm-Leach Bliley Act

HIPPA: Health Insurance Portability and Accountability Act

HITECH: Health Information Technology for Economic and Clinical Health Act

2. Leadership Council Review :

May 28, 2020

3. Introduction / Purpose :

The purpose of this policy is to ensure the security of electronic resources by those granted access to Geisinger Commonwealth School of Medicine (GCSOM) resources. This policy applies to any corporate electronic resources that GCSOM has or may install in the future. Those granted access to GCSOM resources have the responsibility to use electronic resources in a safe, secure, and lawful manner. This Electronic Resources Security Policy complements other GCSOM policies for use of resources. Please read and follow those policies as well.

4. Governance and Enforcement :

CIO

5. Policy :

Geisinger Commonwealth School of Medicine (GCSOM) User Responsibilities

GCSOM supports the installation and usage only of approved electronic resources. GCSOM credentials for use of electronic resources will be assigned by the GCSOM Information Technology Services (ITS). GCSOM credentials should never be shared with anyone, and compromise (or suspected compromise) of GCSOM credentials should be immediately reported to ITS and appropriate management.

Physical Security

- Sensitive workstations, servers, and other hardware must be kept physically secure. This includes the use of locked telecommunications closets, data centers, cabinets, and offices.

- Workstations that have access to sensitive resources should be kept away from casual traffic and onlookers.

Individual/Device Level Security

- GCSOM credentials for use of electronic resources will be assigned by the GCSOM ITS
department. These credentials should never be shared with anyone.

- Any change in the role of a user at GCSOM (eg: promotion, transfer) should be immediately reported to ITS (as well as to HR or others if appropriate) so that the requisite changes in access and security can be processed in a timely manner.

- All users should utilize "strong" personal passwords regardless of whether the system(s) that they access require them to do so. This means that the passwords are at least 8 characters in length and use a combination of letters and numbers in accordance with the global policy implemented for protection from unauthorized access to GCSOM accounts and resources.

- Any compromise or suspected compromise of personal security credentials must be immediately reported to ITS and appropriate management. Credentials may be suspended, reset, or regenerated depending on the circumstances and risk.

- Users are required to maintain current threat protection software on their devices. Failure to do so may result in suspension of access to electronic resources.

- All devices that have the capability to set a "timeout" or inactivity password should utilize them. Timeout/inactivity periods should be set relatively short so that devices quickly become locked if unattended, misplaced, or stolen.

- Wherever possible, GCSOM will enforce strong passwords, periodic password cycling and inactivity timeouts for systems that it utilizes.

Systems Level Security

- Administrative levels of access to GCSOM systems, which include capabilities such as system configuration, security settings, audit trails, etc, will be managed by ITS.

- Access to applications will be evaluated, granted/denied, and managed based on role along with the approval/denial of appropriate application custodians. This process will utilize a formal request process which retains a record of all such activity.

- It is a direct violation of this policy to establish a system/server/application for shared use which has not been expressly approved and deemed secure by ITS.

Network Level Security

- ITS will maintain GCSOM network security. Access to the GCSOM network will require authentication for all users.

- Network level access will include a security review of any device attempting to connect. Access to the network may be limited or denied based on this review.

- Non-GCSOM devices will not be permitted on the secure GCSOM network.

- It is a direct violation of this policy to extend or modify the GCSOM network, or establish a separate network involving GCSOM resources, which has not been expressly approved and deemed secure by ITS.

Perimeter Level Security

- ITS will maintain perimeter defenses such as virus/worm protection, firewalls and intrusion detection/prevention systems. Such defenses may impact the flow of electronic traffic into and out of the organization.

- ITS will periodically test the security of its electronic environment in order to ensure the effectiveness of its defenses.

Privacy Guidelines

GCSOM maintains the right to intercept, monitor, store, review, and disclose electronic resources activity to ensure compliance with this policy, as well as to fulfill GCSOM's responsibilities under the laws and regulations of the jurisdictions in which it operates - for example, to supply information in legal discovery or to regulators. Users should have no expectation of privacy.

- On termination or separation from the GCSOM, the organization will deny access to electronic resources, including the ability to download, forward, print or retrieve any information stored in GCSOM systems.

- Any content created with GCSOM electronic resources is considered the intellectual property of GCSOM.

Credentials and Operations

- GCSOM credentials for use of electronic resources will be assigned by the GCSOM ITS department. These credentials should never be shared with anyone, and compromise (or suspected compromise) of GCSOM credentials should be immediately reported to ITS and appropriate management.

- Any change in the role of a user at GCSOM (eg: promotion, transfer) should be immediately reported to ITS (as well as to HR or others if appropriate) so that the requisite changes in access and security can be processed in a timely manner.

- Users are required to maintain current threat protection software on their devices. Failure to do so may result in suspension of access to electronic resources for the device, the user, or both.

- Any actual or suspected electronic security breach must be immediately brought to the attention of ITS and the relevant management staff.

- Connecting to GCSOM electronic resources from non-GCSOM devices (eg: home, conferences, hotels, etc) should be treated with the same care as would be in place for a GCSOM device if possible (ie: virus protection, firewall, etc).

- Be skeptical of email messages that are from unknown sources or which invite you to open attachments or submit information.

Protecting Customer Information

- GCSOM adheres to applicable laws and regulations regarding the protection of customer information, including but not limited to HIPAA, FERPA, HITECH, the GLB security rule, and the GLB safeguards rule.

- Non-public customer information is maintained within GCSOM systems and is used for internal operations and uses. As such, it is only accessible by those who have a need related to their GCSOM function.

- In the event of a breach, GCSOM will invoke the institution’s Critical Incident Response Plan, and follow the relevant procedures in that plan. It includes notification of the appropriate internal and external parties.

Governance and Enforcement

- This policy is approved by the President's Cabinet and is overseen by the Chief Information Officer or designee, who will review this policy annually to ensure that GCSOM is in compliance with internal and external requirements.

- Outside entities that have shaped the terms of this policy include agencies, accrediting bodies, and state and federal regulations such as HIPAA, FERPA, GLB and HITECH.

- Violations of the Electronic Resources Security policy can result in informal or formal warnings, the loss of electronic resources privileges, and corrective actions up to and including termination.

- In some cases, the nature of the violation may trigger the Critical Incident Response Plan and may require notification of authorities and agencies beyond GCSOM (eg: felonies, harassment, GLB Safeguard Rule, etc).

6. Key Stakeholders :

Students, Faculty and Staff