SECTION: Personnel Policies and Procedures / General Personnel Policies and Procedures **NUMBER: M/1.11**
SUBJECT: Information Security
SOURCE REFERENCE:

Information Security

1. Purpose

The purpose of this policy is to define sensitive information, minimize the risk of loss or exposure of sensitive information maintained by Gadsden State Community College (GSCC) as well as to comply with state and federal requirements for protecting data and reporting data breaches.

2. Scope

This policy applies to all GSCC employees, students, vendors, contractors and others that may use a computer, servers, or any other data system that contains or may potentially have access to GSCC confidential or and personally identifiable information (PII).

3. Policy

3.1 Public and Sensitive Data

GSCC recognizes its obligation to protect the privacy of personally identifiable information (PII) related to its students, faculty, staff, and others. To guide the categorization of information and the development of guidelines for handling and disclosing each type of information, GSCC has defined two types of information: "public" and "sensitive".

Public information refers to any information that GSCC has not classified as sensitive information under this policy. Public information is generally available to anyone who requests it and must be verified for accuracy before release. Summary data that has been aggregated to remove PII is considered public data by default. Only authorized GSCC employees may release public information in accordance with policy M-1.13 outlined in the Employee Handbook.

Sensitive information refers to any information under GSCC control that contains PII. Access to this information is authorized by the corresponding data stewards. Data stewards are required to periodically review access granted to data that falls under their purview. In addition, data stewards are also responsible for disposing of customer data after the regulatory requirements for storage has ended.

Sensitive information may only be stored on data systems owned by the college or on service provider's data systems that have been approved by the Chief Information Officer (CIO). The approved service providers are required to provide documentation that indicates they have implemented acceptable safeguards. The adequacy of these safeguards will be assessed annually as part of the annual report described in section 3.2 of this document.

Sensitive data may only be released to the subject of the information and to authorized GSCC employees who have a legitimate need-to-know in accordance with their current duties. In some cases, outside entities may be granted access to sensitive information if the subject of the

information provides written permission or if otherwise permitted by law. The use of this information is often protected by state or federal laws, including but not limited to:

- Graham-Leach-Bliley Act of 1999 (GLBA) - governs privacy and use of financial information
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) - governs privacy and use of health care information
- Family Educational and Privacy Rights Act of 1974 (FERPA) - governs privacy and use of student information

It is important to note that sensitive data, as defined in this policy and associated policies, includes not only data in use and at rest in GSCC data systems but also paper, voice, or any other form in which GSCC-controlled data may be stored or transmitted.

3.2 Information Security Program

In order to ensure protection of sensitive data and to meet certain GLBA requirements, GSCC establishes with this policy an Information Security Program. This program is to be maintained by the Systems Administrator – Cybersecurity with oversight and direction provided by the CIO. The program is guided by an Information Security Plan that will be evaluated and updated annually by the CIO and the Systems Administrator – Cybersecurity. Additionally, the program establishes a yearly risk assessment that includes system/network penetration testing, regular vulnerability scanning, and patch management.

The Systems Administrator – Cybersecurity will submit an annual report to the CIO that outlines the overall status of the Information Security Program and its compliance with this policy and the Information Security Plan. This report will address issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, as well as recommendations for changes to the information security program.

3.3 Data Breach Response

A data breach is a security incident in which PII and/or sensitive data is compromised. This includes but is not limited to data that is endangered, corrupted, copied, transmitted, viewed, stolen or used by anyone unauthorized to do so. Any known or suspected data breach must be reported to the Information Technology Services (ITS) Information Security Team (defined in the Information Security Plan) to initiate an appropriate investigation. Suspected data breaches should be reported by emailing infosec@gadsdenstate.edu or by calling the ITS Help Desk at 256-549-8341.

Upon being notified of a suspected data breach the Systems Administrator – Cybersecurity will evaluate the report to determine if an actual breach has occurred. If a breach has a occurred the

Systems Administrator – Cybersecurity will begin an investigation and notify the CIO. Members of the Information Security Team will work with data owners to ensure that all access to the compromised resource is removed immediately. If a breach occurs outside of the GSCC network, the appropriate ITS department members will handle the coordination of removing access to compromised data with third party vendors, individuals, etc.

Severity of the breach will be determined by the CIO. If a breach is deemed severe, then the CIO is authorized to create a critical response team. Members of this team will be comprised of selected employees in ITS, the affected unit, additional departments based on data type, or any individual deemed necessary by the CIO or Systems Administrator – Cybersecurity. The Critical Response Team will be delegated duties by the CIO and the Information Security Team to provide additional aid to the incident response process. If the breach involves a suspected crime, the information assurance team will notify Gadsden State Safety and Security. A determination will be made as to whether law enforcement notification is required. If so, the notification will be made.

The Information Security Team will operate according to Incident Response section of the Information Security Plan to mitigate threats and restore normal access to data.

3.4 Information Security Training

All new employees are required to complete information security training at the time of hire. Current employees will have access to training materials as defined in the Information Security Plan established by section 3.2 of this policy.

To assure that information security personnel take steps maintain current knowledge and training related to changing information security threats, the CIO and the Systems Administrator – Cybersecurity will be required to attend at least two information security related professional development sessions a year.

3.5 ITS Change Management

Major changes to ITS systems and services must be planned, documented, and authorized before implementation. The ITS department work order system will be used to request and document major changes to these systems. Changes will be reviewed and approved by the appropriate stakeholders and the appropriate ITS employees before implementation. Emergency changes must be documented and authorized as soon as possible after implementation. Changes that affect the security, integrity, or availability of ITS systems and services must be reviewed and approved by the Information Security Assurance Team before implementation (This team is defined in section 6.0 of the GSCC Information Security Plan). Any unauthorized changes to ITS systems and services must be reported to the Information Security Assurance Team immediately.

3.6 Laptop and Portable Device Encryption

Sensitive information belonging to Gadsden State Community College should not be stored on portable devices and/or removable media unless absolutely required in the performance of your assigned duties or when providing information required by state or federal agencies. Portable devices include but are not limited to laptop computers, tablets, smartphones, jump-drives, etc.

When sensitive information is stored on a portable device or removable media, it must be encrypted in accordance with a currently approved encryption standard. Approved encryption standards include BitLocker for Windows systems, FileVault for macOS, Full Disk Encryption (FDE) for Linux, and any other encryption that meets or exceeds the AES-128 encryption standard adopted by the U.S. government.

Sensitive information belonging to Gadsden State Community College must never be stored on personal portable devices and/or removable media. Additionally, portable devices and/or removable media containing sensitive information belonging to Gadsden State Community College may not be connected to, or used with, personal computers and other personally owned devices.

3.7 Smartphone and Tablet Email Security

Gadsden State Community College email accounts may be used on smartphone and/or tablet devices to facilitate official duties associated with GSCC under certain conditions. For example, if email is to be stored in an account on the device, GSCC requires the use of an appropriate PIN, password, or other security locking method. In this case, the College reserves the right to remotely wipe the contents of any device reported lost, stolen, or maliciously using a GSCC email account.

Users who do not wish to store email on their device, or who do not want to enable security may still use a web-browser on a smartphone or tablet to access email without an associated PIN requirement. Alternatively, a user may use the Microsoft Outlook Web Access (OWA) app, in which case the college reserves the right to remotely wipe the contents of the OWA app but not the entire phone in the case of a lost, stolen or a maliciously used GSCC email account.

3.8 Workstation Security

In order to protect the confidentiality, integrity, and availability of this data GSCC has implemented physical and technical safeguards for all workstations containing or having access to PII and also restricts access to authorized users.

Departments should make a reasonable effort to restrict physical access to domain-joined workstations provided for authorized users. When a workstation is to be left unattended for any length of time the employee responsible for that workstation should lock the screen to prevent unauthorized access. Locking the workstation will not close documents or logout of work sessions but will require entering the workstation password to resume the session. The IT department is

authorized to enforce a 15-minute screen inactivity timeout on the MIS domain workstations via electronic policy updates.

Workstations should only be accessed by authorized users themselves. No user is permitted to use any workstation for regular work that has been logged into by any user other than themselves.

It is not permitted to install any unauthorized software on workstations.

Laptops or any other non-stationary device that contains PII or other sensitive data should be secured when not in use. Methods of securing these devices could include cable locks, locked desk drawers, locked cabinets, or any other reasonable method that prevents an individual from being able to easily steal the device containing sensitive data.

Workstations in public facing areas should have privacy screen filters or other physical barriers installed to prevent exposing sensitive data.

It is recommended that all workstations which interact with critical or sensitive data use an uninterruptible power supply (UPS) to protect the integrity of data in the event of a loss or degradation of electric power.

Information Technology Services (ITS) staff must ensure that all Windows workstations run some form of virus protection. Workstations should also run Endpoint Detection and Response (EDR) software to identify threats in real time. Workstations can be exempted from the EDR requirement based on the interference of EDR with specific programs essential to the function of the college. These exemptions are rare and must be approved by the Systems Administrator – Cybersecurity or the CIO. Workstations are never permitted to run without virus protection.

When a workstation is no longer in service the ITS department will remove and crush all hard disk drives before sending the system to surplus.

3.9 Server Security

Information Technology Services (ITS) staff must ensure that all Windows servers run some form of virus protection. Windows servers should also run Endpoint Detection and Response (EDR) software to identify threats in real time. The Systems Administrator – Cybersecurity may temporarily disable EDR on servers from time to time at their discretion to facilitate certain tasks provided it is re-enabled when appropriate. Servers are never permitted to run without virus protection.

All Linux and Windows servers must be kept up-to-date. Windows servers should have appropriate updates installed within 60 days of release, allowing ITS administrators enough time to test updates for compatibility with GSCC systems. Linux systems should have updates installed within 120 days. If a critical update is known to protect the function of the college, it must be installed immediately upon recommendation by an ITS administrator or the CIO to avoid putting the college

at risk.

Windows servers with RDP access enabled must utilize multifactor authentication. If multifactor authentication cannot be enabled for any of these servers, then RDP access must be disabled.

3.10 Disabling Accounts

An employee's Active Directory account will be disabled the next business day after that person's employment is formally terminated. An Active Directory account may also be disabled immediately if a request is made by the Human Resources department. Additionally, any ITS administrator or help desk employee may temporarily disable an Active Directory account if that person believes the account could compromise the confidentiality, integrity, or availability of GSCC data or data systems. If an ITS employee disables an Active Directory account for this reason, then they are required to report this action to the CIO as soon as possible.

Access to an employee's email account will automatically be terminated when the user's Active Directory account is disabled. Upon Dean approval, the terminated employee's email can be forwarded to another employee.

3.11 Data Retention

Gadsden State Community College will retain employee email for five years from the time an employee discontinues employment with the college. After five years the employee's email will be permanently deleted.

Data stored on college owned desktops, laptops, tablets, and phones left by former employees may be retained directly on this equipment if this equipment will be used by another employee filling that vacant position.

Desktops and laptops that are no longer used by the college will have their hard drives removed and destroyed. Tablets and phones no longer used by the college will be securely wiped according to manufacturer specifications.

All other data owned, produced, or stored by the college such as financial records, personnel records, student records, etc. should be retained for the amount of time required by law for each specific data type. The data owners for each type of data are responsible for ensuring that data under their control is deleted according to the associated laws and regulations.

3.12 Data Encryption

Gadsden State Community College will ensure that sensitive data at rest and in transit is encrypted. Sensitive college data at rest must be stored on encrypted drives. Sensitive data transmitted in any form must use a protocol that utilizes encryption to keep data secure.

4. Policy Compliance

4.1 Enforcement

The Chief Information Officer is authorized to mitigate any non-compliance with this policy at any time either directly or through delegation to staff.

4.2 Exceptions

Any exception to the policy must be approved by the Chief Information Officer.