Grayson College
Written Information Security Program

History

Version No.	Issue Date	Status	Reason for Change
v1.0	10/15/2020	Draft	

Review

Reviewer’s Details	Version No.	Date

1. PURPOSE AND INTENT

Grayson College recognizes the importance in maintaining the security and confidentiality of Personal Information and other sensitive data, in physical and electronic form. Personally Identifiable Information (“PII”), Sensitive Personal Information (SPI), Protected Health Information (PHI) and other Data is essential to Grayson College’s operations and its relationships with students, employees, and business partners. Grayson College is committed to protecting PII, and other Data in its possession by implementing administrative, technical, technological, and physical safeguards that meet or exceed the standards set by applicable laws and regulations for protecting PII, and other Data. The Texas Administrative Code Chapter 202 (TAC§202) defines an outstanding security program that follows closely with the federal requirements defined in NIST 800¬53. This Written Information Security Program (WISP) will ensure that Grayson College is compliant with current state and federal regulations and will prepare Grayson College for future compliance requirements.

The purpose of this comprehensive Written Information Security Program (“WISP” or “Program”) is to: (1) ensure the security and confidentiality of PII, and other Data; (2) protect against reasonably anticipated threats or hazards to security and integrity of PII, and other Data; and (3) protect against unauthorized access to such Information that may result in substantial harm or inconvenience to Grayson College students, employees, independent contractors, and others. Grayson College shall submit to the Texas Office of the Secretary of State biennially this WISP in accordance with §2054.133, Texas Government Code.

2. SCOPE

Grayson College has assessed the internal and external risks to the security, confidentiality, and accessibility of its electronic and paper records containing ePHI/PHI, PII, SPI, and other Data; and evaluated physical and electronic methods of accessing, collecting, storing, using, sharing, transmitting, destroying, and protecting ePHI/PHI, PII, SPI, and other Data. Grayson College has also reviewed the applicable laws and regulations. Based on this evaluation, Grayson College has developed this Program to protect ePHI/PHI, PII, SPI, and other Data, that is processed or possessed by Grayson College from reasonably anticipated threats and hazards that could result in unauthorized access to or use of such Information.

Grayson College will perform on-going reviews and improvements of the Program to address the effectiveness of the WISP, as outlined in TAC§202, considering evolving risks, technologies, business obligations, industry standards, regulations, and legal requirements. Grayson College will review the Program annually and, when changes to business practices, present possible risks to the security of ePHI/PHI, PII, SPI, and other Data

Grayson College's information security practices must comply with a variety of federal and state laws, as well as Grayson College policies. These regulations are generally designed to protect individuals and organizations against the unauthorized or accidental disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver's license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant to the users of Grayson College's information technology resources are listed in the Grayson College Information Security Policy.

To avoid breaches of any law, regulation, contractual obligation, or institutional policy, information technology resources will be regularly tested and audited to assure adherence with both external and internal standards.

Students, faculty and staff are responsible for understanding and observing these and all other applicable policies, regulations and laws in connection with their use of Grayson College's information technology resources.

3. DEFINITIONS

A. **“Access”-**The physical or logical capability to view, interact with, or otherwise make use of information resources.

B. **“Availability”** is the security objective of ensuring timely and reliable access to and use of information.

C.**“Confidential Information”** is information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement.

D.**“Confidentiality”** is the security objective of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

E.**“Control”** is a safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Controls may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

F.**“Data” or “Information”** is defined as information required for college operations, education records, or security-related information, as processed, stored, or transmitted by electronic means.

G.**“Destruction”** is the result of actions taken to ensure that media cannot be reused as originally intended and that information is technologically infeasible to recover or prohibitively expensive.

H.**“Electronic Communication”** is a process used to convey a message or exchange information via electronic media. It includes the use of electronic mail (email), Internet access, Instant Messaging (IM), Short Message Service (SMS), facsimile transmission, and other paperless means of communication.

I.**“Electronic Protected Health Information”** or **“e-PHI”** has the meaning assigned by 45 CFR §160.103. As of the Effective Date, e-PHI means PHI that is transmitted by or maintained in Electronic Media;

J.**“Encryption “**(encrypt or encipher) is the conversion of plaintext information into a code or cipher text using a variable called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

K.**“FERPA”** collectively refers to all regulations having legal force issued by a regulatory agency which implement, explain or interpret the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) that protects the privacy of student education records.

L.**“FISMA”** refers to the Federal Information Security Management Act (FISMA, 44 U.S.C. § 3541)

M.**“Guidelines”** are recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.

N. **“HIPAA Rules”** collectively refers to all regulations having legal force issued by a regulatory agency which implement, explain or interpret the HIPAA or the HITECH Act, including, but not limited to, the Privacy Rule, Security Rule, and Omnibus Rule;

O.**“High Impact Information Resources”** are the Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

1. Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
2. Result in major damage to organizational assets;
3. Result in major financial loss; or
4. Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

P. **“HITECH”** or **“HITECH Act”** means the Health Information Technology for Economic and Clinical Health Act, Division A, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), 42 USC § 300 *et seq*.;

Q. **“Information Resources”** as defined in §2054.003(7), Texas Government Code

R.**“Information Security Officer”** has the meaning assigned by 45 CFR § 164.308. The Information Security Officer is responsible for the continuous management of information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all organizational information systems;

S.**“Information System”** is an interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes, but is not limited to, hardware, software, network Infrastructure, information, applications, communications and people.

T.**“Integrity”** is the security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity

U.**“ITCHE”** stands for Information Technology Council for Higher Education.

V.**“NIST 800¬53”** is the current published version of the NIST Security and Privacy Controls for Federal Information Systems and Organizations.

W. **“Omnibus Rule”** means the final rule published in 78 Fed. Reg. 5566 (2013) that implements several provisions of the HITECH Act designed to strengthen the privacy and security protections established by HIPAA;

X. **“Personally Identifiable Information”** (or “PII”) is defined as:

i. An individual’s name (first name or initial, and last name) in combination with one or more of the following concerning the named individual:

1. Social Security number;
2. Driver’s license number;
3. State-issued identification card number, including passport number;
4. Financial account number;
5. Credit card number;
6. Debit card number;
7. Health insurance identification number; or
8. Medical Information (medical history or medical diagnosis/treatment by a health care professional); or

ii. An email address or username in combination with a password or security question that would permit access to an online account;

iii. Personal Information includes Information in electronic records and hard copy documents.

Y. **“Privacy Rule”** means the standards for the Privacy of Individually Identifiable Information set forth in 45 CFR Parts 160 and 164;

Z. **“Procedure”** are instructions to assist information security staff, custodians, and users in implementing policies, standards and guidelines.

AA. **“Protected Health Information”** or **“PHI”** has the meaning assigned by 45 CFR § 160.103. As of the Effective Date, PHI means Individually Identifiable Health Information (with limited exceptions for information maintained in certain education records or employment records and information regarding a person who has been deceased for more than 50 years) that is transmitted by, or maintained in, Electronic Media or transmitted or maintained in any other form or medium;

BB. **“Residual Risk”** is the risk that remains after security controls have been applied

CC. **“Risk Management”** is the process of aligning information resources risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures.

DD. **“Security Incident”** is an event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources

EE. **“Security Standard”** means the data security guidance set by FISMA and the National Institute of Standards and Technology (NIST).

FF. **“Sensitive Personal Information”** is a category of personal identity information as defined by §521.002(a)(2), Texas Business and Commerce Code

GG. **“Vulnerability Assessment”** is a documented evaluation containing information described in §2054.077(b), Texas Government Code which includes the susceptibility of a particular system to a specific attack.

HH. **“Written Information Security Program”** or **“(WISP)”** means the policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function within Grayson College.

4. RESPONSIBILITY FOR PROTECTING PERSONALLY IDENTIFIABLE INFORMATION, AND OTHER DATA

All Grayson College employees, including part-time, temporary, and contract employees (hereinafter “employees”) independent contractors, and vendors are responsible for maintaining the privacy and security of ePHI/PHI, PII, SPI, and other Data.

Service providers are responsible for the security of ePHI/PHI, PII, SPI, and other Data that the service providers possess or otherwise store, process, or transmit on behalf of Grayson College users, or to the extent that they could impact the security of the user’s data.

5. INFORMATION SECURITY OFFICER

Grayson College will designate and document an Information Security Officer (ISO), and as such they will have the authority and responsibility for the following:

A. Maintaining and updating the WISP at least annually, as required by §2054.133, Texas Government Code;

B. Training employees, both temporary and contract, through initial as well as on-going training, on the WISP, the importance of maintaining the security measures set forth in this WISP, and the consequences of failures to comply with the WISP.

C. Ensuring employees are complying with the measures of the WISP.

D. Reviewing Grayson College’s inventory of information systems and related ownership and responsibilities;

E. Maintaining an inventory of authorized devices and software.

F. Establishing and maintaining the standards for security configurations of hardware and software on mobile devices, laptops, workstations and servers.

G. Reviewing the scope of the security measures in the WISP at least annually or whenever there is a change in business practices that may implicate the security or integrity of records containing personal information.

H. Monitoring the effectiveness of the security program, testing the safeguards contained in the WISP, and making changes when necessary to the WISP.

I. Ensuring that annual information security risk assessments, based on requirements in TAC§202.75 are performed and documented;

J. Overseeing third-party provider contracts and agreements ensuring that there is compliance language in any such agreements, and evaluating any third-party provider’s ability to comply with the agreements.

K. Reporting, at least annually, to the state institution of higher education head the status and effectiveness of security controls; and

L. Informing the parties in the event of noncompliance with this chapter and/or with the institution's information security policies.

M. Grayson College, with the approval of the Texas state institution of higher education head, may issue exceptions to information security requirements or controls. Any such exceptions shall be justified, documented and communicated as part of the risk assessment process

6. LEGITIMATE PURPOSES ONLY

In order to minimize the possibility that PII and other data is lost, stolen, misused or inadvertently disclosed, such information will be collected, maintained, accessed, used, and transferred by Grayson College Related Persons only for legitimate Grayson College business, and only when there is a legitimate work or program-related need to access or use ePHI/PHI, PII, SPI, and other Data.

7. CONTROLLING ACCESS TO PERSONAL INFORMATION

Grayson College uses a range of security measures and practices to control access to and protect PII, and other Data, including the controlled use of administrative privledges. The following requirements apply to all Grayson College Related Persons (employees, students, independent contractors, business associates, and third-party service providers):

A. Access to electronic and hard copy documents containing ePHI/PHI, PII, SPI, and other Data, shall be limited to those persons required to know such information in order to accomplish their job duties or to enable Grayson College to comply with business, institutional, regulatory and legal obligations.

B. Individuals shall limit the amount of ePHI/PHI, PII, SPI, and other Data that they collect in the course of performing their job duties to that reasonably necessary to accomplish their work for Grayson College or to enable Grayson College to comply with business, institutional, regulatory and legal obligations.

C. Employees shall not maintain their own personal ePHI/PHI, PII, and SPI on Grayson College laptops, other Grayson College devices, network locations, or cloud repositories.

D. All hard copy records containing PII, SPI, or PHI shall be kept in locked cabinets/containers or a locked room when the responsible individuals are not physically present at the location of the records. Documents containing PHI and PII shall be secured before permitting individuals not authorized to view the materials into the work area.

E. Access to electronic records containing ePHI/PHI, PII, SPI, and other Data shall be limited to individuals with active user accounts only. Each such individual shall have a unique user-ID and password. Wherever available multi-factor authentication (MFA) technology must be employed.

F. Passwords allowing access to systems with electronic records containing ePHI/PHI, PII, SPI, and other Data shall be changed at regular intervals, minimally every ninety days. Passwords shall comply with the complexity and follow requirements contained in Section 7 below.

G. Grayson College will use the highest currently available commercial encryption technologies for the transfer and maintenance of PHI and other Sensitive Personal Information.

H. Grayson College will install personal firewall software on all computers and laptops that store or access PHI/ePHI or connect to networks on which PHI/ePHI is accessible.

I. Individuals with access to electronic records containing ePHI/PHI, PII, SPI, and other Data, shall lock computers before leaving their desks for extended periods (i.e. by pressing CTRL + ALT + Delete).

J. Individuals shall not disclose their Grayson College user-IDs or passwords to anyone other than the ISO or designated IT Service Provider. User-IDs and passwords must not be placed in areas where they may be viewed or accessed.

K. Individuals printing or faxing documents containing PHI, PII, SPI or other Data shall immediately retrieve such documents from printers and fax machines.

L. Physical access to Grayson College locations by visitors shall be restricted. Visitors shall be required to sign a log. When an individual's assigned responsibilities within Grayson College change, physical and electronic access privileges will be promptly terminated or changed, consistent with the need-to-know limitation for access to ePHI/PHI, PII, SPI, and other Data.

With respect to the use of remote access technologies, Grayson College will take the following measures:

A. Utilize a licensed Virtual Private Network (VPN) with the strongest possible encryption methods for remote access to its systems that contain ePHI/PHI, PII, SPI, and other Data. Restrict remote access to its systems that contain ePHI/PHI, PII, SPI, and other Data to authorized geographic regions.

B. Limit VPN access to those with a valid Grayson College reason, and only when necessary.

C. Implement multi-factor authentication for granting remote access to its systems that contain ePHI/PHI, PII, SPI, and other Data.

D. Install current licensed virus-protection software on all portable devices used to store or transmit ePHI/PHI, PII, SPI, and other Data.

E. Enforce the use of strong passwords for granting remote access to its systems that contain ePHI/PHI, PII, SPI, and other Data.

F. Password protect all portable and remote devices storing ePHI/PHI, PII, SPI, and other Data.

G. Install firewall software on all portable and remote devices that store ePHI/PHI, PII, SPI, and other Data or connect to networks on which ePHI/PHI, PII, SPI, and other Data accessible; per Grayson College Firewall Policy.

H. All portable or remote devices that store ePHI/PHI, PII, SPI, and other Data will employ the highest currently available encryption technologies.

Upon conclusion of an individual's employment or association with Grayson College, all physical and electronic access to College facilities and IT systems will be immediately terminated. Such individuals shall be required to return all Grayson College records containing ePHI/PHI, PII, SPI, and other Data PII immediately.

8. PASSWORD REQUIREMENTS

All Grayson College users must select a unique passphrase or passwords following the guidelines set forth in the Grayson College User Password Policy, which include:

A. Is at least 10 characters long;

B. Contains a combination of uppercase and lowercase letters, numbers, and special characters (i.e. @, !, *);

C. Does not include repeated characters or a sequence of keyboard strokes (i.e. 1234, mmm888, or asdfg); and

D. Does not include any part of the user's name, birthday, or other personally identifiable information, or that of friends and family.

E. Shall be changed at least every 90 days, or as necessary.

9. PERSONAL HEALTH INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION MUST BE MAINTAINED ON GRAYSON COLLEGE PREMISES, SYSTEMS, AND SERVICES

All physical records containing ePHI/PHI, PII, SPI, and other Data must be kept on Grayson College premises unless approved in writing by the Information Security Officer. If authorized, records maintained offsite of Grayson College premises must always remain in the custody and control of the documented authorized individual.

All ePHI/PHI, PII, SPI, and other Data in electronic form shall be encrypted. Therefore, all laptops, desktops, or devices used to perform work for Grayson College that access or store ePHI/PHI, PII, SPI, and other Data must utilize the highest currently available commercial encryption technologies. For purposes of this WISP, "encryption" shall mean the transformation of Data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key. Merely password protecting a document or file does not qualify as encryption.

All records containing ePHI/PHI, PII, SPI, and other Data shall only be maintained on or accessed using Grayson College approved IT services, systems (IT Systems), and devices. Grayson College users may not store or access electronic records containing ePHI/PHI, PII, SPI, and other Data via unapproved personal devices, non-Grayson College accounts, or any non-Grayson College cloud services or repositories. Such records may not be sent to, or stored in, personal email accounts or personal cloud repositories.

10. DESTRUCTION OF RECORDS CONTAINING PERSONAL INFORMATION

Hardcopy and electronic records containing ePHI/PHI, PII, SPI, and other Data shall be destroyed within a reasonable time after they are no longer needed for business purposes, and Grayson College is no longer required to retain them under applicable law or contractual requirements. Under no circumstance shall any documents or Data subject to a litigation hold be destroyed. Hard copy documents containing ePHI/PHI, PII, SPI, and other Data be destroyed by burning, pulverizing, or shredding. Electronic records containing ePHI/PHI, PII, SPI, and other Data will be destroyed or erased so that the Data cannot practicably be read or reconstructed.

Any offsite paper Data shredding service used by Grayson College must provide Grayson College with documentation of the destruction that contains the date of destruction, the method of destruction, a description of the disposed of records, the inclusive dates covered by such records, a statement that the records have been destroyed in the normal course of business and the signatures of the individuals supervising and witnessing the destruction.

11. CONTRACTS WITH SERVICE PROVIDERS

Grayson College shall make reasonable efforts to evaluate, select, and retain third-party service providers that can maintain appropriate safeguards to protect ePHI/PHI, PII, SPI, and other Data compatible with the safeguards provided by Grayson College and required by the FISMA, HITECH Act, HITRUST, the HIPAA Omnibus Rule, and all applicable state laws. The Grayson College Third-Party Provider Information Sharing Security Program shall be the guide.

Grayson College requires that third-party service providers, including vendors, subcontractors, and independent contractors, enter into written contracts (Third-Party Agreements) by which they agree to maintain safeguards that comply with the FISMA, HITECH Act, HITRUST, the HIPAA Omnibus Rule, and Grayson College information security safeguards in the performance of their services for Grayson College . To the extent feasible, third-party service providers shall also be contractually required to report any Data breach promptly, or the loss, unauthorized access, or unauthorized use of any ePHI/PHI, PII, SPI, and other Data owned or controlled by Grayson College.

The Information Security Officer shall maintain a record of all vendors that provide services or products that permit access to ePHI/PHI, PII, SPI, and other Data belonging to or controlled by Grayson College.

12. COMPUTER SYSTEM SECURITY MEASURES

Grayson College shall maintain up-to-date operating systems and security patches for systems or services. Grayson College shall also provide up-to-date versions of licensed system security agent software, including anti-virus and malware protection, together with up-to-date patches and virus/malware definitions.

Grayson College will install firewall software on all portable and remote devices that store ePHI/PHI, PII, SPI, and other Data or connect to networks on which such is accessible. All portable or remote devices that store ePHI/PHI, PII, SPI, and other Data will employ the highest currently available encryption technologies, use passwords/passphrases, and wherever available multi-factor authentication (MFA) technology will be employed.

Licensed system-wide security agent software, which includes malware protection, patches, and virus definitions, is installed on all Grayson College systems. This software will be updated daily automatically (and manually when needed) on all systems.

All Grayson College computer systems will be monitored persistently for unauthorized use of or access. Any unauthorized use or access found will be immediately reported to the Information Security Officer. Further, actions will be taken to assess the impact of the unauthorized use/access, appropriate measures will be taken against employees not complying with this WISP, and updates will be made to the safeguards specified in this WISP as needed to prevent future unauthorized access/use of ePHI/PHI, PII, SPI, and other Data

13. INSTIUTIONAL SECURITY REPORTING

Information Security Officer shall report, at least annually, to the Grayson College President on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this WISP and:

F. Effectiveness of current information security program and status of key initiatives;

G. Residual risks identified and mitigated; and

H. Any requests about information security requirements.

14. PROTOCOL IN THE EVENT OF A BREACH OF SECURITY

The Grayson College Incident Response Plan shall determine any and all actions that shall be taken in the event of a security incident.

Any incident potentially involving the unauthorized access or use of ePHI/PHI, PII, SPI, and other Data belonging to or controlled by Grayson College or the loss of any documents, devices, or Data that may have contained ePHI/PHI, PII, SPI, and other Data, encrypted or unencrypted, shall immediately be reported to the Information Security Officer.

The Information Security Officer shall also be immediately informed of any suspicion: (1) that ePHI/PHI, PII, SPI, and other Data may have been compromised; (2) of any internal or external efforts to compromise Grayson College systems or to access without authorization ePHI/PHI, PII, SPI, and other Data maintained on the Grayson College system; (3) of unauthorized use of the Grayson College system; or (4) the failure of an authorized Grayson College user or independent contractor of Grayson College to comply with the requirements of this Program.

In the event of a breach of security involving the potential loss, unauthorized use, or unauthorized access of ePHI/PHI, PII, SPI, and other Data belonging to or under the control of Grayson College , the College shall: (1) secure and preserve computer systems, logs, and paper files; (2) take systems and devices offline; (3) create forensic images; or (4) take other steps to restrict access to potentially impacted systems, records, and Data. The Information Security Officer shall immediately investigate the incident and promptly take appropriate steps to respond, following the Grayson College Incident Response Plan (IRP), including the issuance of notices under applicable security breach notification laws.

After the investigation and response to any breach of security involving ePHI/PHI, PII, SPI, and other Data, the Information Security Officer shall conduct and document an immediate mandatory post-incident review of events and actions taken by Grayson College, if any, to determine whether any changes to security measures or this WISP are warranted. As part of this post-incident review: (1) the Information Security Officer shall identify administrative, physical, and technological protections that could have prevented, mitigated, or signaled a breach; (2) the Information Security Officer shall adopt such protections through amendments to this WISP and subsequent employee training, review whether contracts or insurance is impacted as a result of the breach and whether any disciplinary measures are appropriate for any employee responsible for the breach.

15. TRAINING

This WISP shall be provided to each of Grayson College ’s employees who has access to, or processes, ePHI/PHI, PII, SPI, and other Data owned or controlled by Grayson College. Each such individual is also required to complete a training program on information security and this WISP. The Information Security Officer shall be responsible for introducing the WISP to new employees as part of Grayson College onboarding process.

16. DISCIPLINE FOR VIOLATION OF THE PROGRAM

Consistent with Grayson College policies, the ISO is authorized by the Grayson College President to ensure that the appropriate processes to administer this program are in place, communicated to, and followed by the college community.

Administrators must ensure that measures are taken within their department to comply with this policy and its related standards, guidelines and practices. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, a written request for exception must be approved by the ISO. Approved requests will be reviewed annually to determine if an exception is still warranted.

Grayson College reserves the right to temporarily or permanently suspend, block, or restrict access to college information technology resources, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of Grayson College information technology resources; to protect Grayson College from liability; or to enforce this policy and its related standards and practices.

Failure to adhere to the provisions of this policy statement or the appropriate use policy statement may result in:

- ·Suspension or loss of access to Grayson College information technology resources
- ·Appropriate disciplinary action under existing procedures applicable to students, faculty and staff, and
- ·Civil or criminal prosecution

Potential violations will be investigated in a manner consistent with applicable laws and regulations, and Grayson College policies, standards, guidelines and practices (TAC§202.72) (TAC§202.73).

The Vice President for Administrative Services or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate college officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

Third-party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to Grayson College.

Appeals of college actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for Grayson College students and employees.

14. POLICIES CROSS-REFERENCED

The following Grayson College policies provide advice and guidance that relates to this Program:

A. Grayson College Information Security Policy
B. Grayson College Incident Response Plan.
C. Grayson College Firewall Policy
D. Grayson College Intrusion Detection Prevention and Security Monitoring Policy
E. The Grayson College Third-Party Provider Information Sharing Security Program
F. Grayson College User Password Policy
G. Grayson College User Account Policy
H. Grayson College IS-Admin Special Access Policy
I. Grayson College Malicious Code Policy
J. Grayson College Computer Policy Compliance Policy
K. Grayson College Network Use and Vulnerability Assessment
L. Grayson College Risk Assessment Guidelines
M. Grayson College Server Administration
N. Grayson College System Development & Acquisition Policy
O. Grayson College Training – Annual Mandatory Compliance
P. Grayson College Electronic Communications Policy
Q. Grayson College Media Sanitization Policy
R. Grayson College NDA Requirement Policy
S. Grayson College Privacy Policy