Grayson College

Information Handling, Backup and Retention Standard

History

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

Review

Reviewer's Details	Version No.	Date

1. BACKGROUND

The objective of this standard is to safeguard the confidentiality, integrity, and availability of Grayson College information by establishing information asset handling standards. These standards apply to server backups, tape, other removable media handling, and physical records. Also, it is essential to properly dispose of information assets after the appropriate retention period has passed.

2. SCOPE

This standard applies to employees, students, and representatives of Grayson College who use College Computer Resources (individually each a "User," collectively, Users"). A "User" includes consultants, contingent workers, and temporary employees. Any Grayson College user who is given access to College Computer Resources should also adhere to this standard concerning those resources. Grayson College's communication systems are intended for use primarily in conducting college operations. Information Governance covers all types of information about students, employees, and college users, but it also covers information about the College, and everyone within Grayson College is responsible for it.

Nothing in this Policy is intended to prohibit users from engaging in communications protected by federal state and/or local law, including but not limited to, communication related to hours, wages, or other terms and conditions of employment, or to affect employees' rights to report matters to governmental authorities in accordance with applicable law.

3. POLICY STATEMENT

The Grayson College Retention Schedule (GCRS) is adopted as an administrative rule of the Texas State Library and Archives Commission (TSLAC) in accordance with Texas Administrative Code, Title 13, Chapter 6, Section 6.10(b).

This retention schedule indicates minimum length of time records series must be retained by a public university or institution of higher education in the State of Texas before destruction or archival preservation. Additionally, the GCRS does not replace the Texas State Records Retention Schedule (RRS). Both the GCRS and RRS should be used by universities when developing their own schedule for approval by TSLAC. Records series listed on the GCRS are those that are commonly found in most public colleges and universities. The retention periods given in the GCRS are required minimums. TSLAC also recommends them as appropriate maximum retention periods.

Grayson College must submit a complete records retention schedule, entered on Form SLR 105, or an approved facsimile, to the State and Local Records Management Division of the Texas State Library and Archives Commission (Texas Government Code, §441.185).

If a federal or state statute or regulation specifies a longer retention period for any records series received, created, or maintained by an agency, the statute or regulation overrides this schedule.

4. REQUIREMENTS

A. BACKUPS

Grayson College is responsible for developing, documenting and implementing backup schedules, outlining the type of backup, interval, storage location and the number of copies for all information resources under their control, in accordance with business, legislative, regulatory and contractual requirements.

Information should be stored at a secure off-site location that is a sufficient distance away from the primary physical location for disaster recovery purposes. The off-site storage location shall have physical, environmental, and media handling controls consistent with, or higher than controls at primary locations.

Backups (media and information) shall be protected in accordance with the classification of the information being stored (e.g., encryption of information at rest).

Periodic testing of the storage media and procedures shall be conducted to ensure the ability to access information (both media and format readability) throughout the retention period, and that such information can be retrieved in an acceptable timeframe.

Users who are permitted to store College information on laptops, mobile devices, and removable media shall be required on a monthly basis to save their information on College network drives for backup purposes.

B. TRANSPORT

When physical transit of College records is required, it should be protected from unauthorized use, misuse, corruption, and physical damage and/or loss.

Paper records containing information classified as Restricted, whether sent through in-house services, government mail or private courier, should be placed in “one-time use” sealed envelopes designated “Confidential – to be opened by addressee only.” Items sent by government mail or private courier shall employ tracking options provided by the carrier

Mailroom, office, or administrative staff should maintain procedures for determining which overnight carriers should be used.

Electronic media containing information classified as Restricted (containing PII, ePHI/PHI, SPI, or confidential Grayson College information) can be shipped between College facilities or to third parties using approved commercial overnight couriers so long as the information is encrypted. The records shall be delivered to a specific party who has been notified of the expected arrival time. In-transit tracking and signature on delivery should be ordered from the courier.

Unencrypted electronic media containing information classified as Restricted shall only be transported by College management or security personnel. The media is to be secured in a locked and sealed container during transport. If travel by commercial airline is necessary, the container shall be carried on the plane and may not be checked as baggage.

Electronic media containing information classified as Restricted, such as back-up tapes and archives are typically transported by the vendor to off-site storage. The media shall be secured by the information steward in a locked and sealed metal or plastic container. The seal number shall be recorded and maintained by the information owner. It is preferable for the information steward to hand-deliver the container

to the vendor's driver, but this is not always possible. The container shall be delivered to the pick-up area no more than 1 hour prior to the pre-arranged pick up time. An employee, security officer or shipping/receiving clerk must sign for the container and maintain custody until picked up by the vendor.

Drivers for an off-site vendor shall be uniformed, bonded, and carry a company photo identification card.

Vendor's vehicles shall have a locked and alarmed cargo area. The cargo area should be air conditioned and heated.

Electronic media records deliveries can only be requested from the off-site vendor by the information owner or pre-arranged designate. If a pre-arranged delivery is to be left in the custody of an information steward or shipping/receiving clerk, the receiving party shall notify the information owner or designate immediately upon delivery.

C. STORAGE

Original paper records, such as contracts or other such paper records required for legal or regulatory purposes, shall be stored in locking fireproof cabinets or within a fire-rated enclosure of deck-to-deck construction with controlled access.

Other paper records that contain information classified as Restricted should be stored within an area with controlled access and may be stored in locking fireproof cabinets, or within a fire rated enclosure of deck-to-deck construction.

The Information Security Officer should ensure that, where required, electronic records are recoverable in the event they are lost, damaged, or altered.

Disks or tapes that contain information classified as Restricted should be stored within an area with controlled physical access.

Paper or electronic media stored off-site, shall be stored in a facility that meets or exceeds the ISO 27002 standards for Company information centers.

D. RETENTION

Grayson College should maintain suitable archiving and record retention procedures, and all backup information in storage must be handled according to the Grayson College Retention Schedule (GCRS) (Appendix

The GCRS should be reviewed at least annually to ensure alignment with the Texas State Records Retention Schedule (RRS); and that it meets current Family Educational Rights and Privacy Act (FERPA), Texas Administrative Code, Texas Government Code, Health Insurance Portability and Accountability Act (HIPAA) compliance and/or any other local, state, federal, or international requirements or law.

Disaster recovery system backups should be created for business continuity purposes only and should not serve as an electronic archive method.

The long-term retention of official electronic records stored on computer tapes or other media shall be organized such that records with comparable retention periods are grouped on the same media are classified against the GCRS and have an official retention period assigned to them.

For record retention purposes this ensures the records will be kept for the appropriate time. Where this is not feasible, all efforts must be taken to anonymize the records as much as possible and to ensure a secure method of transfer and storage.

Information is transferred from paper to electronic records, you should consider whether or not it is appropriate to keep the information in duplicate forms.

Any requests for changes to the retention schedule (such as the addition of new types of record or the amendment of a retention period) should be made in writing/email to the Information Security Officer. The Vice President for Business Services will decide whether any changes are necessary.

5. TRAINING

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

6. 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 Written Information Security Program
B. Grayson College Media Sanitization Policy

APPENDIX A

Grayson College Retention Schedule (GCRS)

Type of record	Minimum retention period
Records containing personal data or sensitive personal data– such as referral forms, drop-in data, feedback/evaluation forms	2 years
Admissions and Assessment	5 years after last attendance
Academic Records	Permanently
Financial Aid and Scholarship Records	7 years or until billing resolution has been resolved, which ever is later.
Student Privacy Records	Until Superseded: The record is replaced by an updated version. If a record subject to this retention period is discontinued or is no longer required by law
Student Conduct Records/Disciplinary Action Records	5 years after last attendance
Contact sheets detailing the support given, topics discussed, specific concerns	8 years
Contact details for the purpose of gathering feedback (email addresses alternatively, telephone numbers)	4 months
Anonymized feedback forms where data has been transferred to a computerized system or report	6 months from data entry or date of the report
Text messages	3 months
Diaries	2 years after the end of the year to which diary relates.
Training inquiries	2 years
General email messages	6 months – attachments and emails should be saved as files rather than saved in the email account
All financial and accounting records including, Daybooks, ledgers, cashbooks, ticket sales, expenses records, purchase invoices, sales orders, sales invoices, credit notes, debit notes, receipts, transactions, cheques, paying in books, bank statements, tax records	6 years
Audit reports – internal and external (including management letters, value for money reports and system/final accounts memoranda)	2 years after formal completion by the statutory auditor
Annual audited accounts and organizational records including Board minutes and agendas	Permanently
Copies of purchase orders or delivery notes	1 year
Funding agreements/SLAs	6 years

Procurement requests/quotations	2 years
Business plans	Permanently
Operational reports	6 years
Meetings and minutes papers (other, including reference copies of major committees)	6 years
Incident records – e.g., breaches of IG or Safeguarding policy, health and safety incidents,	10 years
Complaints	10 years from completion of the action
Serious incident files - events where the potential for learning or the consequences are so significant, that they warrant a comprehensive response, e.g., severe breaches of policies	20 years
Risk Management	30 years
Campus Police Arrest Records	75 years
Campus Security and Incident Reports	3 years
Death and Custody Reports	3 years
Emergency Protective Orders	Period that the order is effective or 2 years after order issued, whichever later
Campus Fire Safety Reports	Permanently
Campus Fire Log	7 years
Campus Fire Alarm and Drill Records	3 years
Subject access requests – records of requests	3 years after the last action
Payroll, income tax records, etc., and related correspondence	10 years after the end of the financial year
Recruitment records (successful)	3 years following termination of employment
Recruitment records (unsuccessful candidates)	1 year
Employment records –personnel files, letters of appointment, contracts, references, training records, equal opportunity monitoring forms, timesheets, leave/absence records, disciplinary/grievance records	6 years after the individual has left
General College Academic Program Administrative Records	5 years
Disclosure of Protected Health Information	6 years
Student Health and Counselling Records	7 years after date of last service or contact.
ADA (Americans with Disabilities Act) Accommodation Requests	3 years after last contact
Professional Accreditation Reports	Permanently