Information Security Guidelines in Support of the Information Security Policy

Overarching Information Security Strategy

Security Roles & Responsibilities

Information Security Officer

Annual Security Awareness Training

Annual Cyber Risk Assessments

Access Control

Data Classification and Protections

Data Classifications and Protections

Data Roles

Data Storage Security Safeguards

Cloud Storage of University Data

Encryption Guidelines

Bit Locker Encryption Instructions

Data Destruction

Data Destruction Schedule

****

OVERARCHING INFORMATION SECURITY STRATEGY

1. **Implement the State System Defense-in-Depth Security Architecture Principles**
    - A Defense-in-Depth Security Architecture establishes five tenets that each IT Security Program can use as guiding principles for their program.
        - Offense informs defense - Use of shared knowledge to learn and adapt.
        - Prioritization - Focus on controls that mitigate immediate risks.
        - Measurements and Metrics – Established standardized performance metrics for reporting across the State System.
        - Continuous diagnostics and mitigation – Established processes and procedures for continued monitoring and improvement of the security architecture.
        - Automation – Automate reliable and scalable security metrics and data for real-time information.

2. **Implement Center for Internet Security (CIS) Controls as our Information Technology Security Framework and Assessment**
    - The Center for Internet Security (CIS) provides security standards and best practices through the utilization of CIS Controls and Benchmarks that are used to measure gaps and capabilities of information technology security programs.

- The State System will utilize the CIS Controls as the baseline information security standard for protecting IT Resources. Information technology security assessments, to be performed on an annual basis, and are to be conducted utilizing the CIS tool 'CIS-CSAT'. Annual assessment timeframes will be communicated by the Office of the Chancellor to the Universities. Refer to Appendix C Recommended Timeline for general timeline information.
- The State System is to follow CIS assessment guidelines that focus on ensuring the CIS Controls are properly in place to mitigate information technology security threats and strengthen the State System's Defense-in-Depth Security Architecture through each University's IT Security Program.

3. **Foundational Controls and Implementation Group Baseline**
   - CIS Controls are categorized through Implementation Groups (IG) developed by CIS. We will implement IG 1 and IG 2.

4. **Information Technology Risk Management Strategy**
   - Our risk control strategies to guide and reduce identified risks.
     - **Avoidance**: To eliminate the conditions that allow the risk to be present at all, most frequently by dropping the project or the task.
     - **Acceptance**: To acknowledge the risk's existence, but to take no preemptive action to resolve it, except for the possible development of contingency plans should the risk event come to pass.
     - **Mitigation**: To minimize the probability of a risk's occurrence or the impact of the risk should it occur.
     - **Deflection**: To transfer the risk (in whole or part) to another organization, individual, or entity.

SECURITY ROLES & RESPONSIBILITIES

Information Security Team:

Information Security Officer – Manager responsible for administration and execution of the overall information security plan for Bloomsburg University of Pennsylvania.

Network Manager – Manager responsible for development and execution of the information security plan for network attached and interconnected systems.

Server Manager - Manager responsible for development and execution of the information security plan for servers and networked storage.

Individual System Administrators – Individual System Administrators are responsible for implementation and certification of the information security plan and industry best practices for information security on their assigned systems.

CONTACT INFO FOR THE INFORMATION SECURITY OFFICER

Questions regarding the classification, storage, transmission or destruction of university data should be directed to the Information Security Officer at wbarnes@bloomu.edu.

ANNUAL SECURITY AWARENESS TRAINING

All employees shall be offered annual security awareness training on various information security topics to help the employees identify information security risks and avoid common mistakes. It is strongly encouraged that all employees take this training.

ANNUAL CYBER RISK ASSESSMENTS

Annually, the information security team will update and evaluate our processes and procedures using the Center for

Internet Security (CIS) security Controls which will allow evaluation of the security standards and best practices to identify gaps and develop our risk assessment and continuous improvement program.

ACCESS CONTROL

Overarching goal: Allow employees access to the least amount of data and systems that is required for their jobs.
Access to Restricted and Sensitive data is based on job needs and supervisor approval.
Each System Administrator shall periodically review the systems they manage to verify that current users who can access the system are still valid.

DATA CLASSIFICATION AND PROTECTIONS

All data within the University shall be assigned one of the following classifications. Collections of diverse information should be classified as to the most secure classification level of an individual information component within the aggregated information.

Restricted: Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. The highest level of security controls should be applied to restricted data.

Examples include, but are not limited to Student Academic Record (FERPA), health records (HIPPAA), SSNs, Credit Card info, transcript information, student/employee data, job applicant data, confidential computing account information, documents and e-mail messages containing deliberative information, other data typically redacted when Right-to-Know requests are fulfilled, etc. Personally identifiable information (PII) is always classified as restricted. PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Sensitive: Data should be classified as Sensitive when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all institutional data that is not explicitly classified as restricted or public data should be treated as sensitive data. A reasonable level of security controls should be applied to sensitive data.

Examples include, but are not limited to any non-restricted data that requires authentication to view except if requested via Right-to-Know requests. This would include the non-redacted portions of e-mail messages, internal documents, information used to secure the university's physical or information environment, etc.

Public: Data should be classified as public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University or its affiliates. While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data.

Examples include, but are not limited any information found via a source that does not require authentication. This would include anything that can be viewed via the university's public website, mobile app, public portals, Pa. Open Records website, advertisements, job openings, university catalogs, press releases, course information, research publications, etc.

DATA ROLES

All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by the University, irrespective of the medium on which the data reside and regardless of format (such as in electronic, paper, or other physical form). The University has implemented appropriate managerial, operational, physical, and technical safeguards for access to, use of, transmission of, and disposal of University data. Restricted data require the highest level of protection. If there is uncertainty regarding the category of the data the higher level of safeguards should be applied.

Data Owner: Senior leadership, typically at the dean, director or department chair level, have the ultimate responsibility for the use and protection of university data. Data owners are responsible for appropriately classifying data.

Data User: Any member of the university community that has access to university data, and thus is entrusted with the protection of that data. Data users are responsible for complying with data use guidelines.

DATA STORAGE SECURITY SAFEGUARDS

Restricted or sensitive data should never be stored on unencrypted mobile devices (laptops, tablets, smart phones), unencrypted external hard drives, or removable media (thumb drives, CDs, DVDs). Likewise, restricted or sensitive data should never be transmitted electronically unless it is appropriately encrypted. If there is uncertainty regarding the category of the data, the higher level of safeguards should be applied. Follow the links for detailed information regarding the safeguarding and encryption of data.

General Safeguards for All Data

- Using the categories Restricted, Sensitive, or Public, all University data should be classified.
- Following initial classification, University data should remain classified at the initial level or reclassified as needed due to changes in usage, sensitivities, law or other relevant circumstances.
- Data should be protected in accordance with the security controls specified for the classification level that it is assigned.
- The classification level and associated protection of replicated data should remain consistent with the original data [e.g. (i) restricted HR data copied to a CD-ROM, or other removable-media (e.g. flash drive), or from one server to another, retains its restricted classification; (ii) printed copies of Restricted Data is also restricted].
- Any physical or logical collection of data, stored, in transit, or during electronic transfer (e.g. file, database, emails and attachments, filing cabinet, backup media, electronic memory devices, sensitive operation logs or configuration files) containing differing classification levels should be classified as a whole at the highest data classification level within the collection. Any data subset that has been separated from any such collection should be protected in accordance with the protection specified for the classification level of the data subset if assigned; otherwise, the data subset retains the classification level of the original collection and requires the same degree of protection.
- Destruction of data (electronic or physical) or systems storing data should be done in accordance with Office of Technology guidelines.

- Before systems or media are reused they should be wiped according to the Office of Technology guidelines to ensure data is unrecoverable.

Safeguards for Restricted Data

- Must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
- Should be labeled Restricted Data.
- When stored in an electronic format should be protected with strong passwords and stored on electronic devices that have protection and/or encryption measures. May only be disclosed on a strict need-to-know basis and consistent with applicable policies and statutes.
- Should be stored only in a locked drawer or room or an area where access is controlled using sufficient physical access control measures to detect and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- When sent via fax, should be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on any public website.
- Should be destroyed when no longer needed in accordance with Office of Technology guidelines, System policies or statutes.

Safeguards for Sensitive Data

- Should be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
- When stored in an electronic format should be protected with strong passwords and stored on electronic devices that have protection and/or encryption measures.
- Should be stored in a controlled environment (i.e. file cabinet or office where physical controls are in place to prevent disclosure) when not in use.
- Should not be posted on any public website unless prior approval is given by an authorized University executive and Pennsylvania State System of Higher Education Office of Legal Counsel.
- Should be destroyed when no longer needed in accordance with Office of Technology guidelines.

Safeguards for Public Data

- Public data are available to the public. Protection considerations should be applied to maintain data integrity and prevent unauthorized modification of such data. Safeguards for Public Data may include:
- Storage on an appropriately secured host.
- Appropriate integrity protection.
- Redundant systems to maintain availability as appropriate.
- Retention according to public record requirements.
- Appropriate recovery plan.

Cloud Storage of University Data

The use of cloud services (Microsoft OneDrive, Google Cloud Drive, Apple iCloud, Amazon Web Services, Box, Dropbox, etc.) for university business requires a vendor contract that has been approved by System legal counsel. The use of the cloud services must comply with applicable System and university policies, System

information security and data classification policies or guidelines, federal and state laws and regulations, and recognized best industry practices. Any decision to use cloud services for the storage of university data in the cloud should take into account the risks and liabilities related to its security, privacy, retention, access and compliance. Generally, cloud services may not be used to store or transmit "Restricted" information or "Sensitive" Data (as defined in the Data Classification section below) unless the approved cloud service contract expressly guarantees the encryption of data in transit and at rest. You may only use the cloud storage vendor(s) listed below.

Currently Approved Cloud Storage Vendors with PASSHE Contract

- ***Microsoft OneDrive***
- ***Google Drive***

Encryption Guidelines

The purpose of these guidelines is to protect restricted electronic data by recommending the use of encryption.

Definitions

Data at rest is a phrase that is used to refer to all data on a physical storage device that does not move, excluding information traversing a network or temporarily residing in computer memory. Data at rest can reside in static files that rarely or never change or can be subject to regular change.

Data in transit is any type of information that is transmitted between systems, applications or locations. Encryption of data in transit is a critical mechanism to protect that data. Unauthorized disclosure or alterations of data in transit could cause perceivable damage.

Data encryption supports data privacy and integrity by providing a method to convert electronic information into a format that is readable only by authorized individuals. These guidelines recommend the use of the following types of encryption for electronic information:

- Full Disk Encryption: Full Disk Encryption is a computer security technique that encrypts data stored on a computer's mass storage and automatically decrypts the information when an authorized user requests it. Full disk encryption is often used to signify that everything on a disk, including the operating system and other executables, is encrypted.
- Content Encryption: Content Encryption is a transparent file and folder encryption technique that ensures individual files and folders are encrypted all the time, wherever they are stored.

Guidelines

Data in Transit Encryption will be encrypted for all non-public classifications of data using approved protocols and methods from the Information Security Officer.

Data at rest: Full Disk Encryption should be used on laptop computers, other mobile computing devices, and electronic storage media for which physical security controls are limited due to the mobile nature of the devices. In cases where laptops will not store any data, exceptions could be considered.

Data at rest: Full Disk Encryption should be used on computers or computing devices storing sensitive or restricted electronic information located in areas not equipped with public access restrictions and

physical theft deterrents.

The use of removable media containing restricted or sensitive electronic information, and which serves as the primary storage device for the information, is strongly discouraged. If it is used, the removable media should be encrypted using content encryption or full disk encryption and stored in a secure, locked location. These guidelines do not apply to entities that use tape media to store non-public or sensitive electronic information.

Content or full disk encryption should be used on removable media containing any electronic information (public or non- public, sensitive or not sensitive).

Select list of approved encryption mechanisms include:

- Microsoft BitLocker (Windows)
- Kaspersky Full Disk Encryption (Windows)
- File Vault 2 (Apple OSX)
- VeraCrypt (multi-platform)
- *(Others not on this list may be approved for specific situations)*

Questions regarding the encryption of university data should be directed to the Information Security Officer at wbarnes@bloomu.edu.

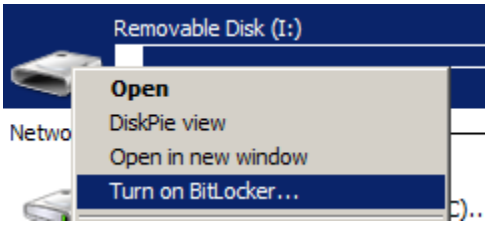
Encryption Guidelines Summary:

Encryption guidelines as a function of device type and data classification:

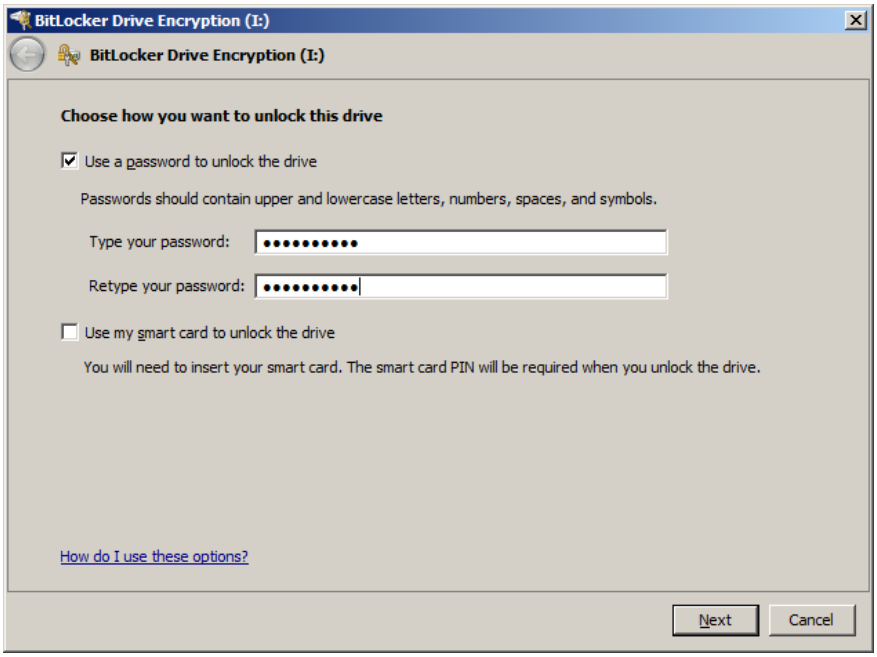
			Data Classification		
			Restricted	Sensitive	Public
Device Type	Laptops, mobile computing devices, and permanently attached storage devices		Yes (Full Disk Encryption)	Yes	No
	Removable storage devices	Primary storage	This application is strongly discouraged; requires encryption. (Content Encryption)	Yes (Content Encryption)	No
		Non-primary storage	Yes (Content Encryption or Content Transport Encryption)	Yes (Content Encryption or Content Transport Encryption)	No
	Other computers or computing devices in areas without public access restrictions		Yes (Full Disk Encryption)	No	No

Encrypting a USB drive with BitLocker on Windows

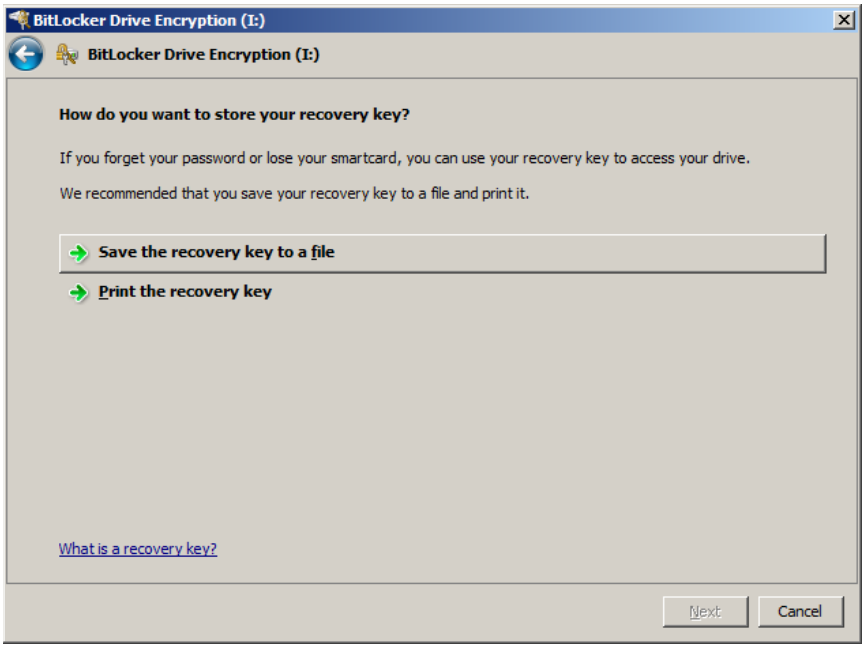
1. Right click on the USB drive in Computers and select “Turn on BitLocker.”



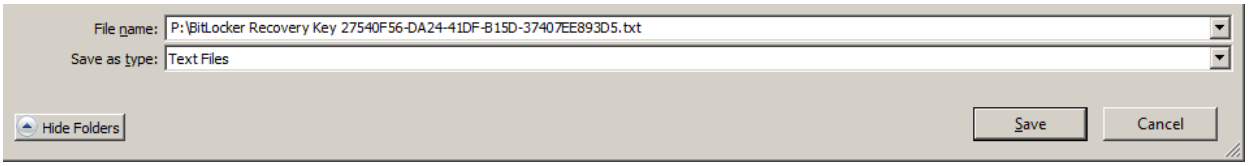
2. Pick a strong password that you will remember.



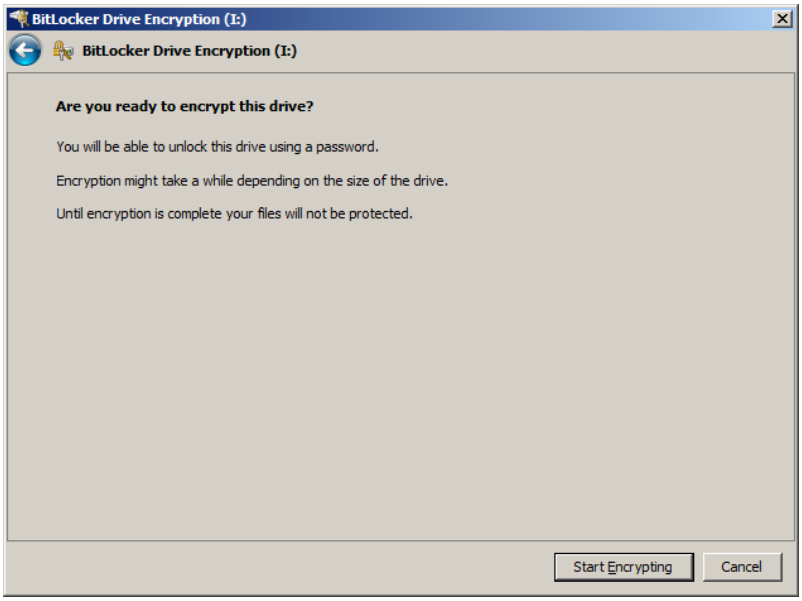
3. Please save the Recovery Key to a file.



4. Save this recovery key to your P:\ drive. (quickest way is to click on the filename and add “P:\” to the front.

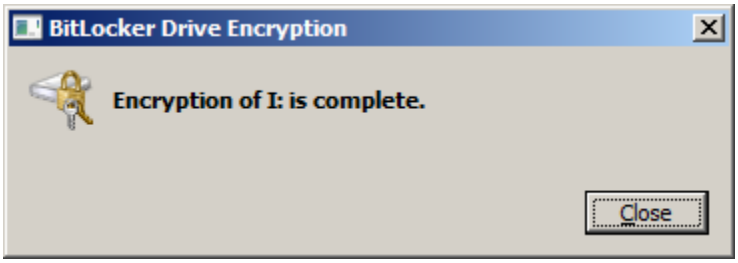


5. Click “Start Encrypting” to start the process:

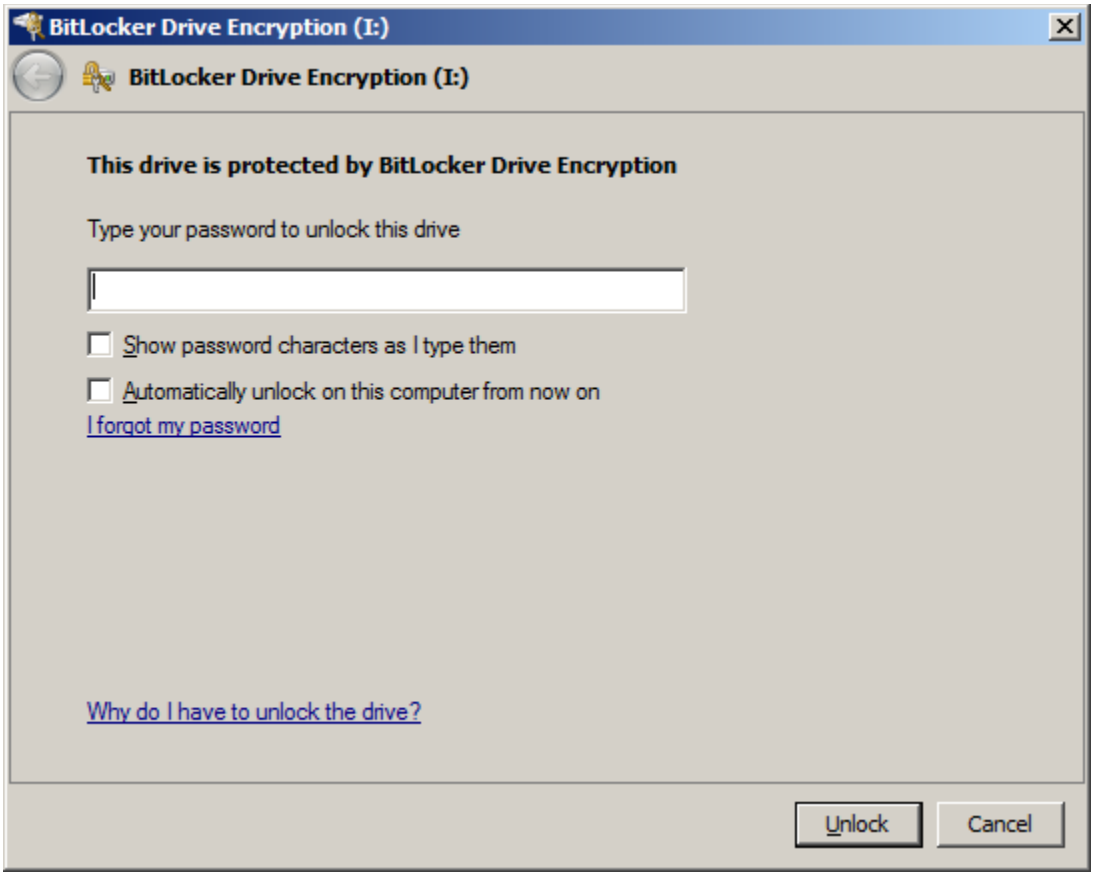


6. Let it encrypt until it is finished.

7. When it is finished, click Close.



When you are ready to use this on a different windows computer, plug it in and open it.
It will prompt you for the password you used when encrypting it and click on “Unlock”.



Destruction of Data Guidelines:

Electronic data: Data stored on a magnetic medium, such as a hard disk, should be sanitized using a disk wipe software that uses 3 passes of random data, at minimum. If this is not feasible, please contact the Information Security Officer at wbarnes@bloomu.edu for further assistance to use the Staples Serialized Secure Data Destruction.

Paper Data: All data on paper must be shredded in a crosscut paper shredder. If this is not feasible, please contact the Information Security Officer at wbarnes@bloomu.edu for further.

Other: Please contact the Information Security Officer at wbarnes@bloomu.edu for assistance.

Data Destruction Schedule

TYPE OF RECORD	OFFICIAL REPOSITORY	DURATION (YEARS)
Benefit Enrollment/Change Forms and Applications	HR/ Benefits	Permanent
Employee Service Records for Retirement	HR/ Benefits	Permanent

Family Medical Leave Act Case Files and Other Medical Documentation for Leave Requests	HR/ Benefits	3 years after case closed or 3 years after separation (whichever is later)
Report of Occupational Injury or Illness and Workers' Compensation Claims and Supporting Documents	HR/ Benefits	For hazard exposure, 30 years after employee separation; otherwise 6 years after claimant stops treatment
Application for Retirement Membership	HR/ General	Permanent
Background Checks	HR/ General	25 Years
Classification and Supporting Documents	HR/ General	10 years
Position Descriptions	HR/ General	To age 75 or 4 years from date last employed
H-1 Visa Scholar Records (temporary employment of internationals under INS regulations)	HR/ General	6 years after expiration of VISA
Official Employee Personnel Files (including application, resume, appointment, salary changes/ salary forms, contracts)	HR/ General	Permanent
Performance Appraisals – Faculty	HR/ General	Keep first 5 appraisals; keep only most recent if post-tenure; upon separation maintain only most recent in OPF
Performance Appraisals – Staff	HR/ General	Keep 3 most recent appraisals; upon separation maintain only most recent in OPF
Sabbatical Leave, Promotion, and Tenure Records	HR/ General	Permanent – approval letter and faculty's sabbatical report; if declined, declination letter
Search Records, including employment applications, resumes, and all applicant search materials	HR/ General	3 years
Tuition Waiver Records	HR/ General	4 Years
Arbitration awards and related documents	HR/ Labor Relations	Permanent
Collective bargaining agreements	HR/ Labor Relations	Permanent

Grievances/ Complaint Issues	HR/ Labor Relations	Permanent
Strike Planning Documentation	HR/ Labor Relations	Permanent
Union Meet and Discuss Minutes	HR/ Labor Relations	10 years
Union Subject Documentation (Side letters, Memos, Correspondence)	HR/ Labor Relations	Permanent
Annual Statement of Financial Interests Disclosure Form	HR/ Payroll	5 years
Camp Workers Payroll Records	HR/ Payroll	Permanent
Financial Disclosure Appeal Form	HR/ Payroll	4 years
I-9 and Employment Forms (Faculty and Staff)	HR/ Payroll	5 years after date of hire, or 1 year after separation (whichever is later)
Imputed Income Records (cell phone usage, etc.)	HR/ Payroll	Permanent
Orientation Workshop Leaders Payroll Records	HR/ Payroll	Permanent
Payroll Correction Records	HR/ Payroll	5 Years
Payroll Deduction Authorization Records (Union dues, bonds)	HR/ Payroll	2 Years
Payroll Register	HR/ Payroll	Permanent
Record of Absence	HR/ Payroll	4 Years
Record of Earnings (W2s, Quarterly Reports)	HR/ Payroll	Permanent
Sick Leave Bank and Donations	HR/ Payroll	7 years
Time, Attendance and Leave Records (Timekeepers' copy)	HR/ Payroll	7 years
Time Records (OT only)	HR/ Payroll	3 Years
Unemployment Comp Records for Individual Employees	HR/ Payroll	3 Years

Employment Verification	HR/ Payroll (Student)	4 years
FICA – Student Schedules	HR/ Payroll (Student)	4 years
Graduate Assistant Contracts	HR/ Payroll (Student)	5 years
I-9 and Employment Forms (includes Change of Address, Direct Deposit, and Local Service Tax Forms)	HR/ Payroll (Student)	5 years after date of hire, or 1 year after separation (whichever is later) Local Service Tax Forms kept only 2 years after date of hire
J-1 or F-1 Visa records (NRA students)	HR/ Payroll (Student)	10 years
Time Records (includes E-time exceptions)	HR/ Payroll (Student)	5 years
Search and Screen Files	Social Equity/HR	3 years from final disposition date (closed, failed, canceled)
Establishment/renewal of Temporary Pool Documents (ad, criteria rating sheet, questions)	Social Equity	3 years from temporary pool expiration date