Bloomsburg University of Pennsylvania
Office of Planning and Assessment

CODE OF ETHICS AND PROFESSIONAL PRACTICE

CONTEXT
The Code of Ethics and Professional Practice for the Office of Planning and Assessment is an adoption of The Code of Ethics and Professional Practice of the Association for Institutional Research (AIR, 2013) with modifications to better align with the context and culture of Bloomsburg University's Office of Planning and Assessment.

PREAMBLE
The Code of Ethics and Professional Practice for the Office of Planning and Assessment (OPA) aims to provide OPA members and colleagues with broad ethical statements to guide their professional lives and to identify relevant considerations when ethical uncertainties arise. The Code of Ethics and Professional Practice also provides a means for individuals new to the profession to learn about the ethical principles and standards to guide their work.

While OPA adheres to Bloomsburg University policies and supports Bloomsburg University's mission to prepare students for personal and professional success, this Code adds to those existing responsibilities and documents. This Code helps define a normative expectation for OPA personnel in their work.

Although the Code provides standards, it does not provide a set of rules. Reasonable differences of opinion can and do exist with respect to interpretation, and specific application must take into account the context of a given behavior. Adoption of a code of ethics cannot guarantee ethical behavior or resolution of all disputes. Rather, it sets forth standards to which professionals aspire and against which their actions can be judged (both by themselves and others). Ethical behavior should result from a personal commitment to engage in ethical practice and an attempt to act always in a manner that assures integrity.

All members of OPA should pledge to maintain their own competence by continually evaluating their work for accuracy, by conducting themselves in accord with the ethical standards expressed in this Code, and by remembering that their ultimate goal is to contribute positively to the field of postsecondary education and student success.

Finally, this Code is a living document that must change and be shaped as the field and practice of assessment continues to evolve and develop.

SECTION I – COMPETENCE

(a) **Acceptance of Assignments.** Accept assignments within one's scope of expertise. Be transparent about limitations of expertise and consult with other professionals when in doubt.

(b) **Provision of Professional Development Opportunities.** Participate in professional opportunities provided by management. Continue to develop professional skill sets as a regular duty.

(c) **Professional Continuing Education.** Develop, maintain, and advance professional skills, knowledge, and performance.

SECTION II – PRACTICE

(a) **Objectivity**.
- i) Unbiased Attitude. Approach all assignments with acknowledgement of personal biases and make all attempts to minimize their effect.
- ii) Conflicts of Interest. Disclose situations in which financial, ethical, or other personal considerations may compromise, or have the appearance of compromising, decisions or the performance of services.

(b) **Use of Accepted Technical Standards.** Conduct all tasks in accordance with accepted technical standards.

(c) **Request Process**. Channel all requests for information or data through the Assistant Vice President of Planning and Assessment for approval whether information or data requested is confidential or not.

(d) **Initial Discussions.** Clarify initially and continuously with the sponsor and/or major users the purposes, expectations, strategies, and limitations of the research.
- i) Recommend research techniques and designs that are appropriate to the purposes of the project.
- ii) Inform sponsors and/or major users if research is likely to yield unreliable results.

(e) **Identification of Responsibility.** Accept or assign responsibility for the competent execution of all assignments and display individual and/or office authorship.

(f) **Quality of Secondary Data.** Exercise reasonable care to ensure the accuracy of data gathered by other individuals, groups, offices, or agencies and document the sources and quality of such data.

(g) **Reports.** Ensure that all reports and projects are complete, clearly written in language understandable to decision-makers, distinguish among assumptions, speculations, findings, and judgments, employ appropriate statistics and graphics; describe the limitations of the project, analytical method, and findings, and follow scholarly norms in the attribution of ideas, methods, and expression and in the sources of data.

(h) **Documentation.** Document the sources of information, methodology for analysis, and arrival at findings to generate institutional memory.

SECTION III – CONFIDENTIALITY

The following information is aligned with Bloomsburg University Policy and Procedure 2510 (Information Security Policy). PRP 2510 "acknowledges the need to protect the confidentiality, integrity and availability of Bloomsburg University data and the systems that store, process, or transmit it".

(a) **Atmosphere of Confidentiality.** Establish necessary procedures and protocols surrounding confidential matters.

(b) **Storage and Security.** Organize, store, maintain, analyze, transfer and/or dispose of data to reasonably prevent loss, unauthorized access, or divulgence of confidential information. Safeguard all sensitive data to guarantee privacy and confidentiality.
   i) Ensure no confidential data is stored on the internal unit drive (shared drive).
   ii) Share and/or transfer confidential data with appropriate personnel via secure and encrypted methods.

(c) **Release of Confidential Information.** Permit no release of information about individual persons that has been guaranteed as confidential, to any person inside or outside the University and/or the Pennsylvania State System of Higher Education (PASSHE) except in those circumstances in which not to do so would result in clear danger to the subject of the confidential material or to others; or unless directed by competent authority in conformity with a decree of a court of law.
   i) Report all requests for confidential data from external entities to the Assistant Vice President of Planning and Assessment, who will report requests to appropriate personnel and channels including the Associate Vice President of Technology and Library Services.

(d) **Special Standards for Data Collection.**
   i) Balancing Privacy Risks Against Benefits. Explore the degree of invasion of privacy and the risks of breach of confidentiality that are involved in the project, weigh them against potential benefits, and make therefrom a recommendation as to whether the project should be executed, and under what conditions.
   ii) Developing Specific Guidelines. Adopt a written description of any specific steps beyond the regular guidelines within the Office of Planning and Assessment that are necessary during a specific assignment to ensure the protection of privacy and confidentiality that may be at specific risk.
   iii) Disclosure of Rights. Ensure all subjects are informed of their right of refusal and of the degree of confidentiality with which the material that they provide will be handled, including where appropriate, the implications of any freedom of information statute. Any limits to confidentiality should be made clear.
   iv) Appraisal of Implications. Apprise university authorities of the implications and potentially binding obligations of any promise to respondents regarding confidentiality and shall obtain consent from such authorities where necessary.

SECTION IV – RELATIONSHIPS TO THE COMMUNITY

(a) **Equal Treatment.** Promote an inclusive workspace with equal opportunity and access regardless of race, creed, gender, sexual orientation, national origin, disability or other accidental quality.

(b) **Development of Local Codes of Ethics.** Continuously reflect on and improve this Code of Ethics to align with the mission and duties of the Office of Planning and Assessment. Circulate OPA's Code of Ethics to the campus community and spread awareness of ethical obligations surrounding work with data and research.

(c) **Custody and Archiving.** Acknowledge data as an institutional historic resource and maintain compliance with Bloomsburg University Policy and Procedure 2200 (Records Management Policy for Historic University Records). Prevent irrevocable loss of data and documentation and advocate for its systematic permanent archiving.

(d) **Self-Assessment.** Develop and implement periodic assessment to evaluate the effectiveness of services provided by the Office of Planning and Assessment.

(e) **Institutional Confidentiality.** Obey policies and procedures set forth by the University and PASSHE that surround confidentiality and/or working with sensitive and confidential data, and adopt additional provisions to safeguard data, as necessary.

(f) **Institutional Review Board (IRB) Approval.** Seek and obtain IRB approval for all research involving human subjects. Know and adhere to Bloomsburg University Policy and Procedure 3990 (Institutional Review Board (IRB) for Human Subjects Research).

(g) **Integrity of Reports.** Ensure accurate understanding and utilization of reports within the university through careful and deliberate presentation and documentation of reports, and continuous promotion of reports. Amend immediately distortions or inappropriate utilizations of authored and/or promoted reports.

(h) **External Reporting.** Submit and/or disseminate accurate information and engage in responsible reporting to federal, state, and governmental agencies, accrediting bodies, and university-wide stakeholders while complying with the standards of accuracy, confidentiality, and professionally responsible interpretation.

Professionally responsible interpretation includes consideration of how the requesting individuals or organizations will employ the information. A sound understanding of how information will be used is fundamental to decisions regarding what type of information and supporting materials is appropriate and whether to participate with the request.

SECTION V – RELATIONSHIPS TO THE CRAFT

(a) **Research Responsibilities.**
- i) Seek opportunities to contribute to and participate in research on issues directly related to assessment, compliance, student success, and other professional activities. Encourage and support the campus community in such endeavors.
- ii) Take responsibility and credit only for work actually performed and/or contributed toward, and acknowledge the work and contributions of others.

(b) **Integrity of the Profession.** Maintain and promote high standards of practice.
- i) Uphold and advance the values, ethics, knowledge, and mission of the profession, and protect, enhance, and improve the integrity of the profession through appropriate study and research, active discussion, and responsible criticism of the profession.
- ii) Contribute to the knowledge base and share with colleagues, through formal and informal means, knowledge related to practice, research, and ethics.

(c) **Professional Accountability**.
- i) Educate colleagues on the standards outlined in this Code and their relevant ethical obligations.
- ii) Hold consultants and third party vendors accountable to the standards outlined in this Code. Initially and continuously clarify with all parties the purposes, expectations, strategies, and limitations of partnership endeavors. Identify and articulate the responsibilities for each party to ensure ethical standards are upheld throughout the entirety of partnership endeavors. This includes distinguishing circumstantial responsibilities (e.g., if student data is moved off the University's server and stored in the cloud, what party is responsible for ensuring data security?).

(d) **False Accusations.** Uphold the reputation of, and never publicly, unjustly, or unfairly criticize the work of colleagues.

(e) **Incompetence of Colleagues.** Consult with colleagues or supervisors, when feasible, and assist in taking remedial action to address incompetence. Report incompetent conduct using University and PASSHE guidelines if efforts to change a colleague's incompetent behavior or practice are unsuccessful, or result in the breach of sensitive information.

(f) **Unethical Conduct of Colleagues.**
- i) Take appropriate measures to discourage, prevent, identify, and correct unethical conduct of colleagues when their behavior is unwittingly or deliberately in violation of this code or of good general practice in institutional research or assessment.
- ii) Seek resolution of unethical behavior of a colleague by discussing the concerns with said colleague or supervisor when appropriate.
- iii) Maintain ethical and professional obligations to report unethical conduct using University and PASSHE guidelines if efforts to change a colleague's unethical behavior or practice are unsuccessful or results in the breach of sensitive information.

Approved by OPA members August 17, 2018

Bloomsburg University's Mission

University Mission

Bloomsburg University of Pennsylvania is an inclusive comprehensive public university that prepares students for personal and professional success in an increasingly complex global environment.

University Values

Bloomsburg University students, faculty and staff value:

» Collaboration Community Critical thinking
» Diversity Excellence Integrity
» Knowledge Opportunity Respect
» Personal and professional growth

University's Vision

Bloomsburg University aspires to:

- be a premier public comprehensive university, recognized as a center of thinking, learning and academic excellence.
- anticipate and address the changing needs of the Commonwealth.
- be a diverse community that produces positive change.
- provide resources to maximize opportunities for success.
- be a good steward of our resources and the environment.
- develop individuals to be contributing citizens.

Source: http://intranet.bloomu.edu/mission

PRP 2510 – Information Security Policy

Document History

Recommended by the General Administrative Committee: February 23, 2016
Endorsed by University Forum: April 20, 2016

1. Rationale for Policy

The Information Security Policy acknowledges the need to protect the confidentiality, integrity and availability of Bloomsburg University data and the systems that store, process or transmit it. This policy applies to all faculty, staff, vendors and other university affiliates who are authorized to access university data.

2. Keywords

information security, security, security policy, institutional data.

3. Background Information

All Bloomsburg University data, and the systems that store and transmit the data, must be protected from unauthorized access and use. All Bloomsburg University personnel and others who have authorization to access university data must be aware of their obligation to protect university data. This is particularly relevant since cloud storage services allow university personnel to place university data on non-university systems. Therefore, it is necessary to have in place appropriate local policies and procedures, as well as formal contracts with cloud storage vendors, which ensure the protection of all university data. Only cloud storage vendors who have current contracts with Bloomsburg University can be utilized to store university data. The University's Office of Technology maintains a list of vendors with whom the university has formal cloud storage contracts. The list can be found in the **Information Security Guidelines in Support of Information Security Policy**.

4. Policy

Throughout its lifecycle, all university data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved by the University's Office of Technology and maintained by the information security officer, given the level of sensitivity, value and criticality that the university data has to the University. The documentation can be found in the **Information Security Guidelines in Support of Information Security Policy**.

Any university information system that stores, processes or transmits university data shall be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved by the University's Office of Technology and maintained by the information security officer, given the level of sensitivity, value and criticality that the university data has to the University. The documentation can be found in the **Information Security Guidelines in Support of Information Security Policy**.

Individuals who are authorized to access university data shall adhere to the appropriate roles and responsibilities, as defined in documentation approved by the University's Office of Technology and maintained by the Information security officer. The documentation can be found in the **Information Security Guidelines in Support of Information Security Policy**.

Maintenance
This Policy will be reviewed by the University's Office of Technology as deemed appropriate based on changes in technology or regulatory requirements.

Enforcement
Violations of this policy may result in suspension or loss of the violator's use privileges, with respect to university data and university owned information systems. Additional administrative sanctions may apply up to and including termination of employment (for personnel) or cancellation of contracted services (for vendors). Criminal or civil prosecution under local, state or federal laws may also apply.

Exceptions
Exceptions to this Policy must be approved by the Office of Technology, in consultation with the Executive Staff, and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Definitions
University data is defined as any data that is owned or licensed by the university.

Vendor is defined as any third party that has been contracted by the university to provide a set of services and who stores, processes or transmits university data as part of those services.

Source: http://intranet.bloomu.edu/policies_procedures/2510

Information Security Guidelines in Support of the Information Security Policy

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.

Data Classifications

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*** is currently the only authorized cloud storage solution

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

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.

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.

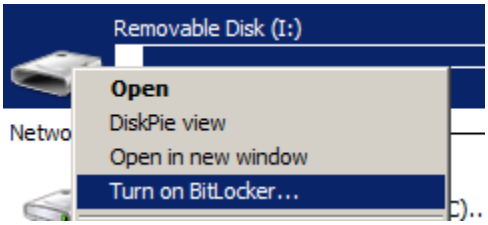
Encryption Guidelines Summary:

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

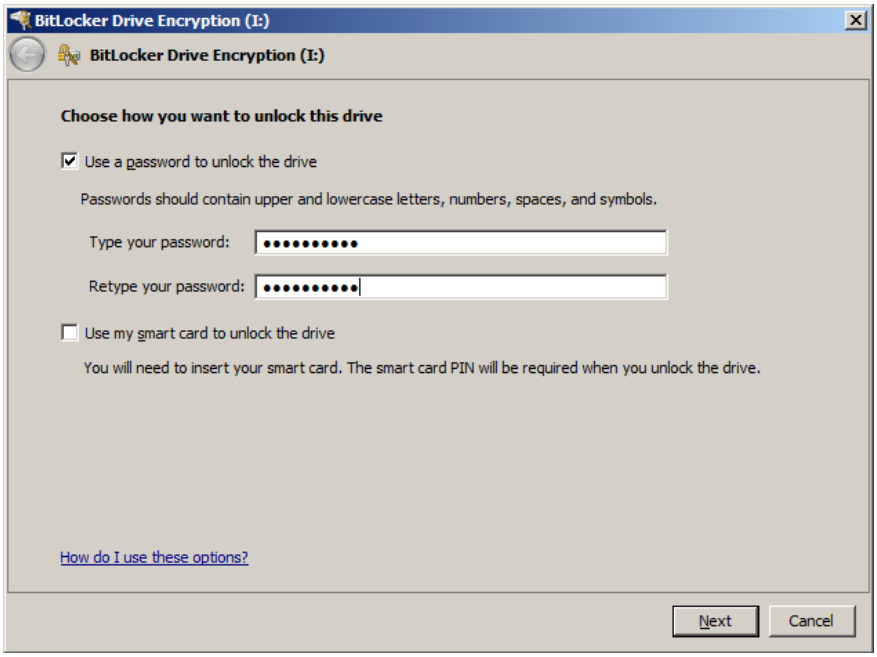
			Data Classification		
			Restricted	Sensitive	Public
Device Type	Laptops, mobile computing devices, and permanently attached storage devices		Yes (Full Disk Encryption)	Yes	No
	Removable storage devices	Primary storage	This application is strongly discouraged; requires encryption. (Content Encryption)	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

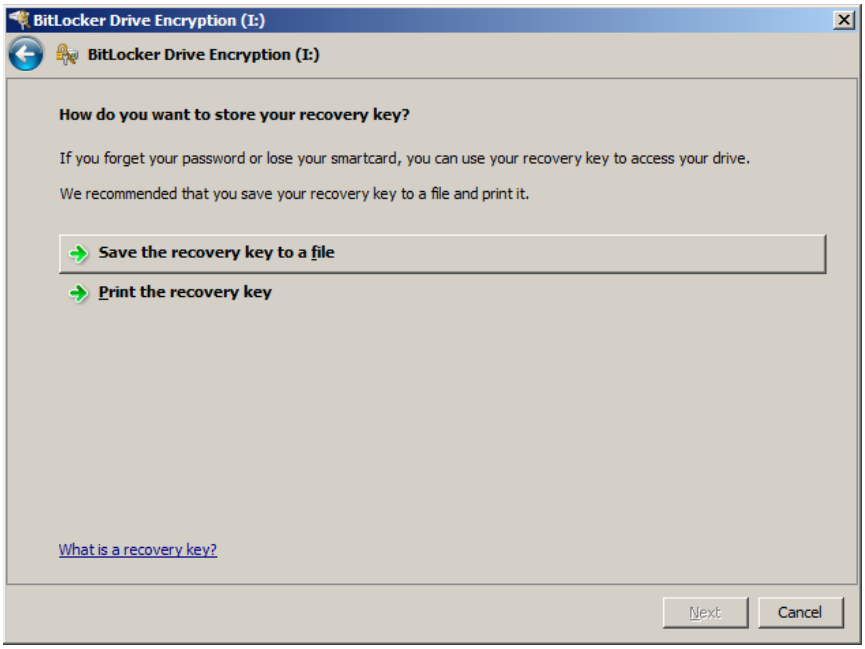
1. Right click on the USB drive in Computers and select “Turn on BitLocker.”



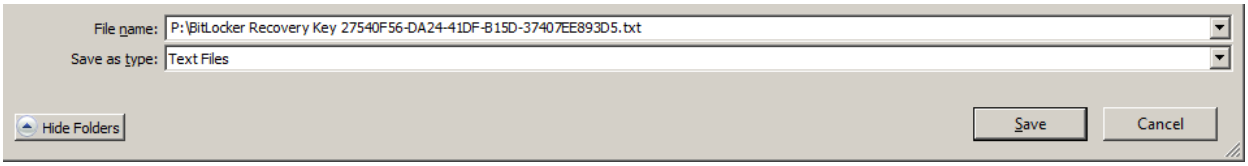
2. Pick a strong password that you will remember.



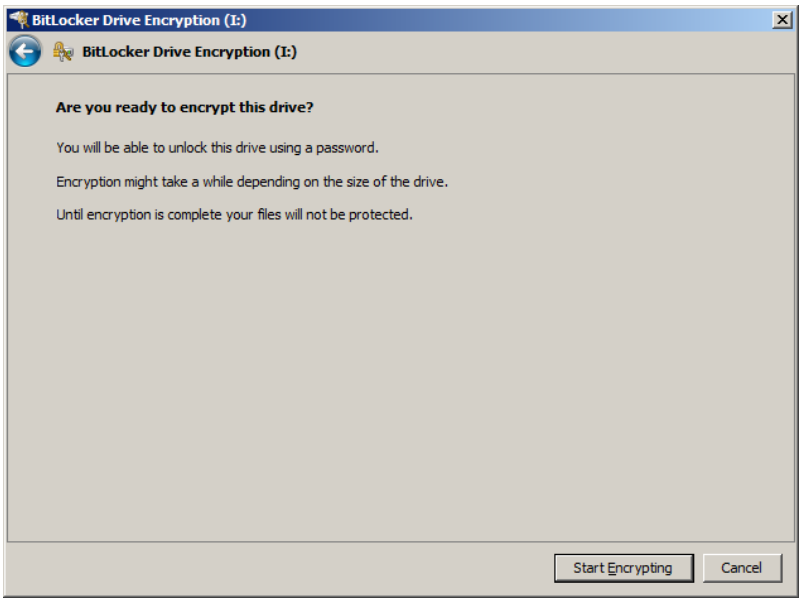
3. Please save the Recovery Key to a file.



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

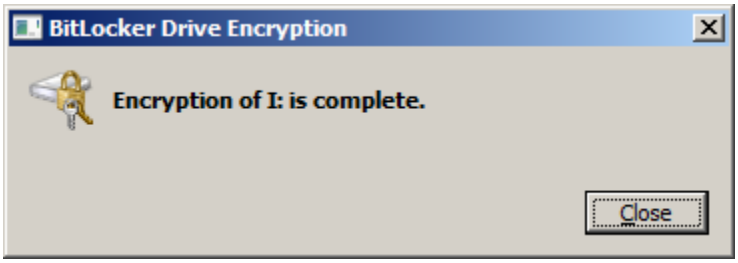


5. Click “Start Encrypting” to start the process:

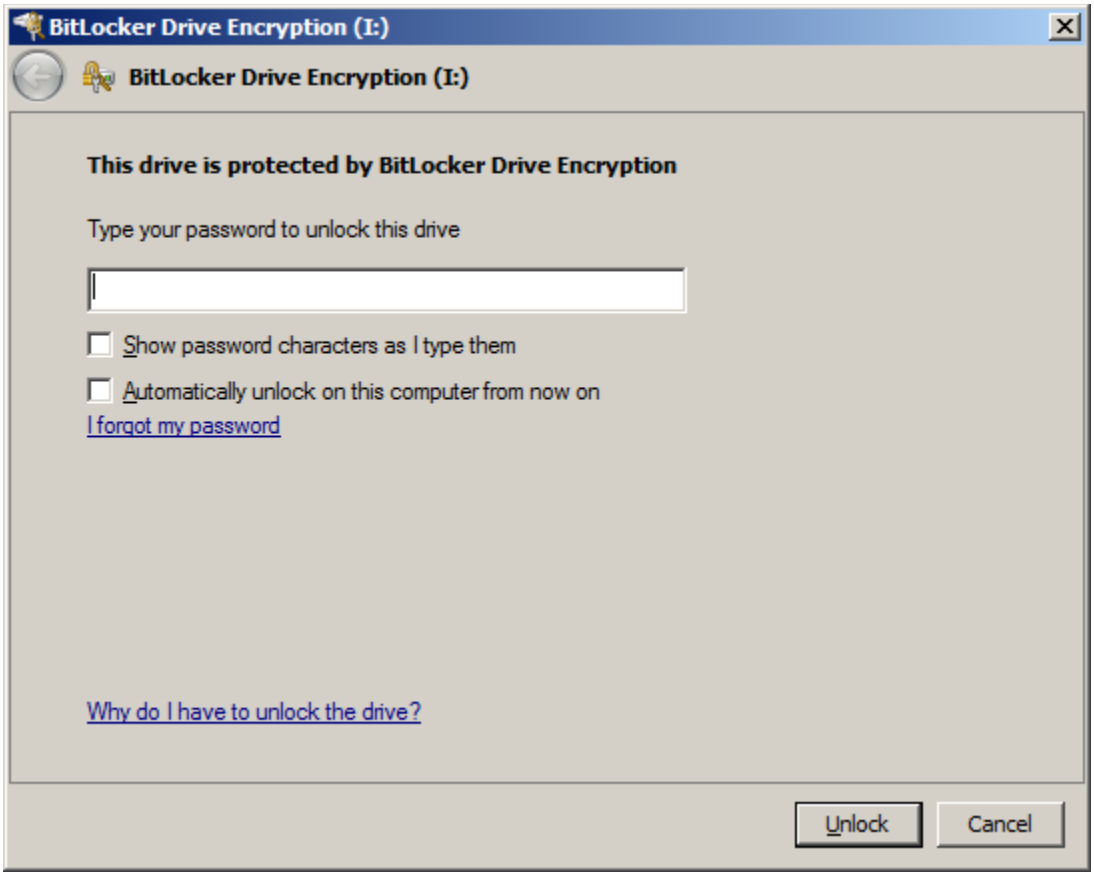


6. Let it encrypt until it is finished.

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

Source: http://intranet.bloomu.edu/documents/tech/InformationSecurityGuidelines.pdf

PRP 2200 – Records Management Policy for Historic University Records

Issued by: James Mackin, Ph.D., Provost and Vice President for Academic Affairs
Notes: Issued by Wilson Bradshaw, Provost and Vice President for Academic Affairs. Effective date: May 29, 1996. Reviewed/endorsed by President's Cabinet February 22, 1996. Revised and endorsed by Forum April 25, 2007.

I. Purpose

To establish general procedures for the permanent preservation of University records of enduring and historic value and to authorize the work of the University Archivist and University Archives for the maintenance of these records.

II. Definition

University records are those produced or received by any agency, affiliated organization, or employee of the University in the official transaction of university business. Records, as defined in this policy, include information recorded in the conduct of the University's mission and bearing directly upon the activities and functions of the University or its officers and employees, regardless of medium or characteristics. The University's records include, but are not limited to, traditional paper documents such as printed forms, reports, correspondence, directives and publications; drawings; engineering diagrams; photographs; films; photographic images of paper records stored as micro-print; and any information produced by computers or other electronic media and stored as discs, tapes, or other machine readable media and data.

III. Policy

A. University Archives Administration of Historic Records

It is the responsibility of the University Archivist to oversee the operations of the University Archives and to work with the managers of all units to identify the permanently valuable records of the University. These managers, in consultation with the Archivist, will also work to identify those records not appropriate for long-term retention. The final decision regarding records that are appropriate for the University Archives resides with the manager of the relevant area. The University Archives, a division of the Harvey A. Andruss Library, is the official repository for the permanent retention of University records having enduring, research and historical values. The University Archives also includes professional and personal manuscript collections donated by members of the academic and administrative staffs and the records of faculty and student organizations. In the execution of the duties of this position, the University Archivist directs the established archival functions of: appraisal, accessioning, preservation, arrangement, description, reference service, exhibition and publication.

B. Types of University Records of Historic Value

The following list of University records of historical value is suggestive. Documentation need not be restricted to these types of records, and it is the responsibility of the University managers, in cooperation with the Archivist, to appraise any additional records that could be considered as having historical value to Bloomsburg University, and revise this list accordingly. As part of their normal duties in maintaining the records of their office, departmental and committee secretaries will work with the Archivist to see that those records determined to be historical are transferred to the Archives on a schedule to be determined by each office. The Archives should also be included on all campus mail and email lists for approved minutes, reports, publications and other University records as defined in this policy. Exceptions or restrictions on access to records can be worked out with the Archivist.

1. Constituting documents (e.g., charters, constitutions, by-laws), policy statements, planning documents, reports [See Glossary] (along with their supporting materials), approved minutes, and subject files [See Glossary] of the University's:

- Council of Trustees;
- President's Office and offices for Academic Affairs, Administration, and University and Student Affairs and all of their reporting units;
- Material from major academic and administrative committees specified in University governance, with the exception of the Institutional Review Board and Promotion, Tenure, and Sabbatical Committees.

2. Reports of:

- self-studies, including 5-year reviews, and accreditation visits;
- annual budgets and audits;
- offices of admissions, institutional research, university relations-public relations both on- and off-campus and development (fundraising);
- research projects.

3. Historically significant records of:

- departments, e.g., subject files, approved minutes, syllabi and course materials, reports, course and program proposals, manuals;
- offices, e.g., subject files, minutes, reports, budgets;
- current, retired, resigned, terminated, or deceased personnel the school employed, e.g. vitae, biographical materials, publications;
- the registrar, e.g., calendars, course descriptions and schedules, graduation rosters, and other reports issued on a regular basis.

4. All University publications produced both on- and off-campus, including newsletters, posters, brochures, flyers, booklets and all promotional materials about or distributed in the name of the institution. These include but are not limited to posters, magazines, catalogs, special bulletins, yearbooks, student handbooks and newspapers, university directories and faculty/staff rosters, alumni magazines, and ephemeral materials [See Glossary]. At least one copy of all publications formerly in print and currently produced solely in electronic form will be made available to the Archives by the originating office. This is to be done in either format (or preferably both) on an ongoing basis whenever a new version is made available.

5. Special format materials documenting the operation and development of the institution, such as:

- audio, audiovisual and multi-media productions - still photographs, slides, and negatives, films, CDs and DVDs, audio and video cassettes;
- maps, blueprints, and plot plans of the campus and its buildings.

6. Masters and Honors theses, and student and departmental papers presented in lieu of a thesis.

7. Digital and other electronic records and databases or lists of where such items are maintained and finding aids for accessing them.

8. Artifacts related to the institution as space permits.

9. Records and papers produced and donated by University-related individuals, e.g., faculty, staff, and students while actively connected with the University, and alumni; records of academic, honorary, service, and social organizations of students, faculty, administrators, and staff on campus; manuscript collections related to Bloomsburg University.

Glossary of Terms

Ephemeral Materials - Items, usually printed documents (e.g. advertisements, tickets, and brochures) created for a specific, limited purpose, collected by a repository as examples for use in exhibits. Individuals often collect ephemera as mementos or souvenirs because of their association with some person, event, or subject.

Report - A document containing the results of an investigation or research, with a narrative, summary, or record of events, decisions, and understandings. Reports can be routine, issued at regular intervals to provide information on normal operations; or periodic, being special reports which analyze a specific problem, opportunity, idea, or physical entity.

Subject File - A collection of file folders containing documents, created by an office or individual, relating to various topics and arranged in alphabetical order by folder heading. Subject files can relate to any type of topic, such as an action, event, organization, person, place, project, or other subject.

Source: http://intranet.bloomu.edu/policies_procedures/2200

PRP 3990 – Institutional Review Board (IRB) for Human Subjects Research

Issued by: James Mackin, Provost and Vice President for Academic Affairs
Effective Date: Fall, 2008
NOTES: Amended by Institutional Review Board Fall, 2002 Reviewed by Graduate Council, January, 1994 BUCC approved April 13, 1994, Forum approved October 19, 1994 Reviewed by Graduate Council, December 6, 2002 BUCC approved April 16, 2003 Reported to Forum Nov. 17, 2004 Amended by Institutional Review Board, December, 2007, Endorsed by Graduate Council, December 7, 2007. Approved by BUCC February 6, 2008. Reported to Forum
Prior version of this policy
Feb. 27, 2008.

Bloomsburg University recognizes its ethical and legal responsibilities to provide a mechanism to protect individuals involved as subjects in research conducted under the auspices of the University. Research, as defined by the Bloomsburg University Graduate Council Research Committee, is the systematic inquiry/investigation of a specified problem or set of problems with the goal of advancing the discipline. Therefore, all research involving human subjects will be reviewed, prior to the initiation of the research, through the procedures set forth by the University and directed by the Institutional Review Board (IRB). Failure to submit research for review and approval is a violation of Bloomsburg University policy.

Rationale

The University policy entrusts the investigator with the primary responsibility for protection of individual subjects. The University assumes the responsibility for ensuring the conditions for protecting human subjects as required by the National Research Act, Public Law 93-348 and implemented by the Department of Health and Human Services (Title 45 CFR 46, Protection of Human Subjects, as amended and by other Federal agencies with appropriate jurisdiction.) The complete document can be reviewed online at the **National Institutes of Health Office of Human Subjects Research, Regulations and Ethical Guidelines**.

The University assumes responsibility for encouraging research activities to benefit advancement of knowledge of human conditions and, at the same time, protecting the rights and welfare of human subjects, the investigators, and the University. This includes assuring the scientific validity of the research methodology as it relates to the protection of human subjects. University faculty, staff, and students conducting human subject research are responsible to comply with this policy and all federal regulations. The IRB reserves the authority to suspend or terminate approval of research that is not being conducted in accordance with the Bloomsburg University IRB policy #3990

Structure

The IRB has the responsibility and authority to review and approve all research involving human subjects.

All proposals in the "Exemption from review" category will be processed by the Director of the Office of Research and Sponsored Programs and the Assistant Vice President and Dean of Graduate Studies and Research. They may be aided in the reviews by members of the IRB committee.

IRB Membership

The IRB shall be appointed by the Provost and Vice President for Academic Affairs. Federal guidelines indicate that members should possess a sufficient background to be able to look at ethical issues and the committee should contain a balance of males and females. A committee comprised of the current IRB Chair, the Director of the Office of Research and Sponsored Programs, and the Assistant Vice President and Dean of Graduate Studies and Research, in consultation with the appropriate college dean, will determine the faculty to be recommended to the Provost to fill the five federally required roles. College representatives will be selected by each college dean from the faculty and recommended to the Provost.

All those considered for membership will have a demonstrated record of research/scholarly activity and/or previous IRB experience, and agree to participate fully in the work of the IRB committee. In compliance with federal guidelines, voting members will be appointed to fill the five federally required roles of (1) science representative, (2) non-science representative, (3) ethicist, (4) diversity issues representative, and (5) a representative from outside the university. In addition to those five mandated positions one voting representative from College of Business, College of Professional Studies, College of Science and Technology, and College of Liberal Arts will be appointed. Thus the IRB membership roster will consist of 9 voting positions.

As allowed by the federal guidelines, an alternate will be appointed for each position, bringing the IRB membership list to a total of 18 individuals. These alternate members are encouraged to participate fully in the work of the IRB committee and are eligible to review expedited proposals. Alternates will vote on occasions when a voting member is absent or when the area of expertise needed for the review is closer to that of the alternate than the voting member. All members must complete the National Institutes of Health IRB Computer-Based Training Course or equivalent before being eligible to vote.

The term of office will be staggered two-year terms. The Assistant Vice President and Dean of Graduate Studies and Research and the Director of the Office of Research and Sponsored Programs will serve as ex officio, non-voting, members. The chair will be elected yearly by and from among the voting members of the IRB.

Administration

The University official responsible for carrying out or delegating executive functions is the Provost and Vice President for Academic Affairs. The executive functions include developing and modifying policy to conform to laws and regulations; providing continuing education for personnel with respect to policy; and providing administrative support and legal assistance to the IRB.

Procedures

Researchers must describe their proposed research to the IRB in enough detail that the potential adverse effects and benefits to human subjects can be evaluated. The IRB forms and procedures provide a means for researchers, subjects, the University, and community to communicate clearly and responsibly about the risks and benefits of research involving human subjects and informants. Copies of all IRB forms and corresponding documentation will be stored by the Office of Research and Sponsored Programs and will be available to the IRB Chair, the Assistant Vice President and Dean of Graduate Studies, the Provost and Vice President for Academic Affairs, relevant federal agencies, and others approved by the Provost and Vice President for Academic Affairs.

Three principles guide the review process:

- Subjects must give their informed consent to participate in research;
- Researchers must provide and protect subject confidentiality;
- Potential risks to subjects must be balanced by potential benefits of the research.

The review process uses the concept of minimal risk to decide the extent to which subject interests warrant formal and extensive review of research proposals. Minimum risk is defined as "the risks anticipated in the proposed activity, are not greater than those ordinarily encountered in daily life or during performance of routine physical or psychological tests." Risks to subjects are minimized (1) by using procedures which are consistent with sound research design and which do not unnecessarily expose the subjects to risk, and (2) whenever appropriate, using procedures already being performed on subjects for diagnostic purposes.

The IRB classifies research into three categories based on the need to ensure that research conforms to the above principles. These categories are Full Review, Expedited Review, and Request for Exemption from Review. These review categories are discussed in detail in the Guidelines for Human Subject Research.

Basic features of each category are:

Full Review - A Full Review occurs when the IRB reviews the proposed research and meets with the principal investigators to discuss and evaluate the impact on human subjects. After review IRB members vote to approve or disapprove the proposal. Full Reviews are conducted for proposed research that involves more than minimal risk or where very careful evaluation or risks and benefits is appropriate, minors or vulnerable populations are subjects, or where adverse impact on subjects may occur due to research activities. For example, research exposing subjects to threats to dignity, physical or emotional injury or discomfort, legal liability or arrest, damage to financial or social standing, or procedures in which subjects experience stress or have their behavior, attitudes or beliefs manipulated by researchers must undergo Full Review. Approval is by majority vote in all cases.

Expedited Review - Expedited Review occurs when at least two members of the IRB, designated by the chairperson, review the proposal and independently indicate their approval or disapproval. Researchers are not required to meet with reviewers. Reviewers frequently give written comments advising the researcher on ways to enhance the protection of human subjects. Reviewers may ask for more information or require changes in procedures to enhance the provisions for informed consent, confidentiality and risk/benefit balance. Expedited research involves minimal risk to subjects but involves procedures with potential impact on subjects; such as the collection of body samples or physiological data, video or voice recordings, or studies involving vulnerable populations or sensitive issues.

Exemption from Review - A Request for Exemption from Review may be received by the IRB Researchers must complete and submit the same forms and documents required for the other review categories. These forms provide reviewers with the information needed to evaluate whether the research qualifies for exemption from review. Exempted research involves research on effectiveness of or the comparison among instructional techniques, curricula, or management methods, the use of educational tests, or the study of existing data.

Student Research - Student research activities are governed by both the requirements of good research and the regulations of the Bloomsburg IRB. Student research is any systematic data collection and recording process done by students that is subject to interpretation and dissemination to solve a problem or advance understanding of a discipline. Dissemination occurs whenever information goes beyond registered students or assigned faculty or supervisors for the course. Examples of student research include the collection of data for a thesis, honors paper, or departmental paper or data collected for publication, distribution, presentation, or that is publicly available beyond the course environment. It is

the responsibility of faculty members overseeing student research activities to ensure that the students meet the professional standards of the discipline and also conform to Policy 3990 and IRB procedures.

Procedures for Appeal

In the event a proposal is not approved at the exempt or expedited level, the researcher may request a full review of the protocol by the IRB.

Procedures for noncompliance - Investigators are admonished to remember that the university policy entrusts the investigator with the primary responsibility for protection of individual subjects. It is the individual investigator's responsibility to be in compliance with this policy. The IRB is the only body authorized to take action when a researcher is in noncompliance with PRP #3990. Noncompliance includes:

failure to submit applicable research involving human subjects for review and approval to the IRB;

failure to conduct research according to the approved protocol as it relates to the protection of human subjects;

failure to immediately notify the IRB when research activity results in an unexpected adverse impact on the subjects.

Allegations of noncompliance (either written or oral) should be directed to the chair of the IRB. The IRB will investigate allegations of noncompliance, maintaining confidentiality in all matters. Only voting members will participate in the investigation. In the event that allegations are substantiated, the IRB will terminate approval of the research and recommend to the Assistant Vice President for Graduate Studies and Research that the research be terminated. These decisions will be communicated to the researcher and the appropriate federal agency or funding agency, if appropriate, by the Assistant Vice President of Graduate Studies and Research. A decision to terminate research may be appealed to the IRB within 15 days of notification.

Source: http://intranet.bloomu.edu/policies_procedures/3990