 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff</p>	<p><i>Policy Title:</i> Encryption of Restricted Data</p> <p>Effective Date: 01/04/2008</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: HIPAA, FERPA, GLB, PCI</p>	<p><i>Policy Number:</i> 9.1.1</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p>
---	---	--

Background

The University of Cincinnati (UC) must protect restricted data (see Appendix A) on its personal computers (PCs) and removable media (USB or thumb drives). After researching the issue, the university determined the best way to protect data is using full disk encryption to secure UC-owned PCs and removable media (see appendix B for architecture and pricing information). Best practices surrounding this type of activity can be found in International Standards Organization (ISO) 17799:27001, ISACA's (IT Audit) Control Objectives for IT (COBIT, and ISO 20000 documentation.

Policy

- All UC-owned PCs that contain restricted data must be secured with full disk encryption.
- UC employees are prohibited from storing restricted data on a PC or server not owned by the university and the university will not represent them should a breach occur.
- Removable media containing restricted data should be encrypted using PGP and must be stored in a secure, locked location. The university strongly discourages storing restricted data on removable media.
- UC will support only PGP encryption for PCs and external storage devices.
- The Office of Information Technologies (UCit) will manage encryption keys and UC Information Security can access the keys if the need should arise.
- UC Information Security has the right to access an encrypted device if necessary for the purpose of investigation or in the absence of the employee who was using the encrypted file system
- If a department or individual has a business need to ignore this policy they need to clearly document and communicate this need via the Risk Acceptance Process (Appendix C).

Audience:

This policy applies to all organizations and individuals associated with UC using a PC or external storage device to maintain restricted data.

Definitions:

- **Risk Acceptance:** When there is business need to not follow a policy or to not remove a risk (too costly, not technically possible, etc.) there has to be a process in place that communicates to management that a residual risk remains. Risk acceptance is the process by which management can approve the risk associated with an action that is not following policy or that is not removing a specific risk.
- **IUC:** Inter-University Council of Ohio
- **PC:** Includes UC-owned desktops, laptops, smartphones, and any other personal device containing data.
- **Removable Media:** Includes CD ROMs, floppy disks, backup tapes, hard drives, memory cards, and USB memory drives
- **Data Classification:** Not all information is equal and so not all information requires the same degree of protection. This requires the data owner to assign information a label that identifies whether or not it requires protection.

Procedure:

HIPAA	Health Insurance Portability and Accountability Act
FERPA	The Family Educational Rights and Privacy Act
GLB	Gramm-Leach-Bliley Act
PCI	Payment Card Industry Standards

Related links:

- [Health Insurance Portability and Accountability Act](#)
- [The Family Educational Rights and Privacy Act](#)
- [Gramm-Leach-Bliley Act](#)
- [Payment Card Industry Standards](#)

Phone Contacts:

UC Information Security	8-ISEC
Director, Information Security	6-9177
UC Office of the CIO	6-2228
UC FERPA Officer	6-9930

Disciplinary Actions:

Violation of this policy may result in revocation of network access for the effected system(s). Violation of this policy may also result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants and dismissal for interns and volunteers. Additionally, individuals are subject to loss of University of Cincinnati Information Resources, access privileges, civil, and in some cases criminal prosecution.

Appendix A (this list is not all inclusive - just an example and guideline)

	UC Restricted Data (highest, most sensitive)	UC Sensitive Data (moderate level of sensitivity)	UC Public Data (low level of sensitivity)
Legal Requirements	Protection of data is required by law (e.g., HIPAA, GLB FERPA, PCI)	UC has a contractual obligation to protect the data	Data that is readily available to the public. This data requires no confidentiality or integrity protection.
Reputation Risk	High	Medium	Low
Other Institutional Risks	Information which provides physical or logical access to restricted data.	Smaller subsets of protected data from a school or department	General university information
Access	Only those individuals designated with approved access and signed non-disclosure agreements.	UC employees and non-employees who have a business need to know.	UC affiliates and general public
Examples	<ul style="list-style-type: none"> ▪ Medical ▪ Students ▪ Prospective students ▪ Personnel ▪ Donor or prospect ▪ Financial ▪ Contracts ▪ Physical plant detail ▪ Credit card numbers ▪ Hazardous chemical location and inventory ▪ Certain management information 	<ul style="list-style-type: none"> ▪ Information resources with access to restricted data ▪ Research detail or results that are not restricted data ▪ Library transactions (e.g., catalog, circulation, acquisitions) ▪ Financial transactions which do not include restricted data (e.g., telephone billing) ▪ Information covered by non-disclosure agreements ▪ Very limited subsets of restricted data 	<ul style="list-style-type: none"> ▪ Campus maps ▪ Personal public data (e.g., contact information) ▪ Name and work phone number

**Specific
Examples of
Restricted
Data**

HIPAA - Protected Health Information

- Patient Names
- Street address, city, county, zip code
- Dates (except year) for dates related to an individual
- E-mail, URLs, & IP #'s
- Social security numbers
- Account/Medical record #'s
- Health plan beneficiary numbers
- Certificate/license #'s
- Vehicle id's & serial #'s
- Device id's & serial #'s
- Biometric identifiers
- Full face images
- Any other unique identifying number, characteristic, or code
- Payment Guarantor's information
- For more information, see the HIPAA web page.

FERPA - Student Records

- Grades – both final and in progress
- Student Financial Services (formerly Bursar's office) information
- Credit Card Numbers
- Bank Account Numbers
- Wire Transfer information
- Payment History
- Financial Aid / Grant information
- Student Tuition Bills

Note that the following data may ordinarily be revealed by the University without student consent unless the student designates otherwise.

- Name
- Date of birth
- Place of birth
- Directory address and phone number
- Electronic mail address
- Mailing address
- Campus office address (for graduate students)
- Secondary mailing or permanent address
- Residence assignment and room or apartment number
- Specific quarters or semesters of registration at Stanford
- UC degree(s) awarded and date(s)
- Major(s), minor(s), and field(s)
- University degree honors
- Institution attended immediately prior to UC

- ID card photographs for University classroom use

Donor Information

- Name
- Credit Card Numbers
- Bank Account Numbers
- Social Security Numbers
- Amount/what donated
- Telephone/Fax #s
- Employment information
- Family information (spouse(s) / children / grandchildren)
- Medical History (alumni/family who have major medical procedures performed at University Hospital)

Faculty/Staff Housing

- Name / Spouse
- Credit rating / history
- Financial worth
- Income levels and sources, etc.

Research Information

- Human subject information
- Lab animal care information

General Information

- Anything / Everything in the Office of the General Counsel

Employee Information

- Social Security Number
- Name
- Date of birth
- Home address or personal contact information
- Benefits information
- Performance reviews
- Worker's compensation or disability claims

Business data

- Credit card numbers
- Bank account information
- Purchasing card (P-card) numbers
- Social Security or other Taxpayer ID numbers
- Contract information (between UC and third parties)

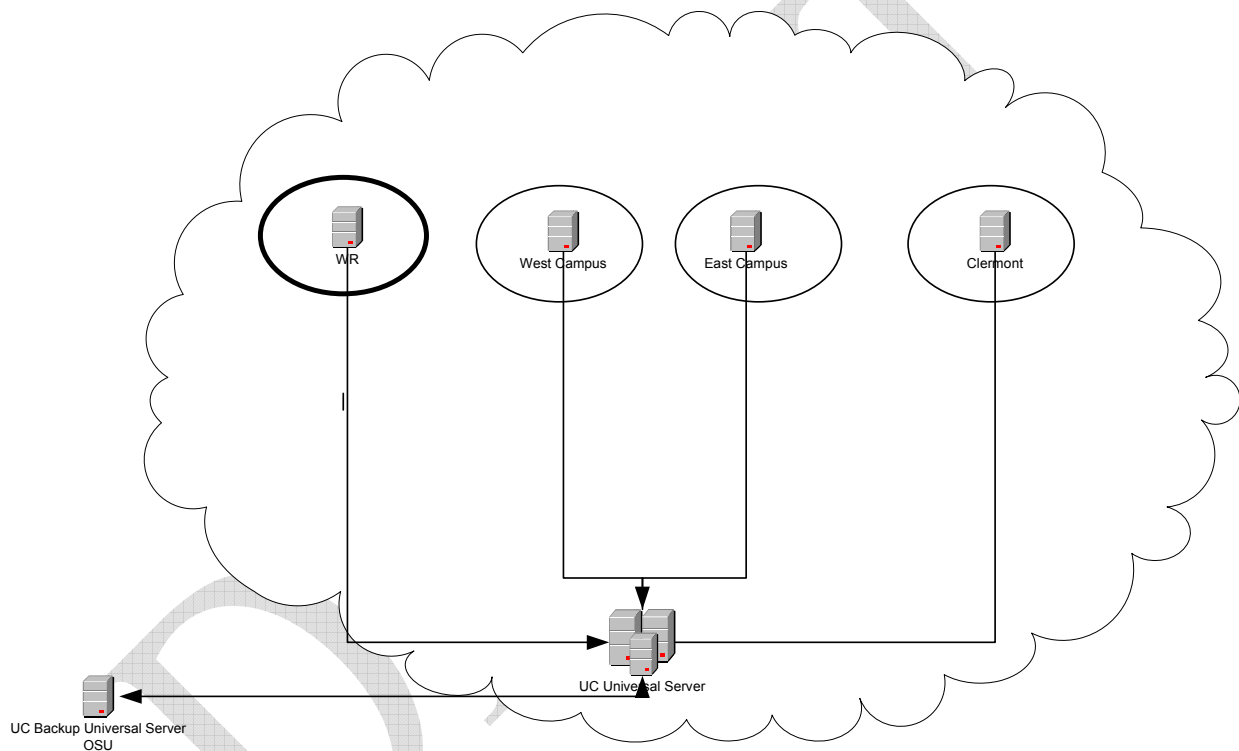
Management data

- Faculty evaluations

Appendix B

Summary:

UC will use PGP Universal Server for key management. UC is working with Ohio State University on having a fail over Universal Server at OSU and OSU will be using the UC Universal Server as their fail over in a reciprocal agreement. The department or college IT contact will download the PGP Desktop encryption software and install it on machines that have a business need for storage of sensitive data.



The annual cost of the UC Full Disk Encryption and Key Management Service is projected at \$12.00 per device. This cost could be as low as \$7.00 per device once UC purchases bulk licenses (50,000) from the vendor. UC will purchase 2,000 licenses for the initial pilot deployment.

Appendix C

Background	<p>It is understood that it is not possible to eliminate all business work from an organization. However, for the University of Cincinnati, there exists a legal duty to mitigate risk to a level that is prudent or that would be acceptable to a “reasonable person”.</p> <p>It is therefore the general policy of UC that all organizations are required to take steps to reduce risk to a level established as best practice.</p> <p>Where an organization elects not to institute a control or process to reduce the risk any further and they feel that there is still a question as to whether the risk they are going to leave in place is reasonable the associated risk or vulnerability left unaddressed must be clearly communicated and accepted by UC Senior management or their designate.</p>
Purpose	<p>The purpose this process is to:</p> <ol style="list-style-type: none">1. Communicate that the University of Cincinnati understands that there may exist business reasons to accept a level of risk in the course of doing business.2. To provide a method whereby an organization can clearly communicate that a risk exists; to clearly communicate the business need for having such a risk and the potential impact of the remaining risk. As well as to provide a mechanism whereby such risks are explicitly approved by management.3. To provide a method by which the required Risk Communication and Risk Acceptance forms can be obtained.
Definitions	<p>Prudent: Wise in handling practical matters; exercising good judgment or common sense</p> <p>Best Practice: A concept which asserts that there is a technique, method, process, or activity that is more effective at delivering a particular outcome than any other. Descriptions of best practices are normally available from a certifying or regulating authority for an industry.</p> <p>Risk: A concept that denotes a potential negative impact or something that increases the probability of a loss.</p> <p>Risk mitigation: Actions taken to reduce the probability that the loss represented by the risk will occur. Mitigation recognizes that the purpose of an organization is to deliver services and goods to their respective customers to meet business goals. It provides for cost/benefit analysis of a mitigating action prior to implementation.</p>

Risk Acceptance Process

- All organizations within the University of Cincinnati are required to follow the best practices for their industry with respect to the mitigation of risk except where there exists a strong business reason to exempt an organization from a particular recommendation or practice.
- Any Risk Exception for ignoring the full disk encryption policy must be documented and approved by senior management. Sensitive data must be protected and if full disk encryption is not being used other steps must be put in place that mitigates the risk of data loss. These mitigation steps must be communicated to UC Management and the risk process is the appropriate vehicle for this communication.
- The approval will be granted or denied via the completion of the Risk Acceptance Form (RAF).
- The RAF must be initially signed by a UC Manager and then forwarded to the Director of Information Security for review and approval/denial or escalation to more senior management.
- UC Information Security is responsible for the maintenance of the official and approved/denied Risk Acceptance Form. The form and training on the risk acceptance process may be obtained from UC Information Security by sending an email to InfoSec@uc.edu or by visiting the InfoSec web site at www.uc.edu/infosec . For audit purposes an unofficial copy of the form may be kept in the files of the department requesting the exception.

InfoSec Risk Acceptance Process

