Title:	Portable Computing Device Security - Laptop Standard	**Related Documents:**	HIPAA Core Standard: Use of Portable Devices
Version:	1		Acceptable Use Policy
Approved:	August 10, 2009		Data Protection and Security Policy
Effective:	August 10, 2009		UAB IT Security Practices

Purpose: The purpose of this standard is to outline the supported portable computing device security configurations for laptop computers at UAB.

Scope: All laptops that are purchased by or for UAB personnel by any funding source are subject to this standard. Regardless of device ownership, laptops that are approved to be used for UAB business must follow these standards.[1]

Standards:

1) **Password protection:** Any computing device that accesses UAB information or systems must require user authentication upon startup and after inactivity.[2]

2) **Storage of sensitive information:** Sensitive information should be stored on a secure server and only accessed from portable devices in accordance with the "Data Protection and Security Policy."[3] Laptops used to store sensitive information will be subject to all requirements set forth in the Data Protection and Security Policy.[4]

3) **Encryption of laptop computers used for UAB Business:** All laptop computers used for UAB business must be encrypted to protect data from unauthorized disclosure.[5]

   Note: Laptops that cannot be encrypted due to incompatibility or obsolescence may not be used for UAB business.

4) **Physical security:** Appropriate physical security measures should be taken to prevent theft of laptops and media.

5) **Lost or stolen devices:** Theft of laptops must be reported immediately to UAB Information Security and UAB Police.

---

[1] See "UAB Business" under Definitions.
[2] See "What are the guidelines for creating a strong password?" at http://main.uab.edu/Sites/it/faqs/49118/.
[3] See "Data Protection and Security Policy" at http://www.uab.edu/it/policies/ElectronicDataDtab.pdf.
[4] See "Sensitive Information" under Definitions.
[5] See "Approved Encryption Methods" at http://main.uab.edu/Sites/it/internal/all/information-security/pgp/ for more information.

6) **Disposal and Reuse:** If a laptop is used for UAB business, when it is retired or reconditioned the data must be destroyed using appropriate overwriting or destruction procedures.[6]

7) **Antivirus:** Laptop computers must use a functioning and up-to-date antivirus program.

Exceptions: Exceptions must be documented and approved by departmental IT representatives as well as by the Dean or Vice President and filed with UAB Information Security. Exceptions should be based on situations where laptops are required and additional controls exist to mitigate the risk of stolen devices.[7]

This standard does not apply to UAB students unless their laptop is used for UAB Business. Departments with students using and handling sensitive data are responsible for identifying and addressing the risks involved in compliance with UAB policy.[8]

Examples of exceptions include:

1) Laptops used in student computer labs or in training initiatives that are automatically wiped of data upon logout and boot.
2) Laptops used for real time imaging like photo albums with real time clock synchronization with an FMRI machine and no UAB sensitive data is stored or accessed.
3) Laptops used in the development of operating system level functionality where no sensitive data is stored.

Procedures: Each department is responsible for developing procedures to comply with these standards.

Departmental Responsibilities:

1) Maintain inventory of all laptops, including personally owned laptops that are approved for UAB business. This inventory should include the following minimal information:
    a. Serial number
    b. Model number
    c. Operating System
    d. Ethernet and wireless MAC (physical) addresses
    e. Owner or assignee
    f. Encryption status
    g. Type of data stored on device (Indicate whether it is used to access/store sensitive information)

[6] See "Secure Media Destruction" at http://main.uab.edu/Sites/it/faqs/57722/ and "Drive Wiping Procedures" at http://main.uab.edu/Sites/it/faqs/49185/.
[7] See "Exception Requests" under Appendix A.
[8] See "UAB Business" under Definitions.

h. Appropriate disposal and reuse documentation

2) Configure all laptop computers to:
   a. Use an approved encryption solution
   b. Use a strong logon password
   c. Use a screensaver password with automatic timeouts after 15 minutes of inactivity.
   d. Use antivirus software with up-to-date definitions.

Definitions:

1) **Encryption:** The use of software to apply an algorithm to data rendering it unrecoverable without authentication.

2) **Laptop:** a type of Portable Computing Device (PCD).

3) **Portable Computing Device (PCD):** includes but is not limited to laptop computers.

4) **UAB Business:** as it relates to laptops, includes devices used by all Faculty, Staff, and Students that access/store information covered by the "Information Disclosure and Confidentiality Policy."[9] Student-owned systems storing only personal academic information are not covered by this standard but may be required to encrypt based on academic activities involving specific UAB data in a patient care or research setting.

5) **Sensitive Information (i.e. "sensitive data"):** UAB's Data Protection and Security Policy defines sensitive data, which includes, but is not limited to:
   a. Individually identifiable information (Example: name and date of birth – see "Information Disclosure and Confidentiality Policy")
   b. Social Security numbers
   c. Credit card numbers
   d. Driver's license numbers
   e. Proprietary research data
   f. Privileged legal information
   g. Data protected by law such as student and patient records

Revision History

Revision	Approval	Remarks	Approval Date	Effective Date

[9] See "Information Disclosure and Confidentiality Policy" at http://www.fab.uab.edu/IT%20Policies%5CInfoItab.pdf.

1	Approved by Sheila Sanders	Initial Portable Computing Devices Standard addressing laptop device encryption	August 10, 2009	August 10, 2009

Appendix A: EXCEPTION REQUEST FORM

Contact information for user requesting exception (i.e. user responsible for the machine involved):			
Name:		BlazerID:	
Phone:		Email:	
Date:		Department:	

Inventory information for the computer that this exception is being requested for:					
Serial #:		Model #:		Operating System:	
Wireless MAC address:		Ethernet MAC address:			

Process for Exception Requests:

1. Fill out the form and submit it your IT support and Dean or Vice President for approval.
2. Send an email to askit@uab.edu with the completed form attached.
3. You will receive an automatically generated email from askit@uab.edu with the ticket number associated with this request.
4. This ticket will be assigned to UAB Information Security for processing and a follow-up email will be generated automatically. If additional information is needed, you will be contacted by Information Security.
5. Upon completion of processing by Information Security, you will receive a final email from askit@uab.edu indicating the status of this request.

1. Why is an exception being requested?

2. What are the risks associated with this exception request (include the type of data stored on the computer)?

3. What mitigation steps are being taken to safeguard University data should the request be approved?

Requestor Signature:		Date Signed:	
Department Technical Approval:		Date Signed:	
Dean or Vice President Approval:		Date Signed:	

. **Appendix B:** For the purpose of this standard, examples of UAB Business include but are not limited to the use of laptops to:

1) Connect to the UAB network if configured to access secured network drives.
2) Accessing any system at UAB where you have more than "self-service" privileges. Examples of systems include:
    a. Oracle HR/Finance
    b. Banner Student System
    c. Optidoc/WEBIT
    d. Budget Model System
    e. Xtender
    f. Sunflower
    g. UAB Report Viewer
    h. BlazerNET
    i. Blackboard Vista
    j. Health Information Systems
3) Contribute to or correspond regarding research projects that UAB participates in or sponsors (by Principal Investigator or members of research team).
4) Store UAB Employee email via an email client (e.g. Outlook, Entourage, Eudora, etc.).