University of Alabama at Birmingham

MINIMUM SECURITY FOR COMPUTING DEVICES RULE

June 2017 (Target)

Related Policies, Procedures, and Resources

UAB Acceptable Use Policy, UAB Protection and Security Policy, UAB Data Classification Rule, UAB Data Protection Rule, Vulnerability Management Rule

1.0 Overview

The UAB Acceptable Use Policy outlines acceptable use of computing and network resources at UAB. The Policy states that computing devices must meet specific technical and security standards before connection to the University network and that computing devices must meet specific protection requirements before storing or transmitting sensitive or restricted data.

2.0 Objective / Purpose

This document outlines the minimum security standards that are required for all computing devices owned by UAB and/or connected to the UAB network, along with all devices that store or transmit Restricted or Sensitive data, as defined by the UAB Data Classification Rule. This document also governs all enforcement procedures and exception requests tied to the Minimum Security for Computing Devices Rule. The purpose of these requirements is to reduce the risk to the security of individual systems and data while mitigating risks to the operation of the UAB network.

3.0 Security Standards Rule

UAB Information Security is adopting the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Security as the basis for the university-wide set of security standards and guidelines.

4.0 Minimum Security for All Computing Devices

4.1 Physical security — Computing devices shall be protected from unauthorized physical access and theft.

4.2 Operating Systems - Current, vendor-supported operating systems are required for all computing devices.

4.3 Patching and updates- All computing devices shall have patches and updates applied on a consistent and regular schedule. Computing devices shall have all applicable security updates installed as soon as practicable, or as defined within the UAB Vulnerability Management Rule.

4.4 Anti-malware software - Anti-malware software shall be used and kept up-to-date on devices where the use of such software is practical.

4.5 Software firewall - Firewall software shall be used and kept up-to-date on devices that have firewall software capabilities.

4.6 Access control— Devices shall require sign-on or login for users. Users shall be authenticated by means of unique ID and passwords/passphrases or by other authentication processes (e.g. biometrics or smart cards). In general, only encrypted authentication mechanisms or protocols shall be used. When passwords/passphrases are used, their construction and management shall comply with the UAB Password / Passphrase Standard.

4.7 Un-authenticated email relays and proxy services - Devices shall not operate as an unauthenticated email relay or proxy service.

4.8 Unnecessary services, protocols and ports – Services, protocols, and ports that are not necessary for the device to perform its function or mission shall be uninstalled.

5.0 Minimum Security for Computing Devices that store or transmit Restricted/PHI and/or Sensitive data

Responsibility for the security of a device covered by this rule and its data shall be assigned to the individual who is designated as its primary user or owner.

The storage of Restricted/PHI data must be approved by the VPIT.

5.1 Servers

In addition to the requirements outlined above in section 4.0 for all computing devices, all server-class devices that store or process Restricted/PHI and Sensitive data shall meet the following minimum security requirements:

5.1.1 Physical security — Server-class devices shall be placed within a protected and monitored area with a secure perimeter (e.g. walls, lockable doors, lockable server racks and windows) that protects the system from unauthorized physical access.

5.1.2 Limit network access — Network access to Restricted and Sensitive systems shall be limited to the least access necessary for the device to perform its function/mission.

5.1.3 Access control — User accounts and users shall have a unique identifier (user ID/login name) that is assigned for their personal use only and not shared. Privileges shall be restricted and controlled in accordance with the principle of least privilege to reduce opportunities for unauthorized access or misuse of the system.

Access and privileges shall be authorized by an appropriate authority and reviewed at regular intervals.

5.1.4 Secure login and authentication — Access shall be controlled with secure/encrypted log-on procedures. Use CAS or other Ticket based Authentication solution (SAML). Systems should avoid processing and handling of BlazerID passwords.

5.1.5 Protection against brute-force login attacks — Controls shall be put in place to limit failed login attempts. (Back off algorithms)

5.1.6 Session controls — Controls shall be put in place to ensure that inactive sessions shall expire after a defined period of inactivity.

5.1.7 Logging, monitoring and review — System administrator, user activities and system events shall be logged, forwarded to the Enterprise SIEM, and reviewed daily. Logs shall be retained for a period of at least one year or a period deemed practicable by the University department/unit responsible for the security of the device.

5.1.8 Identification and management of vulnerabilities — Devices shall be hardened prior to implementation. Security updates shall be applied and unnecessary services uninstalled in order to minimize potential technical vulnerabilities.

Vulnerabilities shall be identified and evaluated using a routine process, and appropriate measures shall be taken to remediate significant vulnerabilities.

5.1.9 Change management — A formal process shall be adopted to review, approve, and test configuration changes before the changes are implemented to ensure that the changes do not adversely impact the operation or security of the device.

5.1.10 Encrypted transmission of data — Encrypted protocols or secure channels shall be used to transmit Restricted and Sensitive data to and from the device. A UAB-approved VPN shall be used to access to UAB resources from outside the UAB network.

5.1.11 Data containment – Controls need to be implemented that govern and prevent unauthorized transmission of Restricted/PHI data from systems that are authorized to process Restricted/PHI data.

5.1.12 Remove Restricted and Sensitive data when no longer needed — A process shall be adopted to regularly review archived files and delete files containing Restricted or Sensitive data when the files are no longer needed.

*** Avoid storing Restricted or Sensitive data unnecessarily. ***

5.1.13 Administrator restrictions - Server administrators are required to use standard, least-privileged accounts and only will elevate to administrative privileges when necessary to perform a specific job task. Web surfing from a server to the Internet by administrators is prohibited, and email clients will not be installed on a server-class device.

5.2 Desktops

In addition to the requirements outlined above in section 4.0 for all computing devices, all desktop-class devices that process Restricted or Sensitive data shall meet the following minimum security requirements:

5.2.1 Physical security — Desktop devices shall be placed in reasonably secure areas, such as lockable offices, and not in publicly assessable areas.

5.2.2 Auto-lock screens — Desktop devices shall be configured to automatically lock and require a logon after being unattended or inactive for a predefined period of time.

5.2.3 Least privilege for user accounts — User accounts shall be configured with the least privileges necessary for the users to perform their job/role.

5.2.4 Protection from drive-by malware — Reasonable methods shall be used to prevent or disable web-browsing capabilities on devices that store or process Restricted or Sensitive data. In cases where it is not possible to disable or prevent web browsing, alternative methods — such as application-layer firewalls, proxy servers and web content filters, or application safe-listing — shall be implemented to protect against drive-by attacks and malware.

5.2.5 Remove Restricted and Sensitive data when no longer needed — Devices shall be configured to automatically delete temporary files, temporary Internet files, clear web browser caches, etc.

A process shall be adopted to regularly review archived files and delete files containing Restricted or Sensitive data when the files are no longer needed.

Restricted data shall not be stored on desktop-class devices.

5.2.6 Encrypt Sensitive data — Sensitive data stored on the device shall be stored in encrypted files or within encrypted volumes.

5.3 Laptops, tablets, and mobile devices

In addition to the requirements outlined above in section 4.0 for all computing devices, all laptop and mobile-class devices that store or process restricted/PHI and/or sensitive data shall meet the following minimum security requirements:

5.3.1 Auto-lock — Devices shall be configured to automatically lock and require a logon, pin, or other means of authentication after being unattended or inactive for a predefined period of time.

5.3.2 Protection from theft — Whenever possible, the device should be protected from theft by storing the device in a secure location, anchoring with a security cable, etc.

Tracking/location software shall be installed or enabled on the device, if practicable.

5.3.3 Least privilege for user accounts — User accounts shall be configured with the least privileges necessary for the users to perform their job/role.

5.3.4 Encryption of laptop computers used for UAB Business - All laptop computers used for UAB business must be encrypted to protect data from unauthorized disclosure.

5.4 International Travel and Export Control

All laptop and mobile-class devices used for International travel shall meet the minimum security requirements in sections 4.0 Minimum Security for All Computing Devices and 5.3 Laptops, tablets, and mobile devices for International travel with Sensitive data. International travel with Restricted/PHI data requires the submission and approval of an Information Security Exception Request form. Please refer to the Data Protection Rule and the International Travel Guidelines <need link to guidelines> for more information.

6.0 Enforcement and Implementation

6.1 Roles and Responsibilities

Each University academic and business unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this standard security rule.

The VP of Information Technology Office is responsible for enforcing this standard security rule.

6.2 Consequences and Sanctions

Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other University policies, including progressive discipline up to and including termination of employment. In the cases where students are involved, such issues will result in the reporting of a Student Code of Conduct violation.

Any device that does not meet the minimum security requirements outlined in this standard may be removed from the UAB network, disabled, etc., as appropriate until the device can comply with this standard.

7.0 Exceptions

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request a security exception, contact the Enterprise Information Security Office at datasecurity@uab.edu.