



**THE UNIVERSITY OF
ALABAMA AT BIRMINGHAM**

Data Security Best Practices

Release 1.0



Reviewed: September 2008



Data Security Best Practices

1. Overview

The following hardening checklist should be followed by all server administrators to aid in securing UAB's data assets. The checklist should be used for test as well as production systems. This should be considered an augmentation to the performance of risk assessments and adherence to UAB policy.

Checklist

1.1 Document Security

- Ensure that authentication is required to access sensitive information. Do not rely on obscure document locations to prevent access (e.g. Do not place sensitive.doc on <http://example.uab.edu/SECRETDOCUMENTS>)
- Limit the use of private identifiers such as Social Security Numbers as much as possible. Such use requires the proper executive approval.
- Ensure that information being made available publicly conforms to UAB's HIPAA and Student Record policies. References are provided at the end of this document.

1.2 Passwords and Accounts

- Change all default account passwords. Remove or disable the account (e.g. Guest and or vendor accounts).
- Do not use system names as account names.
- Provide unique accounts per system administrator (e.g. Use the sudo tool rather than passing out the root account to every system administrator)
- Pick strong passwords/passphrases for users no less than 8 characters in length. For system administrators, pick passphrases no less than 15 characters in length where supported by the operating system.
- Make sure that users do not use passwords assigned by helpdesk staff. Ensure that the users change their passwords if they get reset to a default.
- Provide unique accounts per user rather than having a single group login.
- Grant the least amount of privileges to a user possible. Always consider a user's need to know when establishing accounts and assigning privileges.
- Create and follow procedures for granting and removing access to resources to user and third parties. Ensure that the procedures provide management visibility.
- Review access permissions periodically for correctness (e.g. removing transfers, retirees)



University of Alabama at Birmingham Office of Information Technology

1.3 Logs

- Log successful and failed logon attempts.
- Ensure that application logging is sufficient to diagnose problems. Often, this requires increasing the log detail level (e.g. IIS) or log sizes.
- Review logs on a regular basis for suspicious activity.
- Replicate logs to another system if possible. This helps track down what happened to a system in case of intrusion or other disaster.

1.4 Recovery

- Document backup and recovery plans and test them modifying the plan accordingly.
- Store backups in a secure off-site location on a daily basis. *This does not mean the home or car of a system administrator.*
- Store a copy of the recovery plan and backup software in the off-site location.
- Ensure that replacements can be purchased for systems and backup hardware.
- If the system is critical to service, make sure that downtime procedures exist.
- Make sure that there are administrator access procedures in case the system administrator is unavailable (i.e. passphrases kept in safe with Director-level access).

1.5 Anti-Virus

- Use antivirus software to scan software prior to installation for systems commonly affected by viruses.
- Use antivirus and anti-spyware software on client systems for systems commonly affected by viruses.
- Ensure virus updates are performed daily, if applicable.

Resource: UAB IT provides **anti-virus and anti-spyware software** for all faculty, staff, and students.

1.6 Updates

- Test updates before applying to production systems where possible.
- Adopt change control procedures for critical systems including altering hardware and software configuration, emergency security updates, and user notification. Maintain a log of applied changes.
- Ensure that patches are applied in a timely manner.



University of Alabama at Birmingham Office of Information Technology

- Keep all application and operating systems at the levels currently supported by vendors.
 - If an application or operating system is no longer supported (e.g. NT4), replace it! Watch out for end of life dates (e.g. <http://support.microsoft.com/?pr=lifecycle>) and include them in your budget planning processes.

Resource: UAB IT provides a Windows patch management server (WSUS) and tests patches prior to approving them for distribution.

- Enable only those services required to provide the business function of the system and disable all other services.
- Deploy packet filtering to provide services to only legitimate users (e.g. be sure that backup and administration is not exposed to the entire Internet; use a firewall to block everything but TCP port 80 and appropriate ICMP).
- Use encryption for client-server communication whenever practical.
- Document the exposed TCP/IP ports on a system and monitor for unexpected changes (e.g. using fport.exe).
- Restrict communications to only specific IPs when possible (e.g. A backup client should only be listening to your backup server and not the entire Internet).

1.7 Physical Security

- Maintain servers and network hardware in secured areas and prevent unauthorized access.
- Ensure power availability for critical systems either by appropriate emergency power and/or uninterruptible power supply.
- Keep server areas free of dust and protected from water damage.
- Locate fire extinguishers near the server area. Contact Campus Maintenance or Hospital Maintenance at <http://www.fab.uab.edu> to request an assessment of fire prevention controls at your location.

1.8 Device Security

- Store sensitive data on only properly secured servers whenever possible.
- Do not store sensitive data on devices such as smart phones.
- Use device encryption for protecting notebook computers or USB devices.
 - <http://www.uab.edu/it/software/PGP> for Windows-based notebooks.
 - Use Apple's FileVault for protecting OS X-based notebooks.
- Keep server areas free of dust and protected from water damage.



University of Alabama at Birmingham Office of Information Technology

- Locate fire extinguishers near the server area. Contact Campus Maintenance or Hospital Maintenance at <http://www.fab.uab.edu> to request an assessment of fire prevention controls at your location.

2. Additional Resources

2.1 UAB Policies and Standards

- <http://www.uab.edu/it/policies> - Links to many UAB policies including the *Acceptable Use Policy, Data Protection and Security Policy and World Wide Web Pages Policy*
- <http://www.hipaa.uab.edu> - Links to UAB HIPAA-standards for security. This site can only be read on campus.

Security Code Standards

1. Contingency Planning Standard
 2. Information System Account Management Standard
 3. Information Systems & Network Access Standard
 4. Internet and Email Use Standard
 5. Media Reallocation and Disposal Standard
 6. Risk Analysis and Management of EPHI Standard
 7. Security Incident Response Standard
- <http://students.uab.edu/academics/show.asp?durki=16434> – *Student Records Policy* detailing what information regarding a student can be released without their permission.

2.2 IT Data Security

The IT Data Security office can offer security advice regarding deployments. IT Data Security also provides assistance in the event of a security incident. If you require assistance, please contact 5-0842.

2.3 TIMGroup

The TIMGroup mailing list is a useful forum for discussing server hardening. This mailing list has system representatives from multiple areas of campus. The website is at <http://lists.it.uab.edu/timgroup>

2.4 Other Useful Sites



University of Alabama at Birmingham Office of Information Technology

Multiple groups provide security checklists. They often provide more detail regarding a specific vendor's product. Use these vendor's checklists for help in developing one appropriate for your area.

- <http://www.cisecurity.org/>
 - <http://www.nsa.gov/snac/>
 - <http://www.sans.org/score/>
 - <http://www.microsoft.com/technet/security/topics/ServerSecurity.msp>
- x