IT Security Policy for LSA

LSA.Security

LSA Information Technology
Tuesday, April 6, 2011

This paper outlines the information technology (IT) Security requirements for the College of LSA's cyber infrastructure - this includes the College's computers, networks and data. Updates to this policy have been added in this version to address the findings from the University Audit's 2010 review of research computing in the College of LSA.

The College of Literature, Science and Arts strives to provide an atmosphere that encourages research and instruction. Achieving a balance between ease of use of information technology (IT) systems and appropriate security mechanisms is a delicate balancing act. IT security measures should simply work while providing a reasonable level of risk management. We have focused this document on minimizing the impacts of needed security on day-to-day IT activity in the College. This document is written such that it can allow for some flexibility in security control implementation by allowing various methods of mitigation. It is also written so that where more stringent security requirements are necessary; they can more easily be devised and implemented.

Help and guidance can be found in this document in the form of contact info, a security policy template and web links. Methods are provided for reasonable exception for those systems in the College that cannot meet the security requirements (as required) while addressing the threats they face. As the security mission statement indicates, aligning our objectives with the business objectives of the LSA faculty, staff and students is essential. This document will be regularly reviewed and updated as new technologies become available to the LSA community in LSA cyber space. Those technologies that encourage innovation, diversity and new thinking by providing 'open access' while also providing the necessary protections for our customers, their accounts and their data will be evaluated and, when appropriate, deployed. It is the College's intent to create and maintain a better, safer computing environment for our faculty, staff and students.

Contents

Introduction

This document sets forth the LSA IT security policy for all computing platforms connected to the College's network. Computing platforms (including but not limited to: desktop workstations, laptops, hand-helds, personal digital assistants, servers and network devices) are integral elements in the operations of the College and as such are vital to the College's mission. It is LSA's intent to secure and protect College computers before attackers attempting to gain unauthorized or illegal access compromise them.

The College implemented a mandatory patching requirement for all College computer systems that went into effect on October 31, 2005 (See the Deans' letter announcing the security initiative for LSA in Appendix B). LSA will continue to strengthen the security of its systems by requiring a minimum version for the operating systems (OS) and services/applications for all College computer systems connected to the network. These security enhancements were put in place by January 1, 2007 (See Dean's letter September 2006 in Appendix B).

In May of 2010, a preliminary draft of the report by University Audits detailed the findings of their audit of Research Computing in the College of LSA. The audit also pointed out that some LSA departments were relying exclusively on the LSA IT Security Policy (written, updated and approved by LSA Leadership in 10/2005). The overarching LSA IT Security Policy may not be detailed enough or restrictive enough to apply to areas that handle sensitive or critical data. Therefore, this document has been updated to address this issue.

Because a single insecure computer on the network poses a potential threat to all other computers, users and data, the procedures and requirements listed in this document must apply to all computers in the College that connect to the College's network.

If a computer cannot meet the minimum requirements as described in this document, the user can make use of one or more of the mitigation techniques described in this document. These mitigation techniques are provided as compensating controls to patching/upgrading an insecure computer that cannot meet the minimum requirements. These mitigation techniques can help to secure systems that fall into this category.

Threats to the security of our networked computers continue to grow in number and to evolve in form. Therefore, the LSA security policies will continue to be updated as new threats are identified and as superior countermeasures are developed. The most recent version of the LSA Security Policies will be available on the LSAIT Security Web page at:
http://webapps.lsa.umich.edu/lsait/admin/security.asp

As per Risk Assessment findings/recommendations, much can be improved by further defining IT Security policy for the College of LSA. In lieu of University-wide policy covering the following two issues, LSA.Security has been asked by the Department System Administrators (DSAs) to devise LSA-specific policy on Password-protected screensavers as well as Banner Messages which indicate proper use policies to the user prior to accessing UM IT resources.

This policy document will regularly be reviewed for updates and changes in Information Technology that may require this document be amended to address other risks.

Patching of Computers, Vulnerability Scanning and Management

LSA's intent in the first iteration of our computer security effort was to identify vulnerable computers and patch them before a malicious attacker compromises them. LSA IT Security Administrators utilizing approved University of Michigan scanners conduct monthly vulnerability scans. Currently, eEye Retina Vulnerability Scanners are utilized, starting January 2011 Tenable Nessus will be the approved network scanner. The scans are run against all computers (approximately 11,500 systems) connected to the LSA infrastructure. These scans search for vulnerabilities across multiple operating systems.

These scans start on the first Tuesday of each month and are completed by the second Thursday each month. It is important to note that this scanner is not 100% accurate and false positives occasionally occur. The final decision to identify a system as vulnerable requires careful review by a LSA IT Security Administrator. NOTE: Not all vulnerabilities or missing patches will be detected by network scanning.

Upon reviewing the "scan reports", a Security Administrator will notify IT staff within the units of vulnerable computers. The Security Administrators will work directly with the unit IT staff or the LSA Computer Service Group (CSG) to provide 'one grace request' for the patching of the computer. When a system is verified as patched by the unit IT staff or LSA CSG, the computer will be removed from the list of vulnerable computers.

LSA IT will block network access to any system that shows the same vulnerability on two successive scans. If the computer is not patched, the Security Administrator has the authority to disconnect the computer from the campus network.

Any computer that appears to be manipulating the scanning process to gain intermittent, insecure access to the network or avoid upgrade/patch installation will be removed from the network by the Security Administrator.

Some computers may not be capable of being patched due to specialized equipment or application software that may become inoperable as a result of patching. In these cases, an alternate remedy should be used to protect the computer and the department network to which it is connected. The Security Administrator will assist to determine an alternate solution. To date, alternative working solutions have been found for most of these unique circumstances. See the "Mitigation Techniques" and "Appeals" section for additional information.

LSA IT Security Administrators track scan results by department for use in trend analysis. To reward departments that mitigate identified vulnerabilities, if a department has two contiguous months of no new identified vulnerabilities; their network will be exempt from scanning for the next month. If no new vulnerability is identified the month after that, the department will again be exempt from scanning for the following month. If a new, high risk or remotely exploitable vulnerability is reported, all departments including any exempt departments will be scanned.

Minimum Versions of Operating System (OS) and Applications

The purpose of requiring minimum OS versions is to establish a baseline for computer security across the College. With the increasing threat of computer attacks across the Internet, only the most recent versions of computer operating systems and applications are robust enough to provide protection for user account credentials and institutional data.

All computers in the College that connect to the network are scanned for the version level of their operating systems OS and those services/applications running on them. If a computer is not upgraded to the minimum version level after being identified as below minimum in two successive scans, then it becomes a candidate for removal from the campus network. The minimum versions listed here will be evaluated yearly and revised as necessary. **Units and users will have a minimum of 6 months of notification before a new minimum version level is changed**.

LSAIT will block network access to any system that shows the same vulnerability for two successive scans. If the computer is not upgraded or patched to mitigate the vulnerability, the Security Administrator has the authority to have the computer disconnected from the campus network indefinitely.

Any computer that appears to be manipulating the scanning process to gain intermittent, insecure access to the network or avoid upgrade/patch installation will be removed from the network by the Security Administrator.

Some computers may not be able to be upgraded to the minimum version levels due to specialized equipment or application software that may become inoperable if upgraded. In these cases, an alternate remedy should be deployed to protect the computer. The Security Administrator will assist to determine an alternate solution. To date, an alternate working solution was found for most of these unique circumstances. See the “Mitigation Techniques” and “Appeals” section for additional information.

Minimum Operating System List

The table below outlines the minimum Operating System levels for the most popular computing platforms used by the College of LSA as of Fall, 2010.

Operating System	Minimum Client Level	Minimum Server Level
Windows	XP SP3 (w/current patches)	2003 SP2 (w/current patches)
Macintosh	OSX 10.5.x "Leopard" (w/current patches)	OSX 10.5.x "Leopard" (w/current patches)
Linux – Red Hat	RHEL 4 (w/ current patches)	RHEL 4 (w/ current patches)
Solaris (Sun systems) *	10.0 (w/current patches)	10.0 (w/current patches)
Unsupported Operating Systems**	One of the two most recent releases (w/current patches)	One of the two most recent releases (w/current patches)

** These systems are not directly supported by LSA Information Technology*
*** Operating Systems that are not supported by LSA Information Technology are not exempt from LSAIT security policy. Users of these systems should contact the LSA IT Security Administrators (lsa.security@umich.edu).*

Minimum Versions of Services, Applications, or Daemons

The table below outlines the minimum version level for the most troublesome services/applications that are deployed on College computers as of Fall, 2010.

Application/Service Software	Minimum Version/Patch Level
Adobe Acrobat	Version 8.0 (w/current patches) [1]
Apache	Version 2.0 (w/current patches)[2]
MaxDB	7.3.0 Build 25
McAfee Antivirus Software	8.5 with latest DAT files
Microsoft IIS	Version 6.0 (w/current patches)
Microsoft SQL	Version 2000 SP3a (w/current patches)
MySQL	Version 3.23 OR 4.0
Oracle (Database)	9.2.0.x or 10.1.0.x (w/current patches)
Postfix	2.x
PostgreSQL	Version 8.0.3.x/7.02003.x
Samba	Version 2.2.12 or 3.0.14a (w/current patches)
Sendmail (Mail Server/Daemon)	Version 8.12.10 for Solaris
SSH	Version 2.0 Protocol or better
Veritas Backup Exec	Version 9.1 or 10.0.5484 with Hotfix 24 (w/current patches)

There is some concern about the following applications and these may be addressed in the next evaluation of the minimum applications list: *Java, Quicktime, iTunes, ClamAV, Sophos, Adobe Flash, Microsoft Internet Explorer and Adobe Shockwave.*

[1] Adobe has not released a security update for Acrobat 7 nor any previous versions since 12/2009
[2] 1.3.x if required for certain web applications but the Systems Administrator should review the configuration for known vulnerabilities.

Services and Applications that will be identified and reviewed by the Security Administrator(s)

The following list of applications and services pose a high level of security risk to the College if installed incorrectly, or if protective measures (e.g. firewalls) are not implemented as part of the installation.

- Cleartext FTP
- Cleartext Telnet
- Sendmail (as a Mail Server or Daemon)
- Samba
- Apache
- Microsoft IIS
- Microsoft SQL
- Oracle
- MaxDB
- PostgresSQL
- Any service that uses the SunRPC protocol
- Peer-to-Peer file sharing software (e.g. Napster, Kazaa, emule, etc.)
- Google Desktop Search (Engine)

LSAIT will scan for computers running these services or applications. If a system is identified as running one of these high risk applications, a Security Administrator in collaboration with the local unit IT staff will conduct a risk analysis on that computer. The risk analysis will look at the technical configuration and threat level to the College network. The security administrator will approve these high risk applications provided the system is properly configured, managed, and secured. Alternatively, the Security Administrator can stipulate that the high risk application be disabled entirely or be moved to a production server in LSAIT or ITS.

The mitigation techniques and appeals process described in this document also apply to these applications on LSA computers.

Mitigation Techniques

If a computer cannot be patched or upgraded due to special circumstances then one or more of the following mitigation techniques should be employed by the computer owner or department computer support person in conjunction with the LSAIT Security Administrators to secure the computer. The goal of these mitigation techniques is to achieve compliance and secure the computer thru alternative means. LSAIT's Security Administrators can be reached at lsa.security@umich.edu.

Removal from Network

The quickest way to secure a computer from a network attacker is to simply remove it from the network by disconnecting the network cable. This prevents any attacker who does not have physical access to the computer from being able to access and/or compromise it. This may actually be a good choice for users who are working with extremely sensitive data and are concerned with confidentiality.

Hardware Firewall and/or Virtual Firewall

Hardware firewalls work by allowing only specified communications to reach the computer(s) behind the firewall. This option is fairly easy to implement and can protect multiple computers. Hardware firewall devices (e.g. Linksys, SMC) must be purchased. The cost is generally less than $100 per firewall. Departments are expected to cover the cost of the hardware firewalls. Funds from the Faculty Computing Upgrade Program (FCUP) or other departmental resources can be used to cover this expense. In any case, LSAIT will work collaboratively with the local unit to purchase firewall devices.

The College utilizes approximately 50 different VLAN subnets in day-to-day operations. LSAIT Security is driven to provide protection to ALL LSA assets. One way of protecting this sensitive infrastructure from unauthorized access, is the Virtual Firewall (V-FW). The primary advantage of a V-FW is it adds another layer of security. The V-FW blocks scans from unauthorized individuals, it is hard to attack a target, if you cannot directly access it. The V-FW is a stateful firewall, so any connections originating from behind the V-FW are allowed out and returned. Connections that start from outside the V-FW are restricted and only authorized connections are allowed in, all others are dropped. Another reason for utilizing a V-FW is the college Risk Assessment (RA) covers this area. There are three questions asked about firewalls in the RA questionnaire. Currently RA's are being conducted on Mission Critical and Sensitive systems.

Software Firewall No Longer an Option

Earlier versions of this document included the option of installing a software-based firewall locally on outdated operating systems that did not meet the Minimum Operating system requirements. This version of the LSA IT Security Policy does not allow that option. Instead, the requirement governing outdated Operating Systems

centers on whether the vendor continues to issue security updates to that OS. If the vendor no longer issues OS updates for the operating system then the risk of that system can no longer be mitigated by the presence of a software-based firewall. This is due, in part, to the fact that there are legacy operating systems on LSA networks that include a firewall (as part of the OS) but the vendor no longer provides security updates for. Furthermore, many of the attack vectors require updates to the browser and/or email for protection.

Non-Routable VLAN

A VLAN (Virtual Local Area Network) is a segregated section of the network. The computer system remains on the network but is not immediately visible to outside network traffic. Machines on the same VLAN are free to communicate to each other but all communication exiting the VLAN must pass through a gateway machine. If the computers that need mitigation and need to communicate with one another are also in the same room, a small switch that is not connected to the LSA network can provide this service in lieu of a full-service VLAN. If it is determined that a non-routable VLAN is the best mitigation technique, LSAIT will have to be involved in evaluation, design and deployment of the VLAN to ensure compliance with the College network. The '10 dot' network that is now available on campus is a great starting point in using a Non-Routable VLAN. The 10.x.x.x networks available can communicate with other UM networks but cannot be 'seen' or attacked easily from off-campus.

Web browsing and email access are prohibited on systems requiring mitigation as these are now the primary attack vectors – with the possible exception of needing to download updates for instrumentation software functionality.

Appeals Process

Given our experience with the first iteration of our computer security effort and the mandatory patching of computers across the College, we anticipate very few circumstances that will require use of the appeals process. To date, the LSA Security Administrators (through collaboration with the unit) have been very successful at finding workarounds to unusual computer configurations where patching or upgrading may not be possible. **The Security Administrators are sensitive to the functionality of specific research, scientific and instructional computer configurations in the College.** Every effort is always made to accommodate instruction and research computing while balancing the need for safe computing and sound security practices. This is, after all, the mission of the College.

However, if a workaround such as the mitigation techniques listed in this document are not found suitable for a specific technical reason (e.g. instrumentation connected to a computer that cannot meet the minimum requirements) then the user and their local IT representative should contact the LSA.Security group for assistance by emailing lsa.security@umich.edu.

If the Security Administrator, local IT professional and user are unable to agree upon a proper mitigation technique or workaround, then these individuals should present the specifics about the disputed situation to the LSAIT Security Committee (lsa.it.security.committee@umich.edu). This advisory committee includes faculty members, Key Administrators, and College IT staff. The committee will review the needs of the user and all of the technical details of the situation and make a recommendation to the Dean. The Dean will make the final decision on exceptions to the LSA IT security policy.

In its review, the LSA IT Security Committee will assess the security risk to the University and will involve the U-M Information and Infrastructure Assurance (IIA) group when necessary. The goal of the committee is to ensure that computer systems meet requirements set forth in the Standard Practice Guide (SPG 601.07) and any applicable legal requirements. The committee is also expected to keep the business, academic and research needs of the College in mind when making a recommendation to the Dean.

Antivirus Policy

Link to LSA Antivirus Policy:
http://webapps.lsa.umich.edu/lsait/admin/Policy/LSA-Anti-Virus-Policy.pdf

Physical Security Policy

Link to LSA Password Protected Screensaver Policy:
http://webapps.lsa.umich.edu/lsait/admin/Policy/LSA-screensaver-Policy2.pdf

Link to LSA Banner Message Policy:
http://webapps.lsa.umich.edu/lsait/admin/Policy/LSA-BannerMesg-Policy.pdf

Enhancement/Exception to LSA IT Security Policy

Other than what is already indicated in this document regarding exceptions, another option to obtain exception or set more restrictive security policy to the LSA IT Security Policy is to write your own Unit-specific Security Policy. Your cyber security policy must be approved and will require written documentation of that policy to ensure complete understanding and compliance by all parties. The scope of the policy – what computers or data or research project it covers - needs to be included in the documentation. This "exemption agreement" will require that the user accept full responsibility for supporting the computers/data in scope and acknowledging the risk(s) inherent in not complying with the LSA IT Security policy. Setting your cyber security policy too lax or not restrictive enough, can, if there is a breach of your data, result in you potentially losing your research funding and/or demotion or other similar negative result. Data residing on a non-enterprise system falls under the stewardship of the Principle Investigator (PI) whose data was used to provision the system. Stewardship is not a synonym for ownership – UM still owns the data but the data steward is responsible for the data.

Until you devise your own Departmental policy to address exceptions or more detailed policy to address unique research data requirements in your unit, you are required to abide by the policy described in this document. You are responsible for the security of your network. You should alert your Chair or Director to the existence of this document and the policies included herein. Failure to act on this can result in an unfavorable performance review and resultant possible outcomes from a poor review. You are also responsible for disseminating the information and requirements put forth in this document to your faculty, staff and students. Should you write your own departmental IT Security policy, you need to document it, be able to produce the documentation on demand, inform your IT Staff, key administrator and Chair or Director of the policy – as well as submit your policy to the LSA.Security team. We encourage you to accomplish most of these tasks by posting the policy to a website that requires authentication to access – IT Security policy should be considered confidential. Ultimately, the person using the sensitive data and requesting exception will be assuming the risk.

Link to IT Security Policy Template:
http://webapps.lsa.umich.edu/lsait/admin/IT-Security-policy-template.pdf

Revisions

Updated Minimum OS levels, reversed appendices – cb 11/4/10
Updated readability, acrobat min application, added verbiage on V-FW, and U-Audit findings on Antivirus, Banner Message and Physical Security – cb 11/5/10

Approval Dates

Vulnerability Scanning - Anthony H. Francis 7/2005

Minimum baseline version levels for operating systems (OS) and server applications - Terrence J. McDonald 9/2006

SSN Scanning - Terrence J. McDonald 4/2008

Updates to the Overarching IT Security Policy including Banner Message, Password-protected screensaver and AV requirements - Terrence J. McDonald (Dean's Subgroup Meeting) - 4/2011

Appendix A: University Audits Findings: Research Computing in LSA

<Access to the UM Audits report is available to UM personnel by request>

Appendix B: LSA's IT Security Announcements

The announcement of LSA's IT Security Initiative by Dean Rick Francis, July 2005
http://webapps.lsa.umich.edu/lsait/admin/announcement_IT_Security_Initiative_LSA.pdf

The announcement of LSA's IT Security Policy by Dean Terry McDonald, September 2006
http://webapps.lsa.umich.edu/lsait/admin/deanmemosept2006.htm

The announcement of LSA's SSN Scanning Program by Dean Terry McDonald's Memo dated April 2008
http://webapps.lsa.umich.edu/lsait/admin/deansmemo041008.pdf

Appendix C:

LSA.Security Members:

Christopher Brenner – Data Security Analyst Sr. (IT Security Manager for LSA, IT Security Coordinator, Administrator and LSA Security Unit Liaison)
Robert Pelcher – Data Security Analyst Int. (Backup to Chris Brenner)
Sally Vandeven – Data Security Analyst Int.
David Glaser/Kevin Cauchi – System Administrator Sr. (1/2 time appointment to LSA.Security)
Martin Ye – Web Application Vulnerability Mitigator
Kyle Creyts, Justin Wendl - 2 Interns (non-UM students)

Eric Randle – Contract Software Licensing Administrator (occasionally called upon in IT Security related matters)
(LSA.Security personnel are Infragard Members (www.infragard.net))

LSA.Security's Mission Statement:

To provide a secure computing environment for the College of LSA. To maintain and protect the confidentiality, integrity, and availability of LSA's computers, networks and data. By aligning ourselves with the core business objectives of the College, we help enable the LSA faculty, staff, and students to pursue their respective educational, research, and administrative goals.

LSA Joint IT-Research Committee

This Committee will develop policies and best practices so that units can implement business processes to ensure that the College is compliant with UM and Sponsor rules for purchase, management, use, and security of computing resources including hardware, software, and data. The Committee will act as a sounding board for new issues that arise. The Committee will identify and disseminate through the College's Research and IT Website the policies and resources available to the IT and Research community.