Improving the Security of the User Environment through Standards

(Aka the Desktop Security Standard)

Information Technology Security Standard #1, v13.0

Standards Name: Desktop Security Standard

Original Release Date: 5/26/2005
Latest Revision Date: 10/22/2007

Authority: This standard was approved by the Information Security Council, acting as representatives of the CIO and the Technology Leadership Committee (TLC). It derives its authority from the CIO and the campus Information Technology (IT) community.

Summary: This standard provides the security requirements for all laptops, desktops, and handheld devices used on the campus network or used by employees in their University roles. It is tightly coupled to the Information Security Standard and Remote Access Security Standard and should be read in conjunction with those documents.

Applicability/Scope: The desktop/laptop portions apply to all campus members and all users of the campus network, including guests. The sections on handheld devices apply to all campus members who use those devices as part of their University work. Information regarding removable media can be found in the Information Security Standard, Remote Access Security Standard and the Encryption Standard.

Responsible Office: ITS/CIO.

Part 1: Background

Realities of the Internet and the Campus Network

The campus network is generally open to the Internet. This allows for easy interactions with other organizations, but it also means our ability to keep malware out is very limited. Visiting machines also introduce attack traffic on a daily basis. This means that internal machines will be routinely abused, often without the user having any awareness that damage is being done. Worms and other malware are much more sophisticated than even a year ago and often combine social engineering tricks with technical attacks. What was acceptable security on a desktop, laptop or handheld device two years ago will be inadequate today.

Desktop PC's and laptops are used by nearly every member of the campus community. They give access to all types of University Data, personal information, and campus systems. If the desktop is a weak link in our security chain, it will be found and exploited. Therefore, it is important that we create a strong security standard for the desktop machine and other PC-like devices, in which we combine technical controls with user education and awareness, all backed up by policy. We also must pay close attention to the removable media that are often used within the user environment and take adequate steps to protect the University Data stored on that media.

Driving Influences for Standards

All security is about tradeoffs: we must balance costs versus benefits while considering the university's values. If we can protect 90% of our systems without introducing onerous security measures and without putting highly sensitive data at risk, we will be successful; a higher degree of security, in which users feel a need to circumvent the systems, will be counterproductive. In setting security standards, we should use these drivers:

- Legal and regulatory requirements (HIPAA, FERPA, etc.).
- Sensitivity of the data, with more sensitive data receiving more security protections, tempered by the real-world threats. This implies that we must define different categories for University Data. This process should be driven by the data owners, when they can be identified, but also demands that those who obtain and work with University Data take responsibility for how they protect it.
- Mitigation of threats that could disrupt campus IT services, e.g., PC's infected with worms that overload the network.
- Controlling risks due to access to special systems by the desktop PC. For example, a PC that has software for managing alarm systems may need additional security to ensure it cannot be hacked.

Benefits of Standards

By standards, we mean the application of common practices, tools and techniques across the desktop environment, so that we have greater certainty that a known level of security exists. If our standard demands up-to-date anti-virus software on every machine, then we can have confidence that viruses will be a minor problem. If we have ways to audit machines, we can find problems that slip through the cracks. The use of a managed desktop is the most practical way to achieve these kinds of standards. In addition to the improved protection of University Data and systems that a security standard provides, personal information stored on or transmitted via desktop PC's will be at reduced risk.

Part 2: Desktop Policy and Standards Overview

Desktop Security Policy

The desktop/laptop security policy is composed of the standards described below. Its purpose is to provide the most secure work environment that is suitable for the campus, while considering the needs of an educational institution, thereby reducing the risks to University Data and IT systems. It is expected that all campus units will work towards meeting this policy. Compliance with the policy will normally be left to each unit, but will also be subject to review by Internal Audit.

Campus Minimum Standard

All non-visitor machines *must* meet a campus minimum standard. This needs to be universally applied and exceptions should be rare. This essentially means people run anti-virus software and install security patches on a regular basis. Many machines will already meet this standard.

Handling Visitor Machines

Visitors often come for a single day, but sometimes stay longer, or come at various intervals during the course of a year. We need to apply the minimum standard to those visitors who are either routinely visiting campus, or staying for an extended period (we will suggest that > 2 weeks is an extended period). Visitors that will meet these criteria need to be informed of the standard before they arrive and either ensure that they have the proper tools in place, or be willing to allow campus IT staff to install the required tools. We do not want to impede visitors from doing their work, but we also have found that visiting PC's are often badly infected and disruptive and bring in malware that had not previously found a way onto our network. (Note: it was determined that shorter-term visitors could not be expected to comply with such a standard, so a blanket policy is not reasonable.)

Special Requirement for those running Remote Control Applications

Any Remote Control software *must* be of an approved type and be configured according to a specific standard. The Remote Control software *must* be used in conjunction with the campus VPN systems, which guarantee data security and allow for better access control to internal systems. This also applies to vendors. Exceptions to the VPN requirement may be allowed for accessing specific servers (e.g., Terminal Servers).

Enhanced Standard for Machines Handling Enterprise Data or that have Special Access to Critical Systems

Definition: “Enterprise Data” means non-public University Data. The different classes of University Data are more fully defined in the Information Security Standard.
Definition: the term “handling” (data) implies any access to the data, including read-only.

- These requirements are in addition to the Campus Minimum Standard.
- **The user *must not* run with Administrator-level rights (this means they run as “User”).** This requirement will prevent most malware from executing successfully, since malware often attempts to modify the operating system, and this requires enhanced rights. Exceptions must be approved by the unit’s IT Leader. Methods for providing exceptions are discussed below.
- The user *must not* run servers on their desktop (e.g., web or ftp servers). Exceptions can be approved by the unit, after considering the security risks versus benefits to the campus or unit. Tools such as collaboration software may effectively make the machine a server, but the risks of such tools may be reasonable.
- The user *must* take extra care not to leave Enterprise Data stored locally on the machine.
- ***Any Enterprise Data being taken off-campus, whether stored on a laptop, PDA, or some form of removable media, must be protected in accordance with the Information Security Standard and the Remote Access Security Standard.***
- The user *must* receive the security awareness training for remote access users and will receive additional training on a regular basis.

Special Standard for those Handling Confidential Data

Definition: “Confidential Data” is Enterprise Data of a highly sensitive nature and is fully defined in the Information Security Standard.

Users handling Confidential Data must take great care to keep their desktop environment clean. Data administrators will fall into this category, due to their extensive access rights. Users who handle PHI, contracts, employee records, etc., will also generally fall in this category. The requirements for machines used by people in this category include:

- These requirements are in addition to the Enhanced Standard.
- The machine *must* be configured and managed by a professional IT group.
- Stronger forms of authentication and auditing may be required.
- Before taking Confidential Data off-campus, approval *must* be granted by the Data Custodian or owner of that data set.
- ***Whereas encryption may be waived as an exception for Enterprise Data, Confidential Data must ALWAYS be encrypted when taken off campus. Also see the Information Security Standard and the Remote Access Security Standard for the fullest description of protecting mobile data.***

Exceptions

Of course, not every user (and their PC) will be able to meet all the standards and we must provide ways for people to be granted exceptions to the standards. We also need to consider the sensitivity of the user's work when granting exceptions and should be more careful with users that fall into the "Special Standard." In essence, the unit's technical and managerial leadership should perform some basic risk analysis before granting an exception. Both ITS IT Security and the TLC's Information Security Council will be available to provide timely assistance in making determinations about the risks of allowing an exception.

For all types of users, the following exceptions are acceptable:

- Using a second machine for riskier work.
- Using a virtual machine for riskier work.
- Use of a timesharing system for handling Enterprise Data (e.g., Terminal Server). This is a preferred solution, and IT staff should take advantage of this technique before granting a user enhanced rights to their machine. Users should generally be encouraged to leave all University Data on the campus servers and access it via a secure pathway.

Some types of Enterprise Data, such as e-mail, may need to be carried off-campus as a common practice. The unit may consider encrypting such data too great an impediment to normal business practices. Each unit may grant this kind of exception, but should understand the potential risks that can from disclosure of internal e-mail, or other common Enterprise Data.

For questions about exceptions, IT staff can contact itsecurity@listserv.syr.edu.

The Need for Administrator Rights on Laptops and Other Machines

Laptops and certain internal PC's pose special problems for meeting the standards, since the requirement for "User" rights often creates usability problems. To compensate for granting enhanced rights, machines that are involved in handling Enterprise or Confidential Data *must* include the following additional protections:

- A personal firewall *must* be enabled.
- The initial machine installation and configuration *must* be performed by the unit's professional IT staff.
- A Spyware cleaning program is strongly encouraged.
- Patches must be auto-applied without the need for user interaction.

Each unit must take steps to limit the number of users who are granted Administrator rights, and must limit the amount of time and frequency with which users run with such rights. IT staff should make every effort to educate their users on the dangers of running with enhanced rights. Part three offers methods for providing Administrator-level access.

- **Part 3: Technical Details of the Standards and Meeting Compliance**

Meeting Compliance

The following pages indicate the detailed requirements for meeting compliance with this standard. This includes technical controls, user/administrator practices, and required training.

The word "must" indicates those items that are required; others are either guidelines or options that are not mandatory but encouraged.

Campus Minimum Standard

- For Windows-based desktops and laptops, anti-virus software *must* be installed and set to pull updates at least daily. The rate of release for new viruses is too high to go more than a day without updates. The scanner should examine files, incoming mail, and web traffic and it should examine all executable file types. All local volumes, including removable drives, *must* be scanned. Network shares can be scanned at the server level. If buffer overflow protections exist, they should be enabled, as they provide a good defense for machines that are behind on patching.
- PDA's and smartphones should use anti-virus software, if it is available. The threat to any Windows-based device is significant and growing. Technical staff need to educate their users on the risks these devices pose as more and more people store e-mail, documents, schedules, and phone lists on them.
- Other platforms may not yet require anti-virus software, but units should anticipate that the virus threat to Mac systems is growing.
- Windows-based machines *must* be set to pull Microsoft security patches on a regular basis. This can be done in a variety of ways:
    - A daily check, in which the user maintains control. Users need to be warned (e.g., via CIRT alerts) when it is critical for them to apply new patches.
    - Through a managed method, such as a SUS/WUS server, where the client machine is configured to pull all available patches and applies them without user interaction (except perhaps when a reboot is needed). Here again, there may be communication to the users about any actions required by them. Alternate methods, such as login-time patch application, may work, but any method that requires a user login is likely to be too slow in responding to urgent patches.
- Other platforms, notably the Mac OS X line, require the same diligence in applying security patches and units that run these platforms *must* develop a patch process that operates in a timely manner. Linux is also becoming a risk as more people use Linux installations as a combination desktop/development environment.
- Other patches, such as those for common tools like Acrobat, will be handled in a variety of ways. Often these patches are as important as the MS security patches,

so units *must* have methods for updating these tools when required. We do not apply this requirement to visiting users/machines.
- Placing devices such as a Linksys router (NAT device) in front of the PC while working from home can greatly improve the protections for mobile PC's.

Standard for Machines Providing Remote Access

A machine that can be reached remotely and that is poorly secured is an easy target and a stepping stone to attacking internal servers. People routinely manipulate Enterprise Data on their desktop machines and they must take adequate steps to protect those machines.

- The sanctioned remote control applications are Remote Desktop/Terminal Server, Timbuktu, pcAnywhere, and VNC. Using off-site remote control tools, such as GotomyPC, are considered a violation of this standard.
- Some of these applications do NOT have encryption of the data stream, which makes them a greater risk for exposing data. (VNC and Timbuktu notably.) All remote control applications *must* be used with a campus VPN system, when accessed from off-campus or from high-risk campus networks (e.g., the older AirOrange wireless service). This guarantees that the data stream is protected and that Internet attacks cannot be launched against the remote control applications.
- Alternatively, some can be tunneled though an SSH connection, rather than using a VPN.

Additional requirements for remote control applications:

- The remote control application *must* log all attempts to login, including failures. The account used by the application *must* enforce password strength requirements at least comparable to the campus NetID account.
- The application should use the built-in accounts and login methods of the native operating system, so that separate accounts do not have to be maintained.
- Regardless of how the user is authenticated, there should be a mechanism for locking the account after 3-10 successive failures. Use of applications incapable of such locking are strongly discouraged. Lockouts that automatically clear after a few minutes are acceptable and may reduce denial-of-service conditions.
- These steps will reduce the ability of attackers to brute-force guess a password (internal attacks do occur).

Enhanced Standard for Accessing Enterprise Data

This standard applies to most staff and some faculty; people handling Enterprise Data or whose machine has special access to critical systems (e.g., system administrators) need to follow a more rigorous security standard.

- For Windows platforms, the user *must* operate with Windows "User" rights under normal circumstances. If this is not suitable for their work requirements (and the IT staff can verify this), the department can grant them an exception and alternative methods can be applied. For example, the user might do their Peoplesoft work through a Terminal Server but do other work directly on their PC. Additional approaches to this problem are discussed below.
- For non-Windows platforms, the equivalent of "User" rights *must* be used.
- Access control *must* be used to grant users machine access (i.e., no automatic login). Access control usually consists of a unique identifier (e.g., NetID) and an authenticator (e.g., password). The user first must identify themselves and then authenticate. The authenticator must provide adequate confidence that the user is who they claim to be (thus making password sharing a practice to avoid).
- Users of smartphones and PDA's are strongly encouraged to apply a strong password. If the device is able to lockout access after numerous successive login failures, this control should be used.
- Machines should not be shared, particularly if one of the users has "Administrator" rights. More importantly, accounts should not be shared. Accountability is important.
- To whatever degree is practical (supportable by the technical staff), the use of alternate browsers, such as Firefox, should be encouraged. For all browsers, turning off unneeded scripting systems can be helpful. Many people can live without ActiveX for 99% of their work.
- Storing of University Data on the local machine should be discouraged. In a managed environment, weekly scans for .doc/.xls/.pdf and other documents on the local drives can be useful in detecting careless data storage. As a general principle, no single user should be the sole possessor of University Data; such data *must* be maintained on a properly managed server.
- Auditing of events related to login/logout activity, changes to system security configuration, and uses of certain privileges *must* be enabled. Such auditing data is necessary for determining when attacks have occurred and for determining policy violations. Logs and audit trails should be mined on a regular basis for signs of attack.
- Personal firewalls are recommended, but not required. Personal firewalls will stop many forms of attack and are valuable, but not a cure-all.
- Desktop/laptop machines *must not* function as servers. That is, they should not provide file shares, run web or ftp servers, or have peer-to-peer applications installed. It is difficult enough to properly secure these services on servers, even with full-time administrators. Web and ftp servers are particularly dangerous and are scanned and attacked on a continual basis; even a tiny lapse in proper security will usually result in a hacked machine. Staff and faculty should look to the IT group to provide such services on a managed server.
- A good NTP server should be used. Logs with bad timestamps are difficult to work with (no ability to correlate with other information).
- Users *must* attend security awareness training on a regular basis. This requirement is only in effect when ITS is routinely offering such training.

- Available encryption methods for protecting Enterprise and Confidential Data are further discussed in the Encryption Standard. Modern tools make encryption of data fairly easy and users need to become accustomed to this new tool. PDA's may not support an encryption package, so users of these devices need to take extra care and consider what data they might expose if the device is lost or stolen.

Special Standard for Accessing Confidential Data

This standard applies to a smaller group of people and is driven by regulations (HIPAA, FERPA) and by the data owners.

- Exceptions to the "User" rights standard should be very rare. People handling this type of data *must not* expose it to unacceptable risks. The data custodian should have the right to deny access to their data by machines that do not meet the proper level of security.
- Taking Confidential Data off-campus on laptops poses a very serious risk to the campus; these are precisely the conditions that have led to many prominent news articles about data breaches.
- Users *must not* self-manage machines accessing these kinds of data.
- Stronger authentication methods, such as two factor, should be seen as a long-term goal. Users must be educated about the benefits of these methods.

Providing Administrator-Level Rights

There are many ways to give a user temporary Administrator-level access. The following are some suggestions, but units are free to develop other techniques:

- The user might be provided two accounts: a "User" level account for normal work, and an "Administrator" level account for installing software. While the user is logged in under the Administrator-level account, tools that constantly warn the user about working in this environment should be enabled, so that the user is encouraged to use the less privileged account. It is also possible that the IT staff will create the Administrative-level account but only provide the password to the user when required.
- The unit might develop tools that allow the user to login as an administrator during a specific, limited time period.
- Particular programs that require enhanced rights might be "wrappered" to allow them greater access.
- As previously mentioned, a second, virtual machine might be set up in which the user may have enhanced rights. In this model, it is important that the primary machine be a controlled environment, in which the user has only "User" rights.