Network Attached Security Standard
Version 1.0
ISPC Approved 10/6/2008
Security Standard – Network Attached Systems ................................................................. 4
FAQ ................................................................................................................................. 4
What is this standard about? ......................................................................................... 4
What is a Security Standard? ....................................................................................... 4
What are other institutions doing? ............................................................................... 4
What other resource was considered in drafting this standard? ................................ 5
Who approves changes to the Security Standard? .................................................... 5
Who has reviewed and vetted this standard? .............................................................. 5
Standards & Compliance ............................................................................................. 5
Definitions ................................................................................................................... 6
Physical Security .......................................................................................................... 7
Servers .......................................................................................................................... 7
PCs, Laptops & Mobile Devices ................................................................................... 7
Vulnerabilities & Patches .............................................................................................. 7
Software Patch updates .............................................................................................. 7
Anti-virus software ...................................................................................................... 7
System-based firewall software .................................................................................. 8
Passwords & Authentication ....................................................................................... 8
Passwords ..................................................................................................................... 8
Unencrypted Authentication ......................................................................................... 8
System Hardening ........................................................................................................ 8
Security Logging .......................................................................................................... 9
Security Logging Standard .......................................................................................... 9
Appendix 1: Antivirus & Patching Security Standard .................................................. 10
FAQ ............................................................................................................................. 10
What is this standard about? ......................................................................................... 10
Why do we need it now? ................................................................................................ 10
Antivirus & Patching .................................................................................................... 10
Vulnerability & Patching Standard .............................................................................. 10
Minimum Antivirus & Patching Standard: ................................................................. 10
Network Segmentation .............................................................................................. 11
Basic segmentation standard: .................................................................................... 12
Appendix 2: System-based Firewall Security Standard ............................................... 13
FAQ ............................................................................................................................. 13
What is a firewall? ........................................................................................................ 13
What does a typical firewall architecture look like? .................................................... 13
What is a System-based Firewall? .............................................................................. 13
Why do we need System-based Firewalls now? ......................................................... 14
Third Party Firewall vs. built-in Windows Firewall – Is there a difference? .............. 14
What system-based firewalls are acceptable? ........................................................... 14
Summary ....................................................................................................................... 15
System-based Firewall Software ............................................................................... 15
System-based Firewall Standard ............................................................................... 15
Definitions ................................................................................................................... 15
System-based Firewall Minimum Settings ................................................................ 16
Standard System-based Firewall settings are as follows: .......................................... 16
Appendix 3: Password & Complexity Security Standards ............................................ 17
FAQ ............................................................................................................................. 17
What is this standard about? ......................................................................................... 17
Why do I need a strong password? ............................................................................. 17
How will this standard affect me? ............................................................................. 17
Will this force me to change my current password? .................................................. 17
When might it be inappropriate to configure my device to enforce the minimum password complexity requirements? .......................................................... 17
Aside from the password requirements in the Minimum Standards document, what are some other guidelines I should follow?

Summary
Password Standards
Password Complexity Standards

Appendix 4: Compliance Implementation

FAQ

What is this appendix about?

Definitions
NAC (Impulse) Implementation Specifics
Physical Security
Vulnerabilities & Patching
Passwords & Authentication
System Hardening
Security Logging
Security Standard – Network Attached Systems

FAQ

What is this standard about?
Pacific has developed this Security standard for Network Attached Systems based upon security best practices as well as standards currently in use at other institutions.

Pacific, through the Network Attached Systems Policy, requires compliance with security standards to help protect systems connected to the PacificNet, to comply with audit requirements, and to prevent exploitation of campus resources by unauthorized individuals.

The security standard applies to all systems connected to the campus PacificNet. Systems include computers, printers, or other network appliances, as well as hardware connected to the campus network.

What is a Security Standard?
A security standard outlines the configuration and maintenance requirements of systems on the network, such as using strong passwords and applying patches in a timely manner. This type of practice can be used to remove vulnerable systems from a network before they are compromised or cause some other kind of problem.

What are other institutions doing?
This standard is, in part, based upon the commonly used security policies, procedures and standards of other universities. While other institutions disperse their standards throughout various security, acceptable use policies and procedures, we have elected to use an integrated approach by combining security standards into one document. This method provides a single, centralized location for the Pacific community to reference.

Examples of institutions utilizing security policies, procedures and standards include, but are not limited to:

<table>
<thead>
<tr>
<th>University</th>
<th>Standard Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>American University</td>
<td>Physical Security</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities &amp; Patching</td>
</tr>
<tr>
<td></td>
<td>Passwords &amp; Authentication</td>
</tr>
<tr>
<td></td>
<td>System Hardening</td>
</tr>
<tr>
<td>Chapman University</td>
<td>Vulnerabilities &amp; Patching</td>
</tr>
<tr>
<td>Florida Institute of Technology</td>
<td>Physical Security</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities &amp; Patching</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
</tr>
<tr>
<td>Pepperdine University</td>
<td>Physical Security</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities &amp; Patching</td>
</tr>
<tr>
<td></td>
<td>Passwords</td>
</tr>
<tr>
<td>Santa Clara University</td>
<td>Physical Security</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities &amp; Patching</td>
</tr>
<tr>
<td></td>
<td>Passwords</td>
</tr>
<tr>
<td>St. Mary’s College</td>
<td>Vulnerabilities &amp; Patching</td>
</tr>
<tr>
<td></td>
<td>Passwords</td>
</tr>
<tr>
<td>University of San Diego</td>
<td>Antivirus</td>
</tr>
</tbody>
</table>
What other resource was considered in drafting this standard?
EDUCAUSE is actively involved with cybersecurity, policies, procedures and standards through the EDUCAUSE/Internet2 Computer and Network Security Task Force (http://www.educause.edu/security). This Task Force has developed an IT Security Guide of effective security practices with the overall goal of striking a balance between higher education’s need for open, collaborative networking and security. For more specific information regarding these guidelines, please visit:

https://wiki.internet2.edu/confluence/display/secguide/Home

Who approves changes to the Security Standard?
Changes to the Security standards for networked systems will be approved by the ISPC.

Who has reviewed and vetted this standard?
This standard has been reviewed and vetted by the following:

OIT Directors
OIT Managers
TSPs (through the listserv)
Internal Audit

Additionally, the standards have been forwarded to the Data Stewards for review and comment.

Standards & Compliance

Security standards for network attached systems connected to the University of Pacific’s electronic communication network are detailed below. These standards are approved by the ISPC and are subject to periodic change. Network system users should consult this document to make sure they have the latest security standards before upgrading or changing their equipment.

Where applicable, compliance will be assured through the use of technology systems and applications. Examples of technical controls include, but are not limited to:

- PacificNet (Active Directory) enforcement of password standards
- Network access control technology (such as Impulse) to ensure system patch levels, antivirus and system-based firewall use

<table>
<thead>
<tr>
<th>University of San Francisco</th>
<th>Physical Security Vulnerabilities &amp; Patching Authentication System Hardening Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Villanova University</td>
<td>Vulnerabilities Authentication Access Controls Logging</td>
</tr>
<tr>
<td>Wake Forest University</td>
<td>Physical Security Vulnerabilities &amp; Patching Authentication</td>
</tr>
</tbody>
</table>
• System scanning tools to detect and validate system hardening efforts

More information may be found regarding compliance and implementation in Appendix 4.

Definitions

CIS: The Center for Internet Security (CIS) is a non-profit enterprise that helps organizations reduce the risks of business and e-commerce disruptions resulting from inadequate technical security. CIS members develop and encourage the widespread use of security configuration benchmarks through a global consensus process involving participants from the public and private sectors. More information related to CIS and their security configuration benchmarks can be found on their website: http://www.cisecurity.org

Confidential Information: Confidential Information is defined by Pacific’s Information Management Policy and repeated here for convenience:

Confidential Information is the strictest data classification used by the University and requires maximum control. Depending on the nature or contents of the Confidential Information, disclosure or alteration of this type of information could cause great harm to an employee, student or the University. Confidential Information requires safeguarding, either due to the requirements of law or because of the mandates of prudent and reasonable practices. Access to Confidential Information is limited to specifically authorized individuals of the University and denied to all others, unless and until directed by an officer of the University and upon advice of legal counsel of the University.

LAN: A Local Area Network is a local computer network for communication between computers; especially a network connecting computers and word processors and other electronic office equipment to create a communication system between offices.

Privileged Access: Any University User who owns a userID that allows that individual to administer security controls, userIDs, access rights or information access for others is considered to have Privileged Access. These users are also identified within University Information Technology Policies as a System Administrator or Security Administrator.

Restricted Access Information: Restricted Access Information is defined by Pacific’s Information Management Policy and repeated here for convenience:

The controlling factors for Restricted Access Information are those of confidentiality and integrity. This type of information requires protection from disclosure or alteration by unauthorized persons. Restricted Access Information is restricted to individuals who have been authorized for that information. In most cases access will be limited to specifically authorized University faculty, staff and students. This classification allows access by non-University users (such as prospective students or vendors) when authorized by the appropriate Information Administrator.

The sensitive nature of some types of Restricted Access information may be difficult to recognize because it is often integrated into daily work and/or course assignments or may be handled by a number of users. Other types of Restricted Access information may appear to be more obviously sensitive because they have a rather restricted audience. Either way, it is important to maintain the confidentiality and integrity of this information, regardless of whether it is maintained in a paper or electronic form.
Server: A server is a system that is dedicated to provide a specific service or services. Servers provide the Pacific community with needed services that typically include, but are not limited to:

1. Hosting a web site, portal or page
2. File storage
3. E-mail or messaging services
4. University financial applications
5. Authentication (logon) and access

---

**Physical Security**

**Servers**
- Systems must be physically secured in racks or areas with restricted access. Portable systems shall be physically secured if left unattended.
- Backup media must be secured from unauthorized physical access. If the backup media is stored off-site, it must be encrypted or have a documented process to prevent unauthorized access.

**PCs, Laptops & Mobile Devices**
- Unauthorized physical access to an unattended system can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where Confidential and/or Restricted Access Information is used or accessed, PCs, laptops and mobile devices such as smart phones, must be configured to "lock" and require a user to re-authenticate if left unattended. The table below lists the timeout threshold.

<table>
<thead>
<tr>
<th>Staff PCs/Laptops</th>
<th>Faculty PCs/Laptops</th>
<th>Lecterns with Fixed PCs/Laptops</th>
<th>Mobile Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 Minutes</td>
<td>60 Minutes</td>
<td>120 Minutes</td>
<td>5 Minutes</td>
</tr>
</tbody>
</table>

---

**Vulnerabilities & Patches**

**Software patch updates**
Campus networked systems must run software for which security patches are made available in a timely fashion. They also must have all currently available security patches installed in accordance with the Antivirus & Patching Security Standard [Appendix 1]. Exceptions may be made for patches that compromise the usability of critical applications.

**Anti-virus software**
Anti-virus software for any particular type of system must be running and up-to-date according to the Antivirus & Patching Security Standard [Appendix 1], including clients, file servers, mail servers, and other types of campus networked systems.
System-based firewall software
System-based firewall software must be running and configured according to the System-based Firewall Security Standard [Appendix 2], on every level of system, including clients, file servers, mail servers, and other types of campus networked systems. While the use of departmental firewalls is encouraged, they do not necessarily obviate the need for system-based firewalls.

Passwords & Authentication

Passwords
Campus electronic communications systems or services must identify users and authorize access by means of passwords or other secure authentication processes (e.g. biometrics or Smart Cards).

When passwords are used, they must meet the Password Complexity Standards [Appendix 3]. In addition, shared-access systems must enforce these standards whenever possible and appropriate and require that users change any pre-assigned passwords immediately upon initial access to the account.

Where technically possible, all default passwords for access to network-accessible systems must be modified.

Where possible and appropriate:
- Initial account passwords should be randomized and changed upon first logon
- Systems should be configured with separate accounts for privileged and unprivileged access
- Users should authenticate with an unprivileged account rather than a privileged account
- Privileged access should occur through a privilege escalation mechanism which allows the log to show which user was granted additional privileges
- Privileged access should only be granted for as long as necessary to complete the task which requires additional privileges

Unencrypted Authentication
Unencrypted system authentication mechanisms are only as secure as the network upon which they are used. Traffic across the campus network may be surreptitiously logged, rendering these authentication mechanisms vulnerable to compromise. Therefore, all campus systems must use only encrypted authentication mechanisms unless otherwise authorized by the ISPC.

In particular, historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

System Hardening
Electronic communication systems are used to process and transmit information and services throughout PacificNet. Information and services must be processed and transmitted securely and reliably to assure that data confidentiality, integrity, and availability are preserved.

The IT Security Office (ITSO) provides specific Hardening Checklists for common operating system platforms and systems. These Hardening Checklists provide the foundation for assessing the security state of a particular system, providing a measurable target. The ITSO has selected the CIS standards that are based on internationally known security best practices and are recognized by many organizations as the de facto standard for deploying reasonably secure systems.

Contact the ITSO at ITSecurity@pacific.edu for the current CIS standard and auditing tool.
Security Logging

Security Logging is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Security logging processes consist of activities such as the review of: user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, etc.

The purpose of the security logging standard is to ensure that information resource security controls are in place, are effective, and are not being bypassed. Some of the benefits of security logging are the early identification of wrongdoing and the discovery of new security vulnerabilities.

Security Logging Standard

All systems that handle Confidential Information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. Who or what performed the activity, including where or on what system the activity was performed from (subject)?
3. What the activity was performed on (object)?
4. When was the activity performed?
5. What was the status (such as success vs. failure), outcome, or result of the activity?
Appendix 1: Antivirus & Patching Security Standard

FAQ

What is this standard about?
Weaknesses in operating systems and applications provide a foothold for computer viruses and hackers to attack. This standard is about reducing the risk of malicious computer viruses and malevolent individuals gaining unauthorized access to Pacific’s Confidential and Restricted Access information.

Why do we need it now?
Antivirus software is one of the most important tools in protecting your computer and personal information from viruses and worms. When it comes to technology and security, computers are quite similar to houses. Most people would not leave their doors and windows wide open, exposing their residences to complete strangers. Yet, why are computers often left open and unsecured, virtually welcoming viruses to sneak in the front door or window?

As technology progresses, operating systems (OS) and applications become increasingly more complex. While one would hope for perfectly running software, the reality is that as software complexity grows so do the vulnerabilities and bugs. Operating system and application companies routinely provide security alerting and patches for these vulnerabilities and bugs. The timely patching of vulnerable software is critical in Pacific’s ongoing struggle to protect its Confidential and Restricted Access information.

Antivirus & Patching

The University reduces exposure to risk by establishing antivirus and patching security standards for systems connecting to PacificNet. These standards are based on the common security practices and principles of keeping systems up to date with security patches, use of a personal firewall to filter inbound/outbound applications and access, and malware (computer virus, Trojan, spyware, etc.) detection and removal software.

Vulnerability & Patching Standard

Minimum Antivirus & Patching Standard:
- Operating System (OS) Patches
  - 72 hours of release for critical security patches
  - 1 week for non-critical patches
- Application Security Patches
  - 72 hours of release for critical security patches
  - 1 week for non-critical patches
- Personal Firewall Software
  - Active
  - Patched (within 72 hours of release)
  - Student/3rd Party Owned Systems:
    - May be associated with security suite software (Symantec, TrendMicro, McAfee, Sophos, ZoneAlarm, etc.)
  - University Owned Systems:
    - Symantec Client Firewall or other university purchased equivalent
- Anti-Malware Software
  - Anti-Virus
    - Active
    - Patched (within 72 hours of release)
    - Current pattern files
    - **Student/3rd Party Owned Systems:**
      - May be associated with security suite software
        (Symantec, TrendMicro, McAfee, Sophos, Avast, etc.)
    - **University Owned Systems:**
      - Symantec Anti-virus or other university purchased equivalent
  - Anti-Spyware
    - Active
    - Patched (within 72 hours of release)
    - Current pattern files
    - **Student/3rd Party Owned Systems:**
      - May be associated with security suite software
        (Symantec, TrendMicro, McAfee, Sophos, Avast, etc.)
    - **University Owned Systems:**
      - Symantec Anti-virus or other university purchased equivalent

---

**Network Segmentation**

Isolation of systems by network segmentation occurs when systems fail to meet the Antivirus and Patching standard. Ideally, at risk systems are moved to network segments that are designed to only provide access required for OS and application security updates. Additional segmentation to an Internet only network applies to unauthenticated users.
### Basic segmentation standard:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Segmentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthenticated Users/Machines</td>
<td>Isolation of Systems to Internet Only Network</td>
</tr>
<tr>
<td>Operating System</td>
<td>No Special Segmentation</td>
</tr>
<tr>
<td>Fully Patched &amp; Updated</td>
<td></td>
</tr>
<tr>
<td>Security Applications</td>
<td></td>
</tr>
<tr>
<td>Fully Patched &amp; Updated</td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td></td>
</tr>
<tr>
<td>Critical Updates Pending - Within 72 Critical Patch Window</td>
<td>No Special Segmentation</td>
</tr>
<tr>
<td>Security Applications</td>
<td></td>
</tr>
<tr>
<td>Critical Updates Pending - Within 72 Critical Patch Window</td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td>No Special Segmentation</td>
</tr>
<tr>
<td>Non-Critical Updates Pending - Within 1 Week Patch Window</td>
<td></td>
</tr>
<tr>
<td>Security Applications</td>
<td></td>
</tr>
<tr>
<td>Non-Critical Updates Pending - Within 1 Week Patch Window</td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td></td>
</tr>
<tr>
<td>Critical &amp; Non-Critical Updates – Outside of Patch Window</td>
<td>Isolation of Systems to Internet Only Network for Update Purposes</td>
</tr>
<tr>
<td>Security Applications</td>
<td></td>
</tr>
<tr>
<td>Critical &amp; Non-Critical Updates – Outside of Patch Window</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2: System-based Firewall Security Standard

FAQ

What is a firewall?
A firewall is basically a filter that prevents unwanted communications between systems. Much like a coffee filter prevents the grounds from entering the pot, a firewall prevents things like computer viruses and hackers from entering a network or system.

What does a typical firewall architecture look like?
Firewalls are used at various points or layers within a computer network. Using firewalls in this manner enables Pacific to prevent unwanted activities from a variety of locations. Below is an example of a typical firewall architecture:

What is a System-based Firewall?
A system-based (or host-based) firewall is a software program running on computers (servers, PCs and laptops) that prevents unauthorized access to or from a private network. Firewalls are tools that can be used to enhance the security of computers connected to a network, such as a LAN or the Internet and are a key component of the University’s security framework.

System-based Firewalls are intended to isolate computers from the Internet by inspecting each individual inbound and outbound packet of data to determine whether it should be allowed to pass or be blocked. System-based Firewalls have the ability to further enhance security by enabling granular control over what types of system functions and processes have access to networking resources. These firewalls can use various types of signatures and host conditions to allow or deny traffic.
Why do we need System-based Firewalls now?
When a network is connected to a public network, it is potentially exposed to a number of threats including hackers and malware (computer viruses and Trojans). The proliferation of always on broadband Internet connections increases the University’s exposure to malicious attack and requires users to be ever vigilant of security issues. Inbound network traffic can cause damage to computer files and programs even when the user is away from the computer and the computer is idle. In a system that is not protected with any security measures, malicious programs such as viruses can infect the system and cause damage that may be difficult to repair. The loss of financial records, e-mail, or student data can be devastating to the University or an individual.

Third Party Firewall vs. built-in Windows Firewall – Is there a difference?
The primary advantage of third party firewalls is that they attempt to control outbound connections, whereas the built in Windows firewall will not. Additionally, third party firewalls depend upon the end user's judgment whether or not to allow a program to make a connection.

What system-based firewalls are acceptable?
Symantec Client Firewall
The University of the Pacific has licensed Symantec Client Firewall (SCF), a component of Symantec Client Security (which also includes Symantec Antivirus Corporate Edition, a product separately licensed for use at Pacific). The SCF is deployed with the standard desktop/laptop image.

Internet Connection Firewall
The Internet Connection Firewall (ICF) comes with Microsoft Windows XP Service Pack 1 and later as well as with Microsoft Server 2003. It can fulfill the requirements of the Minimum Standards for Security; however, the Symantec Client Firewall provides additional protection, is available for free to the University community, and is strongly recommended over the ICF.

Instructions for configuring the Internet Connection Firewall are available from Microsoft's security page (http://windowshelp.microsoft.com/Windows/en-US/security.mspx).

Other Firewalls
To meet the Minimum Standards, other system-based firewalls must, at a minimum:
- Be running at all times
- Block inbound traffic to ports that are not running necessary services
- Be capable of logging inbound and outbound blocked packets for troubleshooting purposes

It is strongly suggested that system-based firewalls also:
- Allow all inbound and outbound ICMP traffic
Summary

A system-based firewall is software that runs directly on a networked device (computer, server, PC and/or laptops) and protects that device against attack from the network by controlling incoming and/or outgoing network traffic. There are other kinds of firewalls that sit on the network between one or more hosts and the rest of the network, but their presence does not necessarily exempt protected devices from the need to run system-based firewall software.

System-based firewalls work by logging, passing, or blocking incoming and outgoing network packets. Rules govern what to look for and what to block or pass. Typical firewalls block based on source and destination address and port, packet type, etc. Advanced firewalls identify every application and system component, and rules to allow or block can be specific for each uniquely. A firewall product usually comes with predefined rules to defend against known attacks similar to anti-virus software, and predefined rules for each application and system component's normal activities. Rules may also just log the activity for later inspection or to send or display alarms. Some system-based firewalls can also prevent malicious software from attacking other devices on the network.

System-based Firewall Software

System-based firewall software must be running and configured according to the "System-based Firewall Security Standard", on every level of device, including clients, file servers, mail servers, and other types of campus networked devices. While the use of departmental firewalls is encouraged, they do not necessarily obviate the need for system-based firewalls.

System-based Firewall Standard

The key to a good System-based Firewall practice is striking a balance between security and application requirements. While blocking all inbound and outbound network access would seem to offer the strongest security posture, that stance would invariably interfere with normal computer operations and render most network services useless. Conversely, allowing all inbound and outbound network access offers little or no security to the University's computers and users. This standard was developed in an effort to strike the balance of security vs. usability of the University's computers and services.

One component of this standard is Pacific’s ability to centrally manage and administer firewall configurations and logs. Centralized management of firewall configurations enables for the standardization of key firewall rules, provides the ability to validate the online status of individual firewalls, and allows centralized reporting of security events.

As future threats to the University’s computing resources are realized, the ISPC may modify this security standard document to reduce and/or mitigate identified risks.

Definitions

Standard Image: A standard image is comprised of the standard Operating System, office productivity applications (Word, Excel, etc.), and other known commonly used applications (Banner, FireFox, HEAT, etc.).

Non-Standard Image: A non-standard image may be comprised of those applications found in a standard image and would have other non-documented applications (Internet downloaded, shareware, tools & utilities, and/or self installed applications).

User Prompt: System-based Firewall Applications have the ability to prompt the computer
user when unknown application communications are attempted. Typical requests include:

- **Allow Activity (One Time)** – Communications allowed for the application session duration
- **Allow Activity (Always)** – Communications always allowed, no further prompting
- **Deny Activity (One Time)** – Communications denied for the application session duration
- **Deny Activity (Always)** – Communications always denied, no further prompting

---

**System-based Firewall Minimum Settings**

On some firewalls, when a program needs to talk to another computer on the network, whether it is a web site, email server, or instant message buddy, it opens a door on your computer. The first time a program does this after a firewall is installed, the firewall will ask to allow it. It will generally give three options:

- Denying the program access to the network
- Allowing it just this one time, prompting the next time it wants to use the network
- Allowing it forever, never prompting again the next time it wants to use the network

In general, these warnings should not come up unless a program is run for the first time since installing the firewall, or after a new program is installed. If neither of these situations apply, it would be advisable to block the program and call support.

These minimum settings should provide the appropriate balance of usability vs. security and should minimize exposure to network threats. The tradeoff for this stance is that users are allowed a greater level of flexibility in making decisions to allow or deny application access into and out of their computing environment. Users that are not properly trained on the prompting process could inadvertently deny a trusted application or conversely allow a malicious application. Further end user training and awareness on the appropriate handling of the prompts, specific to the system-based firewall application, is required.

**Standard System-based Firewall settings are as follows:**

<table>
<thead>
<tr>
<th>Minimum Settings</th>
<th>Inbound</th>
<th>Outbound</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Image</strong></td>
<td>Allow (Always) – Known Applications</td>
<td>Allow (Always) – Known applications</td>
</tr>
<tr>
<td></td>
<td>Deny or Prompt (One Time) – All connection requests for non-standard applications</td>
<td>Prompt (One Time) – All connection requests for non-standard applications</td>
</tr>
<tr>
<td><strong>Non-Standard Image</strong></td>
<td>Deny or Prompt (Always) – All connection requests</td>
<td>Prompt (One Time) – All connection requests</td>
</tr>
</tbody>
</table>
Appendix 3: Password & Complexity Security Standards

FAQ

What is this standard about?
A password standard should effectively defend against hostile attempts to steal or “crack” users’ passwords. Various defenses or mitigations for such attacks have been developed. It is widely acknowledged that it is impossible to provide perfect protection for passwords. Given enough time and computing horsepower, a hostile attacker will compromise at least some passwords. Therefore, the aim of a password standard is to make such an attempt difficult and significantly reduce the chances that it will be successful.

Why do I need a strong password?
Passwords are used for various purposes at Pacific. Some of the more common uses include: local accounts, web accounts, and email accounts. A weak (or absent) password is one of the most common ways for an attacker to compromise your account; therefore, you should be aware of how to select strong passwords.

How will this standard affect me?
The Password Complexity Standard does not change our current PacificNet password practice. Older systems that do not recognize punctuation within a password will also remain unaffected. As older systems are replaced, new systems would be expected to comply with the Password Complexity Standard.

Will this force me to change my current password?
No, the Password Complexity Standard does not change University password expiration times or practices.

When might it be inappropriate to configure my device to enforce the minimum password complexity requirements?
It may be inappropriate in situations where the device is single-user (home machines or laptops). While you MUST use a password that meets the complexity requirements, it is not necessary to configure the device to enforce the requirements on these single-user devices.

Aside from the password requirements in the Minimum Standards document, what are some other guidelines I should follow?
1. Do not use an easily guessed password. Some examples of passwords that would be easy to guess:
   - Names of family, pets, friends, co-workers, etc.
   - Computer terms and names, commands, sites, companies, hardware, software.
   - Birthdays and other personal information such as addresses and phone numbers.
   - Word or number patterns like aaabbb, qwerty, zyxvwuts, 123321, etc.
2. Passwords should never be written down or stored on-line.
3. In general, a password should be as long as possible while still being easy-to-remember. One way to do this is create a password based on an easy-to-remember phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmbB1w2R!" or "TmbB1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!
4. Passwords must change on a regular basis. Systems will be configured to initiate a password change every six months. You must also change your password any time you suspect that your account has been compromised or tampered with.
5. Do NOT use the same password for any of your University accounts that you use for a non-University service or third-party web site.

---

**Summary**

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the University of Pacific's network. As such, all PacificNet users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

---

**Password Standards**

Campus electronic communications systems or services must identify users and authorize access by means of passwords or other secure authentication processes (e.g. biometrics or Smart Cards).

When passwords are used, they must meet the Minimum Password Complexity Standards [below]. In addition, shared-access systems must enforce these standards whenever possible and appropriate and require that users change any pre-assigned passwords immediately upon initial access to the account.

All default passwords for access to network-accessible devices must be modified.

Where possible and appropriate:

1. Initial account passwords should be randomized and changed upon first logon
2. Devices should be configured with separate accounts for privileged and unprivileged access
3. Users should authenticate with an unprivileged account rather than a privileged account
4. Privileged access should occur through a privilege escalation mechanism which allows the log to show which user was granted additional privileges
5. Privileged access should only be granted for as long as necessary to complete the task which requires additional privileges

---

**Password Complexity Standards**

Where technically possible, all passwords must meet the following complexity guidelines:

- Contain eight characters or more
- Contain characters from two of the following three character classes:
  1. Alphabetic (e.g., a-z, A-Z)
  2. Numeric (i.e. 0-9)
  3. Punctuation and other characters (e.g., !@#$%^&*()_+-=\[\]{}\["',<>?,./)

The password MUST NOT be:

- A derivative of the username
- A word found in a dictionary (English or foreign)
- A dictionary-word spelled backwards
- A dictionary-word (forward or backwards) preceded and/or followed by any other single character (e.g., secret1, lsecret, secret?, secret!)
Appendix 4: Compliance Implementation

FAQ

*What is this appendix about?*
Where applicable, compliance to the approved Security Standard will be assured through the use of technical systems. This appendix will summarize the technology used to implement the standards, where possible.

**Definitions**

**Network Access Control (NAC):** Network Access Control is a computer networking technology that used to secure the network devices and systems prior to the systems/devices accessing the network. NAC also integrates the automatic notification and fixing of non-compliant systems/devices before allowing PacificNet access. Below are some examples of NAC solutions:

- Impulse Safe Connect
- Cisco Network Admission Control
- Sophos Network Access Control
- Symantec Network Access Control

**Vulnerability Scanner:** A vulnerability scanner is a computer program or system designed to search for and map systems for weaknesses in an application, computer or network.

**NAC (Impulse) Implementation Specifics**

Pacific utilizes NAC (Impulse) for the express purposes listed below:

- Send emergency notifications of campus emergencies as determined by Pacific’s Public Safety Department
- System and device registration (computer name, user name and IP address)
- Ensure systems and devices are operating with the most current operating system security patches
- Ensure systems and devices are operating with a current and active antivirus application
- Ensure systems and devices are operating with current and active system-based firewall
- Stop actively propagating viruses, worms and Trojans across PacificNet

**Pacific will not utilize NAC (Impulse) for any other activity. This includes but is not limited to the following activities:**

- Used in conjunction with KeyServer or any other inventory software
- Monitoring user (staff, faculty and student) network activities
- Monitor users data files or use of data files

Any change in the above NAC (Impulse) practices must first be approved by Pacific’s IT Security Office, the Chief Information Officer and be further reviewed and approved by the ISPC. Furthermore, any/all changes must be fully recorded and detailed in this document.
**Physical Security**

**PCs, Laptops & Mobile Devices**
The Security Standard specifies a system or device lock when the system is not being actively used. This standard will be implemented by utilizing the following:

- *Windows PCs (Desktop & Laptops)*
  Where technically possible, Active Directory will be used to set the minimum timeout before the screen saver is initiated. Manual configuration of the timeout is required for fixed lectern systems and for systems that are not managed by Pacific’s Active Directory.

- *Non- Windows (Desktops & Laptops)*
  The centralized management of non-Windows device locking is not available at this time. Non-Windows devices must be manually configured lock after the appropriate time as indicated by the standard.

- *Mobile Phones & Smart Phones*
  Blackberry devices will be configured through the management system to lock after 5 minutes of inactivity. Where supported, all other brands of mobile and smart phones must be manually configured to lock after 5 minutes of inactivity.

**Vulnerabilities & Patching**

Pacific reduces exposure to risk by establishing antivirus and patching security standards for systems connecting to PacificNet. These standards are based on the common security practices and principles of keeping systems up to date with security patches, use of a personal firewall to filter inbound/outbound applications and access, and malware (computer virus, Trojan, spyware, etc.) detection and removal software.

Pacific ensures compliance to the Vulnerability & Patching standard through the use of NAC technology. NAC technology will be used to ensure connecting systems and devices:

- Meet the patching standard
- Meet the antivirus standard
- Meet the system-based firewall standard

Pacific routinely tests systems for commonly known vulnerabilities and weaknesses throughout PacificNet by utilizing a Vulnerability Scanner. The IT Security Office is charged with maintaining the Pacific vulnerability scanning service. When systems are identified as being vulnerable, the appropriate System Administrator and/or TSP will be notified. For more information regarding Vulnerability Scanning or to request a scan, please contact the IT Security Office at ITSecurity@pacific.edu.

**Passwords & Authentication**

**Passwords**
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the University of Pacific's network.

Pacific enforces password complexity standards through PacificNet through the use of Active Directory. System Administrators are responsible to assure Password Complexity Standards are met for systems that are not authenticated through PacificNet.

**Unencrypted Authentication & Services**
Systems and devices connecting to PacificNet are required to utilize encryption as a part of authentication process. Systems that do not authenticate to PacificNet but store and/or
process Confidential and/or Restricted Access information will be audited for compliance to the standards.

Unencrypted and insecure services will be filtered and blocked at the University firewall.

### System Hardening

The IT Security Office (ITSO) provides specific Hardening Checklists for common operating system platforms and systems. These Hardening Checklists provide the foundation for assessing the security state of a particular system, providing a measurable target. The ITSO has selected the CIS standards that are based on internationally known security best practices and are recognized by many organizations as the de facto standard for deploying reasonably secure systems.

Systems storing and/or processing Confidential and/or Restricted Access information will be assessed through the use of the CIS standard and auditing tool. Exceptions to the CIS standard will be fully documented and where applicable additional controls will be implemented such as more detailed audit logs, firewall rules and weekly vulnerability scans.

### Security Logging

Security Logging is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Security logging processes consist of activities such as the review of: user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, etc.

The Office of Information Technology must maintain a system for the centralization of log files for systems that store and/or process Confidential Information. System Administrators must forward copies of their log events/files to the centralized logging system.