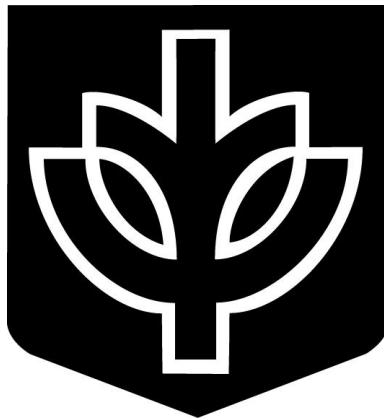


**LOGON BANNERS FOR COMPUTER SYSTEMS
AND NETWORK DEVICES**



Information Security Team
DePaul University
1 East Jackson Boulevard
Chicago, Illinois 60604 US
<https://infosec.depaul.edu/>

13th December 2002

Copyright Notice

Copyright © 2002. DePaul University. All Rights Reserved.

1. "Redistribution of source code, documentation and advisories, must retain the copyright above copyright notice and disclaimer included in Section 4 of this copyright notice."
2. "Redistributions in binary forms must reproduce the above copyright notice, this list of conditions, and the disclaimer included in Section 4 of this copyright notice."
3. "Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software or information without specific prior written consent."
4. "The information contained herein is provided by the regents and contributors 'AS IS' and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the regents or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data or profits; or business interruption) however caused and on any theory or liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this information, even if advised of the possibility of such damage."

Contents

1 Summary	4
2 Logon Banners	5
2.1 Standard Banners	5
2.2 Shortened Banners	5
3 Deployment	6
3.1 UNIX Operating Systems	6
3.1.1 AIX, HP-UX, Linux, Irix, SunOS, and Solaris	6
3.1.2 FreeBSD and OpenBSD	6
3.2 Microsoft Operating Systems	6
3.2.1 Windows NT, 2000, XP	6
3.3 Cisco Internetwork Operating System (IOS)	6

1 Summary

Information security policies are often a covert tactic applied *after* unauthorized intrusion. While such actions may suffice to apply internal disciplinary actions, they often may not withstand legal action during ongoing prosecution of guilty intruders. A computer system that is property of DePaul University intended to meet strict business or academic requirements should display a warning to all users, authorized *and* unauthorized, detailing the proper use and treatment of the computer systems. These messages are often referred to as warning or logon “banners” and encapsulate the applicable sections of security policies detailing access and proper use of a system.

This document intends to assist system administrators and users in configuring their systems properly to display the DePaul University Information Security Team recommended logon banner *prior to* or *immediately following* access to a system.

2 Logon Banners

2.1 Standard Banners

The following banner should be used to display proper access and use of a computer system.

"This is a DePaul University computer system. This resource, including all related equipment, networks and network devices, are provided for authorized DePaul University use. DePaul University computer systems may be monitored for all lawful purposes, including to ensure authorized use, for management of the system, to facilitate protection against unauthorized access and to verify security procedures and operational procedures. The monitoring on this system may include audits by authorized DePaul University personnel to test or verify the validity, security and survivability of this system. During monitoring information may be examined, recorded, copied and used for authorized purposes. All information placed on or sent to this system may be subject to such monitoring procedures. Use of this DePaul University computer system, authorized or unauthorized, constitutes consent to this policy and the policies and procedures set forth by DePaul University. Evidence of unauthorized use collected during monitoring may be used for criminal prosecution by University staff, legal counsel and law enforcement agencies."

2.2 Shortened Banners

Where necessary due to system limitations, the following banner should be used to warn of improper system use.

"This is an actively monitored system. Unauthorized access prohibited."

Shortened banners *should not* be deployed except in the case of system limitations.

3 Deployment

Deploying the INFOSEC logon banners requires system level changes to be made. Various operating systems and network services offer the banner content in various methods; verify that your operating system or network service type and version prior to implementing the following changes.

3.1 UNIX Operating Systems

All UNIX systems should retain the banner text in the `/etc/motd` file. This file is displayed as a "message of the day" intended to inform users as to system news.

3.1.1 AIX, HP-UX, Linux, Irix, SunOS, and Solaris

Under these UNIX operating systems variants, the standard banner should be placed in `/etc/issue`.

3.1.2 FreeBSD and OpenBSD

Under BSD variants the `/etc/gettytab` file is used to distribute logon banners for directly connected terminals such as dialup lines, a console, etc. To display the logon banner, add the banner after each "im" (initial message) to the appropriate stanzas in `/etc/gettytab`.

The "if" (initial file) directive may be used for displaying the contents of a file. Refer to your vendors' documentation for more information regarding the deployment of a logon banner for local "TTY" access and network access.

3.2 Microsoft Operating Systems

3.2.1 Windows NT, 2000, XP

The banner text should be placed into the following registry key.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\  
CurrentVersion\Winlogon\LegalNoticeText
```

3.3 Cisco Internetwork Operating System (IOS)

To configure a Cisco network device (IOS based) to display a warning banner *prior* to login, the following configuration should be implemented via the command line interface.

```
router# banner login #
```

After input of the logon banner is complete, terminate the configuration with a single "#" character.