

Computing Security Resources

Resources for...

Windows users

- **Routine Up-keep** at *least* monthly:
 - **Windows Update** <http://windowsupdate.microsoft.com>: Keep your operating system up to date with the latest functional and security patches.
 - **Office Update** <http://office.microsoft.com/officeupdate>
- Symantec Endpoint Protection is available from the Case [Software Center](#). Use it!
- Regularly use the [Microsoft Baseline Security Analyzer \(MBSA\)](#) to audit your computer's security. This tool is easy to use, and not only identifies problems, but *tells you how to correct them*. It knows about IIS and SQL Server, among other important applications. This program supersedes HFNetChk.
- Microsoft's main security website: <http://www.microsoft.com/security>, and the more technical TechNet security site, <http://www.microsoft.com/technet/security>.
- Microsoft's [Windows XP Security Guide](#)
- Microsoft's [Windows Vista Security Guide](#)
- Microsoft's [Windows 7 Security Guide](#)
- Tools for IIS:
 - Microsoft [IIS Lockdown Tool](#)
 - Microsoft [UrlScan Security Tool](#)
- fport from [Foundstone](#) lists the open TCP & UDP ports on your system, and the programs that have them open. (This is like Unix lsof.)

System administrators

- Symantec Endpoint Protection is available from the Case [Software Center](#). Use it!
- Logon banners improve the ability to prosecute intruders. Here's an [example](#).
- To test the security of an SMTP (mail) server you run (such as Sendmail), telnet to <telnet://relay-test.mail-abuse.org>.
- If you need a certificate signed or one that will be recognized outside the University, see the Case Middleware Engineering group's offering at <https://its-services.case.edu/middleware/Responsibilities/SSL/SSL.html>.

Policies

Acceptable Use Policy

[Case ITS Acceptable Use Policy](#)

Excessive outgoing bandwidth consumption

Users may not consume a disproportionate amount of outbound network bandwidth.

SMTP Policy

[CASE ITS SMTP Policy](#)

User-provided domain names

Users may not cause a hostname outside the Case domains to point to an IP address within the Case address spaces.

User-provided wireless access points

Users may not connect a wireless access point to the network, nor use the wireless capabilities of a network-connected computer to provide wireless network access.

Sniffing Policy 1.0, 2004-03-22

The use of network sniffers (software that opens a network interface in promiscuous mode) is prohibited on the Case network without prior arrangement with ITS. By using a sniffer, one gains access to data not normally available to him. This data may include some that is regulated by the ITS Ethics Policy.

Software firewalls

ITS recommends that users employ host-based firewall software on their individual computers. Windows XP and Mac OS X users should enable the firewall features available in those OSes. Unix users should run ipchains, iptables, ipfw, or something similar.

Hardware firewalls (revision posted 2005-01-24)

ITS has received requests from several labs & departments concerning deployment of hardware firewalls. Hardware firewalls are prohibited on the network. Rather than deploy a firewall to protect valuable information assets, those assets should be placed into an ITS data center. ITS's policy is that all business-critical information assets are to be housed on ITS-managed servers in an ITS-managed data center.

Regulatory Compliance

All University information systems are subject to the following federal regulations:

- Family Educational Rights and Privacy Act (FERPA), concerning student records. Stated in the [Case General Bulletin](#).
- Gramm-Leach-Bliley Act (GLBA), concerning financial information handling.
 - [FTC information](#)
- Health Insurance Portability and Accountability Act (HIPAA), concerning medical information. More info at <http://www.hhs.gov/ocr/privacy/> and at CWRU ITS's [HIPAA information page](#).

More ITS policies

Please see [more ITS policies](#).