

## Information Technology (IT) Security Program

*This brochure provides a ready source for locating current IT security information. Consult these sites often because policies and guidance documents are continually being updated.*

*For further questions about the information in this brochure, contact Rob LeVine, NIEHS ISSO, 919-541-7559 or send an email to: [levine1@niehs.nih.gov](mailto:levine1@niehs.nih.gov)*

### NIEHS ISSO Web Page:

<http://www.niehs.nih.gov/isso>

Includes our local web resources for computer security. Use this web site to find contacts, virus information, incident procedures, FAQ, documents, and tools.

### NIEHS Announcements Web Page:

Often includes computer security news and important information for NIEHS users. <http://www.niehs.nih.gov/announcements>

**NIEHS Publications with IT Security Information:** The NIEHS community is kept informed about IT security events, concerns, and information through various publications (e.g., CTB's *Connections*) and periodic announcements.

### NIEHS Frequently Asked Questions (FAQs) on security topics:

<http://www.niehs.nih.gov/isso/faq.htm>

On-line answers to common security questions from the NIEHS community

## NIH CIT References

*Great information, but use **NIEHS** contacts!*

*NIH information includes contacts and procedures written for users in Washington D.C. NIEHS has local contacts and procedures.*

### NIH Frequently Asked Questions (FAQs):

<http://irm.cit.nih.gov/nihsecurity/secfaqnih.htm>

More security topics, but remember that NIEHS may have local contacts and procedures.

**Non-Technical Security News:** An NIH site for hot security alert information such as a virus outbreak. This site is intended primarily for end users seeking security assistance, practical advice and general user training. Consult your CSP or ISSO for additional information and assistance. <http://securitynews.nih.gov/>

**CIT Security Web Page:** The NIH main security menu provides access to tons of information about security tools, training, policy, guidelines, support groups, incident response, and other technical advice. <http://www.cit.nih.gov/security.html>

**Email Viruses & Anti-Virus Information:** We use several methods to protect against virus infection in your mail and file transfers. Administrators can find advisories, updates and technical guidance on managing virus outbreaks at this site. <http://antivirus.nih.gov/>

**Advice for Application Developers:** All developers and application test teams (NIH staff and contractors) who design, program, and test applications need to reference this list of potential system vulnerabilities. <http://irm.cit.nih.gov/security/SecAdxApDv.html>

## Policies & Guidance

**Rules of Behavior: The 1-stop document on security for users at NIH.** These rules govern the use of IT equipment (including remote users). Computers, peripheral equipment, software, and data at NIH must be protected and used only for official government purposes.

<http://irm.cit.nih.gov/security/nihitrob.html>

### Unwanted E-mail, Spam, & Chain Letters:

Do you need advice on how to deal with unsolicited email messages and announcements? Proliferation of this type of e-mail can flood the network infrastructure and reduce response time.

<http://www.niehs.nih.gov/isso/spam.htm>

**Passwords:** These password guidelines will help control access to your systems. To maintain security, passwords should not be shared, posted in plain sight, or easy to guess.

<http://www.niehs.nih.gov/cio/pwpolicy.htm>

**VIRUS Procedures:** The ISSO virus information web page is at:

<http://www.niehs.nih.gov/isso/viruspg.htm>

### Remote Access Procedures and Policy:

Users accessing NIEHS resources from off-site locations raise concerns for potential system and network vulnerabilities.

<http://www.niehs.nih.gov/compuref/remotelhome.htm>

### Suspicious activity & security incidents:

A security incident involves illegal access to NIEHS technology, inappropriate use of computers, or abuse of privileges on the network. If you suspect an incident, refer to:

<http://www.niehs.nih.gov/isso/problems.htm>

## IT Security Management & Technical Support Teams

**Information Technology Management Committee (ITMC):** The NIH ITMC provides leadership and direction on NIH-wide IT security initiatives. The ITMC Security Subcommittee addresses mitigation of agency-wide problems and system security threats.

**Computer Technology Branch (CTB):** This office serves as the focal point for NIH IT security. CTB develops and coordinates NIEHS initiatives and guidance, performs security scans and risk assessments, responds to security incidents, tracks virus and intrusion activity, and provides information and training support. CTB coordinates guidance with NIH's CIO and ISSO.

**Incident Response Team (IRT):** Response team members are trained in investigating IT security events such as web defacements, computer compromises, intrusions, and viruses. The IRT procedures can be found at: <http://www.niehs.nih.gov/isso/problems.htm>

**Computer Support Person (CSP):** The CSP contacts respond to all calls for computer assistance. Contact information can be found at: [http://www.niehs.nih.gov/lsp/lspguide/1\\_chart.htm](http://www.niehs.nih.gov/lsp/lspguide/1_chart.htm) The CSP is the first point of contact for most computer security issues and problems.

**Firewall Team:** CIT has a support staff that maintains the NIH network backbone firewall(s). CTB manages the NIEHS firewall. Contact your ISSO for question about firewalls.

**UNIX Information:** For technical information on UNIX security, contact Roy Reter, SCL.

**E-Mail Your ISSO at "Security - IT" from the address list.**

## Primary Security Contacts

**Information Systems Security Officer (ISSO):** The Computer Technology Branch assigns the Information Systems Security Officer (ISSO) to implement information security policies and collaborate on security issues with NIH. The ISSO is the primary contact to the NIH Incident Response Team.

**Scientific Computing Lab (SCL):** This office offers a wide variety of services for the Department of Intramural Research, DIR, and the Office of Scientific Director, OSD, communities. Roy Reter serves as their computer security contact. For more information:

<http://dir.niehs.nih.gov/dirosd/scl/programs.htm>

## Appropriate Use Policy

This policy is intended to allow the maximum flexibility possible for using NIH IT resources without compromising the integrity of NIH and/or its IT resources.

[http://www.niehs.nih.gov/compuref/policy/it\\_use.htm](http://www.niehs.nih.gov/compuref/policy/it_use.htm)

## Security Training

Practical and quick computer security advice: Very good site to get good information quickly. [http://securitynews.nih.gov/security\\_advice.html](http://securitynews.nih.gov/security_advice.html)

NIEHS Security Awareness Training: <http://www.niehs.nih.gov/compuref/security/sectrain.htm>

## Security Scan Your Own Computer!

If you would like to scan your own computer system (not applicable to Macintosh systems), any NIEHS user can access this link for a single system security scan: <https://sun1.cit.nih.gov/>

# IT Security Program

## Resource Guide



<http://www.niehs.nih.gov/isso>

**Computer Technology Branch  
National Institute of Environmental  
Health Sciences  
National Institutes of Health**

May 2002

