Illinois Department of
Innovation & Technology

Bruce Rauner, Governor
Hardik Bhatt
Secretary Designate Department of Innovation & Technology
State CIO

Department of Innovation & Technology
Acceptable Use Policy

This Acceptable Use Policy (hereafter referred to as 'AUP') specifies certain actions prohibited by Department of Innovation & Technology (hereafter referred to as 'DoIT' or 'Network') for users of the Illinois Century Network (ICN). DoIT reserves the right to modify this Policy at any time to stay in compliance with all known laws, regulations, policies, and security requirements that may be established by appropriate legislative or regulatory authorities or enacted by DoIT management. By using ICN, any customer, user that has gained access to ICN through a customer account, employee or third party (hereafter referred to as "Customer") unconditionally accepts the terms of this policy.

Authorized Use

ICN systems and services are for the use of authorized users only and are subject to routine network monitoring by DoIT staff to audit network security and performance. DoIT reserves the right to deny IP addresses or revoke IP addresses and/or deny service to any Customer violating the AUP.

Illegal Use

The ICN may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation coming to or from any network or system is prohibited. Illegal use includes, but is not limited to, material protected by copyright, trademark, trade secret or other intellectual property rights which is being used without proper authorization; government and military data protected by law and applicable national security policies and concerns; ICN data protected by public policy; and material that, in DoIT's sole discretion, is obscene, defamatory, constitutes an illegal threat, or violates export control laws or any other laws or applicable regulations, or any use which compromises the integrity of the ICN or any other network connected to the ICN.

System and Network Security

Violations of system or network security are prohibited, and may result in criminal and/or civil liability. Use of the ICN constitutes consent to DoIT' routine network monitoring. Should any violations of the law or this AUP be discovered during monitoring, DoIT will involve and cooperate with local, Illinois, and Federal law enforcement authorities for resolution.

Examples of unlawful acts, system, or network security violations include, but are not limited to, the following:

1. Unauthorized access to or use of data, systems or networks, including any attempt to probe, damage, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network. DoIT may scan or test the vulnerability of ICN systems or networks that it is responsible for or manage.
2. Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.
3. Interference with service to any user, host or network including, without limitation, email "bombing", email "spamming", flooding, deliberate attempts to overload a system, and broadcast or "smurf" attacks is prohibited.
4. Unauthorized access to any data, system, or network from a system or network for any purpose which is not lawful or which is intended to do harm.

5. Forging any part of TCP-IP packet header or header information in an email or a newsgroup posting. Electronic forging of any kind to include, but not limited to, IP addresses, domains and business names.

DoIT Definitions

1. Email "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

2. Email "spamming" is a variant of bombing; it refers to sending email to hundreds or thousands of users (or to lists that expand to that many users). It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of an incorrectly set-up responder message.

3. Flooding, or SYN floods, occurs when a target machine is flooded with TCP connection requests. The target host becomes extremely slow, crashes or hangs.

Broadcast or "smurf" attacks cause network links to become overloaded. The "smurf" attack sends a stimulus stream of ICMP echo requests “pings” to the broadcast address of a subnet.