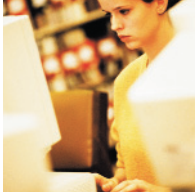


## ACCEPTABLE USE POLICY



This Acceptable Use Policy (hereafter referred to as 'AUP') specifies certain actions prohibited by the Illinois Century Network (hereafter referred to as 'ICN' or 'Network') for users of the Network. The ICN 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 ICN management. By using ICN services, any customer, employee or third party unconditionally accepts the terms of this policy.

### AUTHORIZED USE

The ICN is a publicly owned private network established by the ICN Act (20 ILCS 3921) and signed into law on June 8, 1999. ICN systems and services are for the use of authorized users only. Authorized users are subject to monitoring of all activities on ICN systems and recorded by ICN staff during routine network monitoring for the purpose of security and network performance audits. Any user of ICN systems expressly consents to such routine monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, ICN staff may provide the evidence of such monitoring to law enforcement officials. Further, if illicit activity of any kind is suspected as a result of the aforementioned routine monitoring, an internal investigation may result and employment may be suspended or terminated pending the outcome of such investigation. The ICN also reserves the right to deny IP addresses or revoke IP addresses.

### 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 unauthorized network or system is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property rights 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 ICN's sole discretion, is obscene, defamatory, constitutes an illegal threat, or violates export control laws or any other laws or applicable regulations. Any violation of the above which compromises the integrity of the ICN or any other network connected to the ICN is strictly prohibited.

### 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 network constitutes consent to ICN's routine network monitoring. Should any violations of the law or this AUP be discovered during monitoring, ICN 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. ICN employees may scan or test the vulnerability of ICN systems or networks that they are responsible for or they manage.

2. Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network. ICN employees may monitor data or traffic on any ICN network or system owned and operated by the ICN or for which the ICN is expressly responsible to manage through agreement with the owner. 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.
3. Unauthorized access to any data, system, or network from an unauthorized system or network for any purpose which is not lawful or which is intended to do harm.
4. Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting. Electronic forging of any kind to include but not limited to IP addresses, domains, business names, etc.

### ICN DEFINITIONS

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

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.

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.

Having read the ICN Acceptable Use Policy, the undersigned agrees to abide by the provisions herein. By signing this document, the undersigned acknowledges that if the provisions of the Policy are violated, the undersigned may be subject to disciplinary action or referral to the legal authorities. If disciplinary action is initiated, due process as provided by the Illinois Century Network policy will be followed. In consideration for the privilege of using the ICN and in consideration for having access to the public networks, I hereby release the ICN, its staff, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the ICN's acceptable use policy.

Institution (if applicable): \_\_\_\_\_

Printed Name: \_\_\_\_\_

Address: \_\_\_\_\_

Signature: \_\_\_\_\_

*(individual or authorized representative if an institution)*

Date: \_\_\_\_\_ Phone Number: \_\_\_\_\_

ICN Employee Location (if applicable): \_\_\_\_\_