



MILITARY DEPARTMENT OF INDIANA
JOINT FORCES HEADQUARTERS – INDIANA
ADJUTANT GENERAL'S OFFICE
2002 SOUTH HOLT ROAD
INDIANAPOLIS, INDIANA 46241-4839



Indiana Civilian Cyber Corps (ICCC)

Acceptable Use Policy

Purpose: The purpose of this policy is to outline the acceptable use of Information Technology (IT) resources and to promote the efficient, ethical, and lawful use of ICCC and/or ICCC-related IT resources. This policy addresses the responsibilities and obligations of users once access is granted. This policy is intended to protect ICCC and ICCC-related members as well as State of Indiana, partner, and client owned resources. Acceptable use is always ethical, reflects professional honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and an individual's right to privacy, freedom from intimidation, harassment, and unwarranted annoyance.

Applicability: This policy applies to all personnel granted access to ICCC and/or ICCC-related IT resources.

Policy:

1. ICCC IT resources are provided for ICCC-related activity and are to be used in a manner consistent with State of Indiana policies, regulations, and procedures, including ICCC/State of Indiana professional standards of ethical behavior.
2. Users have no right to privacy related to their use of IT Resources. Any information created or stored on IT Resources is subject to public disclosure. The State reserves the right to monitor all use of IT Resources, including email, Internet history, and Internet traffic.
3. Users must protect IT Resources from unauthorized access, theft, damage, and modification. The user must lock any State-managed device when not in use and protect State provided equipment from theft and unauthorized use when outside the office.
4. Users must protect all State-owned data and will not access or disclose information for which they have no authorization or business need.
5. The viewing, storing, or accessing of illegal content is not permitted.
6. ICCC Members will not use ICCC and/or ICCC-related IT resources to view, store, or access obscene materials, such as pornography, except when clearly required to do so in the course of their work such as may occur as part of an incident response.
7. ICCC Members will may not use ICCC and/or ICCC-related IT resources to support or oppose a candidate for public office or a ballot measure in a manner contrary to Indiana laws governing the political activities of public employees.
8. Use of ICCC IT resources, including the posting of information on ICCC-related environments, must comply with applicable copyright laws. When posting or downloading information to or from the internet, the user is responsible for ensuring that copyright law is not violated.
9. All software installed, stored, or operated on ICCC and/or ICCC-related systems must be properly licensed, whether used for educational, professional, or private use.
10. Users are not authorized to access, use, copy, modify or delete data, or grant access to others, in a manner inconsistent with ICCC and State of Indiana information security policy.
11. Users may not gain access to any files, data, or systems through the use of another user's User

Indiana Civilian Cyber Corps (ICCC) Acceptable Use Policy

ID and/or Password unless authorized to do so as part of an authorized operation or activity approved by an authorized individual.

12. Users must not share login IDs or passwords to IT Resources with other people.
13. Users may not forge or misrepresent their identity, or enable others to falsify an identity, when using ICCC and/or ICCC-related IT resources unless authorized to do so as part of an authorized operation or activity approved by an authorized individual. This type of forgery can result in criminal penalties and disciplinary action.
14. Users of ICCC and/or ICCC-related IT resources with access to personally identifiable information (PII) are responsible for the continued protection and integrity of such data.
15. Users are required to return IT Resources that have been provided to them by the State--computers, mobile phones, and all other devices--no later than at the time of their separation. Failure to return IT Resources will be viewed as theft and addressed accordingly.
16. Users must report known or suspected violations of this agreement to their supervisor.

Agreement:

The system being accessed is a Federal, State, Municipal, or (Other) _____ resource restricted to authorized personnel. Unauthorized access or use of this system is strictly prohibited and closely monitored. Usage is governed by and subject to United States and Indiana laws and policies. There is no expectation of privacy with respect to material placed on or viewed by the system with exception to specific status or statutes. In accordance with Federal and State laws, monitoring may result in acquisition, recording, and analysis of any and all data communicated, transmitted, processed or stored on the system. Anyone using this resource including any devices attached to this system consents to the items listed above, but not limited to, and does so in accordance and with the understanding of being subject to administrative action, civil and criminal penalties.

I understand that my failure to abide by this Acceptable Use Policy may result in initiation of civil actions or penalties up to and including initiation of an investigation, or referral of criminal charges under the Uniform Code of Military Justice (UCMJ), per Indiana Code 10-16-6-10.

I, _____ (Full Legal Name), enter into this agreement freely and without reservation, hereby affirming that I have read, understand, and comply with the acceptable use policy as provided above.

Member Signature: _____

Date: _____

Signature Witnessed by:

Full Legal Name: _____

Signature: _____

Date: _____