Acceptable Use Policy

1 OVERVIEW

As State of Illinois employees, we have access to State information and State systems, technology and other information resources, including State-owned hardware, software, and computer network access. This Policy refers to all such information, data, systems, technology, and resources collectively as "Information Technology Resources (IT Resources)". As stewards of IT Resources, each of us is responsible for protecting those resources.

Inappropriate use exposes the State and its agencies to risks including cyber-attacks, compromise of network systems and services, information breaches and legal issues. Inappropriate personal use of IT Resources on State time also deprives the State of another valuable resource – your time and service.

To avoid these problems, every employee who accesses IT Resources (Users) must know and understand the following guidelines and conduct their activities accordingly.

2 GOAL

The goal of this Acceptable Use Policy is to establish appropriate and acceptable practices and responsibilities regarding the use of IT Resources, which will protect proprietary, personal, privileged, or otherwise sensitive data.

3 SCOPE

This Acceptable Use Policy requires statewide compliance, and it covers and applies to:

- All State agencies, boards, commissions, IT service providers, and any other entities that use IT Resources;
- All personnel, employees, and contractors, of the Illinois Department of Innovation & Technology ("DoIT"), and of all State agencies, boards and commissions that use IT Resources. All such personnel are referred to as a "User" or "Users" in this policy;
- All IT Resources, including systems and technology capabilities developed, acquired, or used as a service, whether the IT Resource is internally or externally developed, housed or maintained.

This policy establishes minimum guidelines for acceptable use. A User's agency policy may be more restrictive, and to that extent will supersede the minimum requirements of this policy.

4 REQUIREMENTS

4.1 General Use and Ownership

4.1.1 Every User must avoid all activity that compromises the security, performance or integrity of IT Resources, or that negatively impacts the IT Resources or other Users.

4.1.2 State employees, vendors, business partners, and other governmental agencies must first be authorized by DoIT or client agency designated staff before accessing IT Resources.

4.1.3 All individuals who access IT Resources may be required to undergo personnel screening. Such screening could include a background check, which shall be proportional to the data classification, business requirements, and acceptable risk, each based on the IT Resources being accessed.

4.1.4 Users must use IT Resources within the scope of their employment or contractual relationship with the State only, and must agree to abide by the terms of this policy. Such agreement will be evidenced by the User's acceptance of the terms and conditions of this policy.

4.1.5 Users shall promptly report to their supervisor and/or the service desk all security incidents, disruption of service, actual or suspected theft, loss and/or unauthorized disclosure of IT Resources.

4.1.6 The State audits IT Resources to secure its information systems and ensure compliance with this policy.

4.1.7 Limited, reasonable personal use of State Network Resources, in accordance with this Policy, is allowed. Users should be aware that all usage may be monitored and there is no reasonable expectation of privacy in the use of IT Resources.

4.2 Security and Information

4.2.1 All Users must undergo Cybersecurity Awareness Training, pursuant to 20 ILCS 450/25.

4.2.2 Users may access, use or share IT Resources only to the extent necessary to fulfill assigned job duties. All IT Resources must be handled with due care and confidentiality. Users who create, receive, process, edit, store, distribute or destroy IT Resources which are confidential, sensitive in nature, and/or governed by federal or state laws, rules or regulations must understand their responsibilities to protect such information.

4.2.3 All computing devices, which include personally owned devices, that connect to the State of Illinois internal network must first be authorized.

4.2.4 System and user level passwords must meet DoIT's password length and complexity requirements.

4.2.5 Use of another User's password or any other authentication capabilities is strictly prohibited.

4.2.6 User privileges must not be elevated without formal approval by authorized personnel.

4.2.7 Technical personnel must utilize accounts specified for elevated privileges.

4.2.8 Computing devices must be secured with a password-protected screensaver enabled, as applicable. Users must lock the screen or log off/sign out of the device when the device is unattended.

4.2.9 Users must use caution when opening e-mail attachments received from unknown senders, as attachments may contain malware. Users must also use caution when clicking on hyperlinks in email, as this could result in a successful cyber-attack.

4.3 Unacceptable Use

The following activities are prohibited. State Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access if it is disrupting production services).

Under no circumstances should any State resource be used to engage in any illegal activity.

The examples listed below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.3.1 Prohibited System and Network Activities

4.3.1.1 Violations of any copyright, trade secret, patent or other intellectual property, or any similar laws or regulations. This includes, but is not limited to, the installation or distribution of "pirated" or any other software products that are not licensed for use by the State.

4.3.1.2 Unauthorized copying, sharing and/or distribution of copyrighted material.

4.3.1.3 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate

management should be consulted prior to export of any material.

4.3.1.4 Careless introduction of malicious programs into the network or server (*e.g.*, viruses, worms, Trojan horses, and e-mail bombs).

4.3.1.5 Revealing your account password to others or allowing others to use your account. This includes family and other household members. If the User losses control of their credentials they should report this to the helpdesk or their appropriate IT or Security staff and immediately change their network/email password.

4.3.1.6 Using IT Resources to obtain or transmit material that is in violation of sexual harassment or hostile workplace laws in the User's local jurisdiction, including but not limited to publishing, distributing, selling, displaying, possessing obscene materials such as pornography, child pornography, cyberbullying and threats of violence.

4.3.1.7 Effecting security breaches or disruptions of network communication.

4.3.1.8 Port scanning or security scanning is expressly prohibited unless prior notification to DoIT Division of Information Security is made. Security scanning conducted by or with express authorization from the Chief Information Security Officer ("CISO") is excluded from this prohibition.

4.3.1.9 Executing any form of network monitoring that will intercept data not intended for the User's host, unless this monitoring activity is a part of the User's normal job/duty.

4.3.1.10 Circumventing User authentication or security features of any host, network or account.

4.3.1.11 Installing password crackers, denial of service tools, key loggers or any other software or tools designed to acquire unauthorized access to data or IT Resources. Use of such tools can be acceptable, but only with express authorization from the CISO.

4.3.1.12 Utilizing tools such as unauthorized browsers to access the 'dark web' unless expressly authorized by the CISO.

4.3.1.13 Introducing honeypots, honeynets, or similar technology on the State network unless expressly authorized by the CISO.

4.3.1.14 Interfering with or denying service to any User (for example, a denial of service attack).

4.3.1.15 Using any program/script/command, or sending messages of any kind, with

the intent to interfere with, or disable, a User's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.3.1.16 Providing information about, or lists of, State employees to parties outside of State established processes.

4.3.1.17 Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation, or which may compromise the security of the State, IT Resources, and/or DoIT Client Agencies.

4.3.1.18 Installing software that has not been authorized in writing by the requestor's manager and an appropriate service request submitted to designated IT staff or Help Desk for processing.

4.3.1.19 Attaching devices that have not been authorized in writing by the requestor's manager and then submit appropriate service request to designated IT staff or Help Desk for processing.

4.3.1.20 Using IT Resources to play or download games, music or videos that are not in support of business functions.

4.3.1.21 Using peer-to-peer or file sharing software must be authorized by the CISO.

4.3.1.22 Utilizing IT Resources for activities that violate policies established by State agencies, boards or commissions.

4.3.1.23 Moving, adding, or altering the security and/or security-related configurations of State owned workstations, mobile devices, network equipment, software or services.

4.3.1.24 Sharing or storing IT Resources via unauthorized cloud services.

4.3.2 Prohibited Email and Communication Activities

The purpose of the State's e-mail system is for correspondence relating to the mission of the agency, board or commission. E-mail is a resource provided to agencies, boards and commissions, and Users to enhance work performance and productivity, enable efficient communication, and to record and preserve the work performed in accordance with State law. The following are prohibited activities:

4.3.2.1 Sending "junk mail" or advertising material to individuals who did not specifically request such material (email spam).

4.3.2.2 Any form of harassment via email, telephone, or instant messaging.

4.3.2.3 Unauthorized use, or forging, of email header information.

4.3.2.4 Solicitation of email for any other email address (other than that of the poster's account), with the intent to harass or to collect replies.

4.3.2.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.3.2.6 Sending unsolicited email from within the State networks.

4.3.2.7 Users are not allowed to create or open archived .PST files unless first authorized in writing by the requestor's manager and then submit appropriate service request to designated IT staff or Help Desk for processing.

4.3.2.8 The Enterprise email system includes a disclaimer notification at the bottom of every email sent from the system. Additional disclaimers must be approved by the User's agency senior management or their legal department.

4.3.2.9 Sending broadcast messages to all agency email Users within the scope of the Enterprise Email system without appropriate authorization.

4.3.2.10 Misaddressed messages shall not be forwarded unless the User is familiar with both the sender and the recipient, and knows the message pertains to legitimate State business. In all other instances the sender should be notified, if possible, that the message was misaddressed or misdirected and the email deleted.

4.3.2.11 Users may not create email rules or other automated processes to forward any email to external email accounts; personal or otherwise. This includes carbon copying to personal accounts.

4.3.2.12 Users cannot retain or export a copy of email when terminating employment with the agency unless authorized by agency senior management or agency legal department.

4.3.3 Prohibited Activities When Using Collaboration Tools (Audio, Video, File Sharing, Group Chat, Remote tools and Online Meeting tools):

4.3.3.1 Using collaboration resources for monetary gain or for commercial, religious, or political purposes not directly related to State business.

4.3.3.2 Capturing, opening, intercepting or obtaining access to collaboration tools, except as otherwise permitted in the performance of assigned job responsibilities.

4.3.3.3 Giving the impression to others that the User is representing, giving opinions or otherwise making statements on behalf of DoIT, unless in the performance

of assigned job responsibilities.

4.3.3.4 Users will not directly or by implication employ a false identity.

4.3.4 Prohibited Blogging and Social Media Activities

4.3.4.1. Nothing in this Policy is intended to interfere with, restrain, or impinge upon any User's Constitutional rights, nor upon communications regarding wages, hours, or other terms and conditions of employment. Users have the right to engage in or refrain from such activities in accordance with any other applicable statues, rules, regulations or policies.

4.3.4.2. Users are prohibited from making comments or otherwise communicating about customers, residents, vendors, suppliers, coworkers, or supervisors in a manner that is vulgar, obscene, threatening, intimidating, harassing, libelous, or discriminatory on any grounds.

4.3.4.3. Privacy and confidential information requirements also apply to blogging and social media activities. As such, Users are prohibited from revealing any private, confidential or proprietary information, trade secrets or any other material protected from disclosure by applicable statutes, rules, standards, contracts and policies when engaged in blogging and/or social media activities.

4.3.4.4. When using social media in a non-official, or personal capacity:

- Users who identify themselves as a State employee or have a public-facing position should ensure their profile and related content conforms to applicable requirements, such as (but not limited to) the State Officials and Employees Ethics Act (5 ILCS 430).
- Users should add a disclaimer to their social networking profile, personal blog, or other online presences that clearly state that the opinions or views expressed are the User's alone, and do not represent the views of the User's employing agency or the State.
- In a publicly accessible forum, Users shall not discuss any agency or State-related information that is not already considered public information. The discussion of sensitive, proprietary, or confidential information is strictly prohibited. This rule applies even in circumstances where password or other privacy controls are implemented.

4.3.4.5. Users must comply with all applicable laws regarding trademarks, logos, intellectual property, rights of publicity, and any other third-party rights. Users

may not infringe on State-owned trademarks, logos, intellectual property, or rights of publicity.

4.4 Internet Access

Internet access is provided to meet informational needs and support the mission and goals of the State. All Internet usage utilizing IT Resources falls under this Acceptable Use Policy, regardless of equipment ownership. Misuse of Internet access may result in loss of Internet access privileges, or discipline, up to and including discharge.

Internet use is monitored by the State. Suspected misuse of the Internet should be reported to the applicable DoIT Client Agency for review and determination of appropriateaction.

5 POLICY COMPLIANCE

In order to implement this Policy, DoIT may establish supplemental policies, standards, procedures and guidelines and designate responsibility to specific personnel. To the extent necessary, each Client Agency and/or DoIT Division must establish procedures to achieve Policy compliance. It is the responsibility of all Users to understand and adhere to this Policy.

The DoIT Division of Information Security will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Policy owner.

All Users of DoIT and DoIT client agencies are required to complete the Ethics Training Program and Cyber Security Awareness training as part of the initial training for new users and annually thereafter. Any break in service, as defined by governing HR policy, will require retraining.

Any exception to this Policy must be approved by the DoIT Division of Information Security in writing and in advance of any action otherwise contrary to this Policy.

Failure to comply with this Policy may result in the CISO, or designee, temporarily discontinuing or suspending the operation of the information system, access, solution and/or resource until such compliance is established by the CISO or designee. Failure to comply with this Policy could also result in discipline, up to and including discharge.

Noncompliance with this Policy may constitute a legal risk to the State, an organizational risk to the State in terms of potential harm to employees or resident security, or a security risk to State Network Operations and the user community, and/or a potential personal liability.

The
presence of unauthorized data in the State network could lead to liability on the part of the State, in addition to the individuals responsible for obtaining it.

6 APPLICABLE LAWS, GUIDELINES OR SOURCES

Applicable laws, rules and regulations include, but are not limited to, those found in the State Enterprise Information Security Policy, and the State Officials and Employees Ethics Act, 5 ILCS 430 and 20 ILCS 450/25.

7 RELATED POLICIES, STANDARDS AND GUIDELINES

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

CERTIFICATION

I have been issued a copy of the Department of Innovation & Technology Acceptable Use Policy. I understand that compliance with the State's policies and regulations is a condition of employment and that it is my obligation to read, understand, and remain current with any new or amended policy, rule, directive or regulation. I further understand that a violation of any State policy, rule, directive or regulation may result in disciplinary action, up to and including discharge.

[Please sign below]

Signature **Date**

I UNDERSTAND THAT NO STATEMENT IN THIS POLICY SUPERSEDES THE PERSONNEL CODE OR ANY NEGOTIATED CONTRACT, NOR DOES THIS POLICY CONSTITUTE OR IMPLY ANY CONTRACTUAL OBLIGATIONS.

IT IS THE RESPONSIBILITY OF EACH EMPLOYEE TO COMPLETE THIS CERTIFICATION AND RETURN IT TO HIS OR HER IMMEDIATE SUPERVISOR. THE SUPERVISOR MUST FORWARD THE COMPLETED FORM TO THE PERSONNEL OFFICE FOR INCLUSION IN THE EMPLOYEE'S OFFICIAL PERSONNEL FILE.

PUBLICATION APPROVAL FORM

Publication Name(s):	Version #(s):
Acceptable Use Policy	03/22/2022
Overarching Enterprise Information Security Policy	03/22/2022

PROCESS, PROCEDURE, & STANDARD PUBLICATIONS

	Print Name	*Signature*	*Date*
APPROVER	Adam Ford		3/22/2022

Instructions:

1. **Complete signature process**
2. **Digitally scan signed Publication Approval Form**
3. **E-mail pdf version of Publication Approval Form and WORD version of document to:**
   DoIT.EUC.SVCMGMT@Illinois.Gov