STATE OF TENNESSEE

Acceptable Use Policy
State of Tennessee Information Technology Resources

Purpose:
The purpose of this policy is to outline the acceptable uses of State Information Technology (IT) resources for the State of Tennessee. The policy outlines the standards and constraints for acceptable use of State IT resources, regardless of hosting location, which means all equipment, networks, hardware, software, data, technical knowledge, expertise and other resources including, but not limited to, computing equipment, phones, end-user and application software and telecommunications equipment whether owned, leased or otherwise provided by the State. This policy is in place to protect both the users of State IT resources and the State of Tennessee. Inappropriate use exposes the State to many risks including non-compliance with local, state and federal laws, rules and policies, violation of contracts and licenses, and compromise of State IT resources.

References:
Tennessee Code Annotated, Section 4-3-5501, et seq., effective July 1, 2015.
Tennessee Code Annotated, Section 10-7-504(i), effective May 30, 2001.
Tennessee Code Annotated, Section *10-7-512, effective May 27, 1999.*
Information Systems Council Policies
State of Tennessee Enterprise Information Security Policies.

Objectives:
- Ensure the confidentiality, integrity and availability of State IT resources that may be processed in any manner by the State or any agent of the State.
- Ensure proper usage of State IT resources.
- Prevent access to State IT resources from unauthorized users or unauthorized access or unauthorized use.
- Inform users there is no expectation of or right to privacy in their use of State IT resources.
- Prevent individuals from using State IT resources to obtain anything of value to which those individuals are not entitled.
- Prevent individuals from wrongfully or improperly using or harming State IT resources.

Scope:
This Acceptable Use Policy applies to all users who have been provided access rights to the State of Tennessee IT resources, State provided email, and/or Internet via agency issued network or system User ID's. This Policy applies to all government branches of the State of Tennessee pursuant to *Tennessee Code Annotated, Section 4-3-5501, et seq.* and the Information Systems Council policies. Each branch, department, agency or political subdivision of the State can create its own policy, but it must be at least as restrictive as this policy.

Use and Prohibitions:

A. Information Technology Resources
State employees, vendors/business partners/subrecipients, local governments, and other governmental agencies may be authorized to access State IT resources to perform business functions with or on behalf of the State. Any user of State IT resources must act within the scope of his/her employment or contractual relationship with the State and must agree to abide by the terms of this agreement as evidenced by his/her signature. Transactions resulting from any activity using State IT resources are the property of the State and are thus subject to open records laws.

A public record is defined as follows:

> *"Public record(s)" or "state record(s)" means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. (Tennessee Code Annotated, § 10-7-301(6)).*

State records are open to public inspection unless they are protected by State or Federal law, rule or regulation and include, but are not limited to, draft letters, working drafts of reports, and what are intended to be casual comments. Be aware that anything sent as electronic mail could be requested to be made available to the public.

Prohibitions

- Accessing, viewing, copying, sending, sharing and/or selling any information that is confidential by law, rule or regulation, or not otherwise available, without proper authorization.
- Utilizing or installing unauthorized or unlicensed software on State IT resources.
- Leveraging IT resources that have not been authorized by Department of Finance and Administration, Strategic Technology Solutions.
- Using State IT resources to play or download games, music or videos that are not in support of business functions.
- Leaving workstation unattended without engaging password protection for the keyboard or workstation.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using State IT resources in support of unlawful activities.
- Utilizing State IT resources for activities that violate policies.

- Storing non-State data on State IT resources including, but not limited to, pictures and videos.

B. Email

Email and calendar functions are provided to expedite and improve communications among IT resources users.

Prohibitions

- Sending unsolicited junk email or chain letters (e.g. “spam”) to any users of the network.
- Sending any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or malicious programs.
- Sending copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher.
- Sending or receiving communications that violate policies established by the Department of Human Resources or the agency where the user is employed or under contract.
- Sending confidential material to an unauthorized recipient or sending confidential e-mail without the proper security standards (including encryption if necessary) being met.

Email created, sent or received in conjunction with the transaction of official business are public records in accordance with Tennessee Code Annotated, §§ 10-7-301 through 10-7-308, and the rules of the Public Records Commission.

C. Internet Access

Internet access is provided to State IT resources users to assist them in performing the duties and responsibilities associated with their positions.

Prohibitions

- Using the Internet to access non-State provided web email services.
- Using the Internet for non-State approved business purposes.
- Using the Internet for un-approved offsite storage.
- Using the Internet when it violates any federal, state or local law.

D. Endpoint

Endpoint devices are provided to IT resources users to facilitate work efforts and to provide access to additional State IT resources and services.

Prohibitions

- Concealing or masking identity to hide activity.
- Removing or deactivating monitoring or logging software.
- Taking any action to circumvent security controls or administrative support or maintenance.
- Creating accounts that have not been authorized.
- Running unauthorized software or scripts.

- Accessing IT resources for purposes other than those for which the access was granted.
- Taking actions to hide files.

Statement of Consequences
Noncompliance with this policy may constitute a legal risk to the State of Tennessee, an organizational risk to the State of Tennessee in terms of potential harm to employees or citizen security, a security risk to the State of Tennessee's IT resources and the user community, a privacy risk to State of Tennessee assets and/or potential personal liability. The presence of unauthorized data on State IT resources could lead to liability on the part of the State as well as the individuals responsible for obtaining it.

Statement of Enforcement
Noncompliance with this policy may result in the following immediate actions:

- Written notification will be sent to the head of the appropriate agency and to designated points of contact in the human resources office and the IT resources office in the agency where the user is employed to identify the user and the nature of the noncompliance. In the case of a vendor, subrecipient, or contractor, the contract administrator will be notified.
- User access may be terminated immediately, and the user may be subject to subsequent review and action as determined by the agency, department, board, commission leadership, contract administrator or other appropriate authority.

Personal Incidental Usage
Users may make calls, use the Internet, and send and receive emails for incidental and occasional personal use provided that such use does not:

- Violate any laws, rules, regulations or policies.
- Disrupt, distract from, or interfere with State business.
- Constitute private business activities.
- Contravene supervisor direction regarding personal use of State IT resources.

Users may not obtain or use data obtained as a result of or through their position as a user for personal purposes. Users should be aware that all usage may be monitored and that there is no expectation of or right to privacy.

It is not a violation of this policy to obtain and use data pursuant to the Tennessee Public Records Act.

Review of this document takes place within the STS Policy Review Committee sessions and will occur on an annual (within every three hundred and sixty-five (365) days) basis at a minimum.

STATE OF TENNESSEE

Acceptable Use Policy
State of Tennessee Information Technology Resources
User Agreement Acknowledgement

As a user of State of Tennessee IT resources, I agree to abide by the State of Tennessee Acceptable Use Information Technology Resources Policy and the following promises and guidelines as they relate to the policy established:

1. I will protect State IT resources against unauthorized disclosure and/or use.
2. I will maintain all computer access credentials in the strictest of confidence; immediately change them if I suspect their secrecy has been compromised and will report activity that is contrary to the provisions of this agreement to my supervisor and to the office of the Chief Information Security Officer.
3. I will be accountable for all transactions performed using my computer access credentials.
4. I will not disclose any confidential information other than to persons authorized to access such information as identified by state or federal laws, regulations or policies
5. I will not obtain or use data obtained as a result of or through my position as a user for personal purposes.
6. I agree to report to Strategic Technology Solutions Customer Care Center, any suspicious network activity or security breach.

Privacy Expectations

The State of Tennessee monitors State IT resources, including, but not limited to, real time monitoring. Users have no expectation of or right to privacy. All transactions and communications are considered to be State property and may be examined by management for any reason including, but not limited to, security and/or employee conduct.

I acknowledge that I must adhere to this policy as a condition for receiving access to State of Tennessee IT resources.

I understand the violation or disregard of this policy may result in my loss of access and disciplinary action, up to and including termination of my employment, termination of my business relationship with the State of Tennessee, and any other appropriate legal action, including possible prosecution under the provisions of the Tennessee Personal and Commercial Computer Act of 2003 as cited at Tennessee Code Annotated, § 39-14-601 et seq., and other applicable laws.

I have read and agree to comply with the policy set forth herein.

EMPLOYEE

_____	_____
Type or Print Name	Edison Employee ID
_____	_____
Signature *	Date

NON-STATE EMPLOYEE

_____	_____
Type or Print Name	Vendor ID
_____	_____
Signature	Date

* By acknowledging this policy via the Edison system, I agree that my acknowledgement is the equivalent to my handwritten signature