Acceptable Use of TennCare Resources Policy

v4.0 – August 11, 2023

Policy Name:	**Acceptable Use Policy**	**Revision #:**	**4.0**
Supersedes:	**State of Tennessee Bureau of TennCare Acceptable Use Policy: Rules of Behavior, Network Access Rights and Obligations Rev 9/29/2020**		
Approved by (signature):			
Date:	**August 11, 2023**		
Approved by (Name):	**Lauren Davidson**		
Approver (title):	**Chief Information Security Officer (CISO)**		
Effective Date:	April 1, 2022		

Document Information

Revision History

Version	Author	Date	Comment
2.1	Kris Goins, KPMG	2/14/2022	Updated full document per State request
3.1	Ngozi Onukogu/Scott Monfort	7/27/2023	Annual review, update, and addition of CJIS information

Review and Approval History

Name	Organizational Role	Date	Reviewed/Approved
Lauren Davidson	TennCare CISO	4/1/2022	Approved – version 3.0
Lauren Davidson	TennCare CISO	8/11/2023	Approved – version 4.0

Table of Contents

1. Introduction

The TennCare Acceptable Use Policy (AUP) describes the requirements and defines the authorized actions that may be performed when accessing the State of Tennessee and TennCare resources and data.

It is the TennCare user's responsibility to read, understand, and conduct their activities in accordance with this policy.

For the purposes of this policy, State and TennCare terms shall mean both TennCare specific resources as well as resources managed on TennCare's behalf by the State of Tennessee or its contractors. Resources shall be defined as IT equipment, devices, computer systems, appliances, scripts, bots, emails, internet, phone, fax, voicemail, infrastructure, TennCare data, software, and hardware whether owned or managed by the State, TennCare or third parties on behalf of the State or TennCare.

2. Purpose

The purpose of this policy is to establish the appropriate and acceptable behaviors regarding the use of TennCare information resources and to educate personnel on their responsibilities when accessing information systems data.

3. Scope

This policy applies to all TennCare employees, consultants, contractors, and other persons who are under the direct or indirect control of and who access State of Tennessee and TennCare networks, systems, devices, data, or facilities.

4. Policy

4.1 Acceptable Uses and Behaviors

TennCare information system resources are intended to be used in support of official TennCare business and users of these information resources shall exercise good security practices to ensure the protection of TennCare information systems and data.

Acceptable uses and behaviors include, but are not limited to the following:

- Access and use State and TennCare technology resources and data that they are authorized to access and that are necessary for conducting the business tasks assigned to them.
- Report harmful events or policy violations involving TennCare assets or information to TennCare management, a member of the TennCare Security Team, or a member of the Cyber Security Incident Response Team (CSIRT) without unreasonable delay and **no later than within one (1) hour of occurrence/discovery**. Events include but are not limited to, the following:
    - Technology incident
    - Data incident
    - Unauthorized access incident
    - Facility security incident

    - Policy Violation
- Use a secure printer to print sensitive materials.
- Secure sensitive documents and storage media in a locked cabinet.
- Maintain the confidentiality of personal authentication information.
- Ensure user account passwords are not shared with others.
- Immediately change a password if the security of the account is ever in doubt.
- Activate a password-protected screensaver whenever leaving a TennCare computer unattended.
- Log off, lock, and secure workstations, laptops, and sensitive data when the workstation is unattended.
- Log off from applications or the TennCare network when they are no longer needed.
- Challenge unauthorized personnel who may not be following procedures for visitor sign-in, appropriate badge use, escort control or entry into TennCare facilities.
- Complete all mandatory training (e.g., security and privacy awareness, role-based training, etc.) prior to accessing TennCare systems and periodically thereafter as required by TennCare policies.

4.2 Unacceptable Use

The following list is not intended to be exhaustive and is a framework for activities that constitute unacceptable use of TennCare information and TennCare information resources.

Unacceptable use includes, but is not limited to the following:

- Unauthorized use or disclosure of TennCare information and TennCare information system resources.
- Knowingly or willingly concealing, removing, mutilating, obliterating, falsifying, or destroying TennCare information.
- Sending personal, private, sensitive, or confidential information, including Personally Identifiable Information (PII), Federal Tax Information (FTI), Protected Health Information (PHI), FBI Criminal Justice Information (CJI), and Social Security Administration information (SSA), to an unauthorized recipient or sending sensitive email without the proper security standards being met.
- Connecting unapproved devices to TennCare's network or any TennCare information resources.
- Connecting TennCare information resources to unauthorized networks.
- Installing, downloading, or running software that has not been approved in accordance with TennCare policies.
- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate.
- Sending or receiving communications that violate policies established by TennCare.
- Using network resources to play or download games, music, or videos that are not in support of business functions.
- Connecting to commercial/web email systems for personal use.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and

unwanted email content using TennCare information resources.
- Tampering, disengaging, or otherwise circumventing TennCare or third-party information technology security controls.
- Accessing or attempting to access data outside of assigned job duties or divulging such information to unauthorized parties.
- Unauthorized use or disclosure of personal, private, sensitive, or confidential information.
- Using Instant Messaging or Internet Relay Chat (IRC) or messaging services if not the provided by the State and TennCare.
- Using the internet in any way that violates Federal, State, or local law.
- Using TennCare information or TennCare information resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity.

4.3 Limited Personal Use

TennCare information resources are intended for business use only. Limited personal use of TennCare information resources is permitted provided such use:

- Is otherwise consistent with this policy.
- Is limited in amount and duration.
- Does not result in direct costs to TennCare.
- Does not impede the ability of the individual or other users to fulfill their duties and responsibilities to TennCare.

Users of TennCare information technology should have NO expectation of privacy. All information located on TennCare information technology resources is owned by TennCare and may be subject to open records requests and may be accessed in accordance with the Tennessee Public Records Act under Tennessee Code Annotated (TCA) 10-7-101 et seq.

4.4 Restrictions to Off-Site Transmission and Storage of Information

TennCare information technology users must not transmit restricted TennCare, non-public, personal, private, sensitive, or confidential information, to include PII, FTI, PHI, CJI, and SSA, to or from personal email accounts or use a personal email account to conduct the organization's business unless explicitly authorized.

TennCare users must not store restricted TennCare, non-public, personal, private, sensitive, or confidential information, to include PII, FTI, PHI, CJI, and SSA, on a non-TennCare issued device, or with a third-party file storage service that has not been approved.

Devices that contain TennCare information must always be attended to or physically secured and must not be checked in transportation carrier luggage systems.

4.5 Accessing Social Media and other Networking Sites

TennCare information technology users are prohibited from accessing social networking sites such as Facebook, Twitter, Instagram, LinkedIn, as well as video-hosting sites such as YouTube and Tik-Tok on TennCare information system resources without prior authorization. Sharing, storing, or disclosing sensitive information with third-party organizations and/or using third-party applications

(e.g., DropBox, Evernote, iCloud, etc.) unless authorized and with formal agreement in accordance with TennCare policies is prohibited.

5. Compliance

Compliance is required with all TennCare policies, procedures, standards, and guidelines. If requirements or responsibilities are unclear, seek assistance from your supervisor or the TennCare Information Security and Privacy Offices.

Noncompliance with this policy may result in the following:

- Written notification will be sent to designated TennCare managers and points of contact in the user agency's Human Resources and Information Systems Offices to identify the user and the nature of the noncompliance as "cause."
    - In the case of a vendor, sub-recipient, or contractor, the contract administrator will be notified.
- User access may be terminated immediately by the Chief Information Security Officer (CISO) or a Systems Administrator. The user may be subject to subsequent review and action as determined by the agency, department, board, or commission leadership, or contract administrator.

6. References

The following documents contain additional guidance in the appropriate use of TennCare information technology resources:

- TennCare Information Security Access Control Policy
- TennCare Information Security Configuration Management Policy
- TennCare Information Security Personnel Security Policy
- TennCare Information Security System and Information Integrity Policy
- IRS 1075 (version 11-2021)
- FBI Criminal Justice Information Services (CJIS) Security Policy

7. Acknowledgment of Policy

All users of TennCare information system resources must acknowledge, in writing, that they have received a copy of this policy. Written acknowledgement will be required by all users of TennCare information system resources on an annual basis.

I have read, understand, and will abide by the above Acceptable Use Policy when using a computer and other electronic resources owned, leased, or operated by TennCare and the State of Tennessee. I further understand that I have no expectation of privacy when connecting any device to the Tennessee Wide Area Network and that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation of this policy, my access privileges may be revoked, and disciplinary action may be taken, 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 Computer Crimes Act as cited at TCA 39-14-601 et seq., and other applicable laws.

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

Signature: _____

Print Name: _____

Title: _____

Date: _____

TennCare User ID (if provided): _____

TennCare Division
or Company Name: _____

Create Verification PIN (4 digit): _____

If an Organization or Trading Partner account:
I further agree that as a designated representative for the Organization, all documentation is being adequately maintained for all individuals accessing TennCare systems demonstrating awareness of this Acceptable Use Policy.

- Tax ID: _____