Time Clock Standard

Introduction

Research found the time clock systems are a logical inclusion in the State of Oklahoma's digital transformation to gain efficiency in use of government resources. The time clock systems fit with disseminated staffing models and automation.

Purpose

This document establishes a technical standard for State of Oklahoma agencies and partners requiring a time clock system. This tool is necessary for agencies, partners and vendors that plan, architect, design, implement or manage a time clock system including collection devices and application.

Definitions

EU-US privacy shield – The EU-US framework was designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic Ocean with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

FedRAMP – The Federal Risk and Authorization Management Program is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

ISO – The International Organization for Standardization is an international standard-setting body composed of representatives from various national standards organizations.

IVR – Interactive voice response is a technology that allows humans to interact with a computer-operated phone system using voice and tones input via the keypad.

NIST – National Institute of Standards and Technology. NIST's goal is to help businesses and organizations secure information that is sensitive but not classified.

RFID – Radio frequency identification is a technology that uses radio waves to passively identify a tagged object.

SOC 2 Type II – An internal controls report capturing how a company safeguards customer data and how well those controls are operating.

Standard

TimeClock Plus is the standard for State of Oklahoma agencies and partners:

- SOC 2 Type II certified and maintains compliance with the EU-US privacy shield. Services are housed in the US with cloud infrastructure provider, Amazon Web Services. All TimeClock Plus infrastructure providers are SOC 2 Type II, ISO, NIST and FedRAMP authorized and maintain facilities secured against electronic and physical intrusion.
- Supports a diverse workforce by offering time collection from a variety of sources, including a pc/web browser, fixed-mount time collection devices, mobile applications and

an IVR phone-in system. These options offer flexibility in deployment and will support a variety of time capture priorities.
    - Speed (card swipe: magnetic, bar code and proximity/RFID card readers).
    - Accessibility (WebClock browser access).
    - Validation (biometric fingerprint or hand scanner readers).
    - Remote access (mobile clock with geo-fencing and offline time collection).
- Adheres to the policies and standards defined by the HCM division when implemented for entities utilizing the state standard HCM application.

Quality of service for the TimeClock Plus product is managed through a service level agreement with the vendor and the oversight is from an OMES contract monitor.

Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 03/21/2022	**Review cycle:** Annual
Last revised: 03/21/2022	**Last reviewed:** 07/13/2023
Approved by: Joe McIntosh, Chief Information Officer	