ROOSEVELT UNIVERSITY

RU Policy No. 2.18

Responsible Division: Human Resources

Originally Issued: 02/2020

Last Revised: 02/2020

Revised Effective Date: 02/2020

Finger-Scanning Technology Policy and Procedure

Policy Statement

To efficiently and securely track its employees' time records and for employee identification purposes, Roosevelt University (the "University") uses a timekeeping system that uses finger- or hand-scanning technology for identification. These timeclocks convert a scan of the employee's fingerprint, fingertip, and/or handprint ("finger scan") into an encrypted mathematical representation. Only the mathematical representation created from the finger scan performed during enrollment is saved. The technology does not collect and store fingerprints or handprints, nor does it retain such images. As such, the University believes the system does not collect, capture, or store a biometric identifier or biometric information as those terms are defined in the Illinois Biometric Information Privacy Act. Nevertheless, the University has elected to publish this Policy and Procedure.

The University reserves the right to modify or amend this Policy at any time, at its sole discretion. Any change to this Policy will become effective at the time designated above. This Policy does not constitute an express or implied contract between Roosevelt University and any past, present, or prospective student, employee (including administrator, faculty, or staff), contractor, or volunteer.

This Policy governs conduct on all of the University's properties, including but not limited to the Auditorium Theatre of Roosevelt University ("ATRU"). Unless otherwise stated, the following definitions shall apply to this Policy:

- "**Biometric identifier**" shall refer to the retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry belonging to an Employee.

- "**Biometric information**" shall refer to any information, regardless of how it is captured, converted, stored, or shared, based on an Employee's biometric identifier used to identify an Employee.

"**Employee**" shall refer to all employees (including administrators, faculty, and staff), contractors, and volunteers.

Policy

Purpose: The University utilizes the timekeeping system described herein for Employee identity verification and time entry purpose in compliance with federal and state wage and hour laws.

Description of the Timekeeping System: The University uses a timekeeping system that uses finger- or hand-scanning technology for identification. These timeclocks convert a scan of the employee's fingerprint, fingertip, and/or handprint ("finger scan") into an encrypted mathematical representation. Only the mathematical representation created from the finger scan performed during enrollment is saved. This technology does not collect and store fingerprints, nor does it retain fingertip images. As such, the University believes the system does not collect, capture or store a biometric identifier or biometric information as those terms are defined in the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* Nevertheless, the University has elected to provide this Policy and Procedure, along with a Written Release. The University shares timekeeping data with its payroll vendor for the purpose of processing payroll and issuing paychecks. Data may also be shared with a vendor that maintains, updates, fixes, or troubleshoots the timeclock.

Consent: Employees are required to use finger-scanners included in the timekeeping system as a condition of employment and to consent to the collection of the finger-scan mathematical representation by this system. This Consent shall be provided in the Finger-Scanning Technology Written Release.

Disclosure: The University will not disclose, redisclose or disseminate the saved encrypted mathematical representation to anyone other than its payroll vendor and any other vendors that maintain, fix, update or troubleshoot the timeclock for the purposes identified above without/unless:

A. First obtaining written employee consent to such disclosure or dissemination;

B. The disclosure or re-disclosure completes a financial transaction requested or authorized by the employee;

C. Disclosure or re-disclosure is required by state or federal law or municipal ordinance; or

D. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

The University will not sell, lease, trade, or otherwise profit from the saved encrypted mathematical representation; however, the University may pay its payroll vendor for timekeeping and payroll products or services utilized by the University. The University may also pay a vendor to maintain, fix, update or troubleshoot the timeclock.

Retention and Destruction Schedule: An employee's mathematical representation will be retained only until the initial purpose for collecting or obtaining the biometric identifier or information has been satisfied, which means that the University will instruct its payroll vendor to permanently destroy the saved encrypted mathematical representation within thirty (30) days of an employee's transfer to a position that does not utilize the timekeeping system (if applicable) or within ninety (90) days of an employee's termination. The University will delete any copy of the encrypted mathematical representation within its possession within ninety (90) days of the employee's transfer to a position that does not utilize the timekeeping system (if applicable) or within ninety (90) days of an employee's termination. The University will follow these guidelines unless the law dictates otherwise.

Storage, Transmission, and Protection: The University shall use a reasonable standard of care to store, transmit and protect from disclosure the saved encrypted mathematical representation. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the University stores, transmits and protects from disclosure confidential and sensitive information, such as account numbers, PINs, driver's license numbers and social security numbers.

Enforcement: An Employee who violates this Policy and Procedure will be subject to disciplinary action, up to and including termination.

Entities Affected by this Policy

All Divisions of the University.

Related Documents

All University Policies, including: RU Policy No. 2.17 (Professional Code of Conduct); RU Form No. 2.18F (Consent to Collection of Biometric Information).

Revision and Implementation

The Vice President for Human Resources shall have the authority to revise this Policy, subject to the approval of the President's Executive Council (if required).

The following shall have the authority to establish any procedures necessary to implement this Policy: Vice President for Human Resources/Chief Human Resource Officer, Vice President for Finance & Administration/Chief Financial Officer (and/or, as authorized by the Vice President, the Director for Campus Safety and the Senior Foreman for Facilities), and Vice President for Information Technology/Chief Information Officer.