COMPREHENSIVE ADULT
STUDENT ASSESSMENT SYSTEMS

CASAS Human Resource Security Policy

Debalina Ganguli 9/8/2025

Purpose

The Human Resources Security Policy ensures that all employees, contractors, and third-party vendors are aware of and comply with the security requirements of CASAS.

The underlying core of CASAS internal and external operations is our information database systems and technology resources. These systems and resources are the property of CASAS and are intended solely for business use. All employees are expected to appropriately use, safeguard, and maintain the quality assurance and integrity of the technology-based infrastructure.

This policy establishes guidelines to protect confidential student and personnel data, intellectual property and business information, and information technology (IT) resources including but not limited to computer hardware and software, telecommunications infrastructure, networks, email, and internet and intranet systems from unauthorized access, misuse, and security breaches.

Scope

This policy applies to:

- All current and prospective employees, contractors, and third-party vendors with access to confidential data and all IT systems including software, databases, servers, computers, and laptops.
- All sensitive organization information, including student data, intellectual property, and financial records.
- All employee records and processes, including hiring, onboarding, role-based access, and termination.

This policy aims to:

- Protect student-level data that comprises personal (private) information and all personnel information from threats.
- Reduce the risk of unauthorized access to all applications, secure networks, and business information including financial and employee files.
- Establish security roles and responsibilities for personnel.
- Prohibit installation of any software by employees at their workstation using unknown passwords or releasing passwords to other persons without prior approval or authorization from the IT security manager or the executive management team.
- Ensure secure onboarding, access control, and offboarding procedures.

Roles and Responsibilities

- **Executive Management Team**
  - Oversee that all employees, contractors, and third-party vendors are following security protocols and controls in accordance with established policies and procedures.
  - Responsible for administering, reviewing, revising, interpreting, and applying this policy to ensure ongoing compliance.
  - Oversee all investigations.
- **Human Resource Coordinator**
  - Implements background verification checks for new hires.
  - Ensures all employees sign confidentiality agreements before employment begins.
  - Completes an accurate check of an employee's application form.
  - Coordinates with IT security manager for secure offboarding procedures.
- **IT Security Manager**
  - Ensures policies align with data protection regulations and business needs
  - Implements role-based access controls (RBAC) for employees based on job functions.
  - Provides security awareness training during onboarding and periodically thereafter.
  - Manages account provisioning and deactivation for employees and third-party contractors.
  - Conducts periodic audits of processes to ensure compliance and monitor unauthorized access or unusual activity.
- **Employees, Contractors, and Third-party Vendors**
  - Must comply with all security policies and attend required trainings.
  - Must review the reference documents listed at the end of this document.
  - Must report security risks (e.g., suspicious activity, insider threats) to IT security manager or the executive team.
  - Must not share passwords, sensitive data, or confidential documents without authorization.

Security Procedures

- **Pre-Employment Screening and Background Checks. CASAS** conducts background verification checks for all new hires
    - E-Verify: To confirm work authorization
    - Identity check against a passport/identification card or equivalent document that contains a photograph
    - Employment and reference verification
    - Education and certification validation
- **CASAS Confidentiality and Non-Disclosure Agreement (NDA.** All employees, contractors, and third-party vendors must sign a Confidentiality Agreement and NDA before accessing sensitive data.
- **Contractors and Third-Party Vendors Security**
    - Vendors and contractors must sign the **CASAS Independent Contractor Agreement** before accessing any CASAS systems.
    - Vendor access is restricted to necessary business functions and monitored by the IT security manager.
    - All third parties handling data must comply with security and privacy standards.

Secure Access Control and Authorization

CASAS manages student-level data that comprises personal (private) information in compliance with all applicable federal and state privacy laws including, but not limited to, the FERPA of 1984 (20 U.S.C. Sec 1232g), HIPAA, COPPA, CCPA, California Education Code sections 49060 to 49070, and California Assembly Bill 1584. CASAS security measures articulated in the **CASAS Statement Regarding Privacy and Confidentiality** incorporate advanced industry standards and protocols to ensure data is secure and confidential.

Role-Based Access Control (RBAC): Employees and contractors are granted only the minimum access necessary to perform job duties. Access is reviewed annually to ensure compliance with job-role requirements.

Employee Identification and Authentication: All employees and contractors must use multi-factor authentication (MFA) to access CASAS systems. Shared user accounts are strictly prohibited for security-sensitive applications.

Security Awareness and Training

Mandatory Trainings. All employees must complete security awareness training as scheduled by the IT Security manager. An automated compliance monitoring system

tracks employee compliance with training requirements. The training courses will include the following topics:

- Data privacy best practices
- Phishing and cyber threat awareness
- Incident reporting procedures

Threat Prevention. Employees must immediately report suspicious behavior or security concerns to HR or IT security. IT security regularly monitors for any unauthorized system access, unusual data transfers, or policy violations.

Employee and Contractor Offboarding and Access Termination

When an employee, contractor, or vendor leaves CASAS, the following security measures apply:

Account Deactivation: System access rights of user are revoked immediately upon termination or suspension of employment, contract, or agreement.
Return of Assets: Employee, contractor, or vendor must return all CASAS-owned devices, badges, and records before departure.
Post Employment Responsibilities: Review of the CASAS Confidentiality and NDA compliance with confidentiality agreements during exit. Former employees, contractors, or vendors are prohibited from accessing CASAS systems or data after their employment ends.

Violation, Enforcement and Disciplinary Process

Personal, unauthorized, or inappropriate use of CASAS information systems and resources will result in administrative or disciplinary action, up to and including immediate termination.

- **Policy Violation** includes but is not limited to:
    - Not complying with security guidelines
    - Disclosing confidential information
    - Dishonest or fraudulent acts
    - Forgery or alteration of documents
    - Misappropriation of funds, securities, supplies, or other assets
    - Impropriety in handling or reporting money or financial transactions
    - Personal gain from insider knowledge

    - Accepting or seeking material value from contractors or vendors
    - Destruction or inappropriate use of any CASAS assets
    - Not completing required security trainings
- **Reporting Security Incidents:** Employees, contractors, or vendors must report any security concerns (e.g., unauthorized access, data breaches). Any detected or suspected fraud, data security breach must be reported to **All Voices**, the immediate supervisor, or IT security manager or the executive team.
- **Investigation Responsibilities:** The executive team is responsible for investigating security breaches, suspected fraud, or misconduct. The executive team will appoint an investigation team to look into the allegations. All information regarding the investigation will be treated confidentially. Investigation results will be disclosed to those with a legitimate need-to-know. Disciplinary actions will be reviewed by the executive team and if necessary, outside counsel. Decisions to prosecute or refer to law enforcement will be made with legal counsel.
- **Disciplinary Actions**
    - Formal warnings and additional training
    - Restricted or revoked access to CASAS systems
    - Employment termination for severe or repeated violations
    - Legal action for intentional misconduct or data breaches

Reference documents

1. CASAS Privacy Compliance Statement
2. CASAS Confidentiality and Non-disclosure Agreement
3. CASAS Code of Conduct
4. CASAS Appropriate Use of Technology Resources
5. CASAS Independent Contractor Agreement