730.1 Social Security Number (SSN) Access and Protection Policy

Policy Title: Social Security Number (SSN) Access and Protection Policy
Policy Number: 730.1
Responsible Office: Information Technology Services
Approval Authority: Administrative Council; President's Cabinet (Final Approval)
Applies To: Employees, functional offices, student workers, contractors, or authorized users who request or receive access to view SSNs in approved systems.
Alignment: FERPA; GLBA; federal and state identity protection requirements; recognized access control frameworks (as updated)
Effective Date: May 2026
Current Version: 1.0.0
Supersedes: None
Next Scheduled Review: January 2027

I. Policy Overview and Purpose

This policy establishes strict controls governing access to Social Security Numbers (SSNs) within approved institutional systems. It limits access to authorized individuals based on documented business necessity and protects Restricted Information in accordance with legal and institutional security requirements.

II. Scope

This policy applies to all employees, contractors, and authorized users who request or are granted access to view or process Social Security Numbers within institutional systems.

III. Definitions

Business Necessity — A validated operational need that requires access to SSNs when no alternative identifier can fulfill the function.

ERP Administrative Interface — The administrative interface of the institutional Enterprise Resource Planning (ERP) system used for managing sensitive institutional and student information.

Least Privilege — Granting the minimum access necessary to perform job duties, particularly for SSN-level data.

Restricted Information — Highly sensitive data requiring strict safeguards, including identity-critical data such as Social Security Numbers (SSNs).

Social Security Number (SSN) — A Restricted Information identifier requiring the highest level of safeguards under federal and institutional policy.

IV. Standards and Requirements

Access to view Social Security Numbers within the institutional Enterprise Resource Planning (ERP) system is strictly limited and granted only when required to perform official job responsibilities. Access must be based on **business necessity** and limited to the minimum level required.

SSN access is granted on an individual basis and is not included within standard ERP role-based access profiles due to the sensitivity of the data.

While certain offices may require access to SSNs:

- Business Office
- Admissions and Records
- Financial Aid

Access is **not** automatically granted within these offices; individual approvals are required.

SSN access approvals must align with the Data Owner assignments defined in the Data Governance and Security Oversight Policy (735.0).

Employees requesting SSN access must submit a formal request including:

- Justification for SSN access
- Description of job duties requiring access
- Acknowledgment of confidentiality responsibilities

V. Authorized Use

Authorized access to SSNs may be used solely for legitimate institutional purposes, including:

- Federal and state reporting
- Financial aid processing
- Tax reporting and compliance
- Identity verification when no alternative identifier exists

Whenever possible, institutional ID numbers must be used instead of SSNs.

VI. Prohibited Use

Users with SSN access may not:

- Access SSNs for personal or non-official purposes
- Share SSNs with unauthorized individuals
- Print, download, store, or transmit SSNs outside approved systems
- Use SSNs as routine identifiers when alternatives exist

VII. SSN Minimization Standard

Even when SSN access is granted, employees must minimize the use of Social Security Numbers and must use institutional identifiers whenever possible. SSNs may only be used when legally required or when no alternative identifier can fulfill the documented business need. SSNs must never be used as default identifiers, printed, downloaded, or transmitted outside approved systems.

VIII. Approval Workflow

Requests must first be approved by:

- Requests originating from Admissions must be approved by the Director of Admissions.
- Requests originating from the Business Office must be approved by the Vice President of Finance.
- Requests originating from the Financial Aid Office must be approved by the Director of Financial Aid.
- Requests originating from any other department must be approved by the Vice President of Instruction.

Final approval and access provisioning is completed by the designated ERP Security Administrator.

IX. Training Requirement

Before access is granted, employees must:

- Complete FERPA and data security training
- Acknowledge institutional sensitive-data policies

X. Access Provisioning Standards

Upon approval, ITS will:

- Grant the minimum permissions necessary
- Document the approval and access level
- Ensure access aligns with job responsibilities

XI. Review and Recertification

- SSN access will be reviewed at least annually
- Supervisors/approvers must recertify continued need
- Access is removed immediately upon job changes or separation

XII. Monitoring and Auditing

The institution may:

- Monitor ERP access logs
- Conduct periodic audits
- Investigate suspected misuse or unauthorized access
- Access to SSNs is subject to periodic review

XIII. Enforcement and Sanctions

Violations of this policy may result in enforcement actions in accordance with the Data Governance and Security Oversight Policy (735.0) and the ITS Enforcement and Escalation Standard (735.0.1).

XIV. Exceptions

Exceptions must follow the authoritative exceptions framework defined in the Data Governance and Security Oversight Policy (735.0).

Due to the Restricted classification of Social Security Numbers, any exception to SSN access or handling requirements requires:

- Approval from the appropriate functional leader (Vice President of Finance, Director of Admissions, Director of Financial Aid, or Vice President of Instruction, as applicable), and
- Approval from the Director of Information Technology Services.

Exceptions to SSN restrictions may be granted only when required for legally mandated institutional functions, including federal or state reporting, financial aid operations, payroll, taxation, or other regulatory obligations.

XV. Revisions

This policy shall be reviewed annually to ensure continued accuracy, regulatory compliance, and alignment with institutional practices. Revisions shall follow the College's established approval process, and all individuals are responsible for compliance with the current approved version. Version history shall be maintained in accordance with institutional documentation standards

Version	Date	Description	Approved By
1.0.0	Jan 2026	Initial release of SSN Access Policy	President’s Cabinet