Prairie State College Procedure: Secure Handling of SSN

Audience:

- All faculty, staff and students
- All employees, both permanent and temporary
- All contractors, vendors and any others (including 3rd parties) entrusted with SSN information.

Definition:

It is the intent of Prairie State College to protect the personal information of its students, staff, faculty and other individuals associated with the college from unauthorized access or disclosure, and possible misuse or abuse. This policy is designed to establish awareness and provide guidance on the proper handling of Social Security Number (SSN) information maintained by or on behalf of Prairie State College.

Policy Statement:

Social Security Numbers may not be captured, retained, communicated, transmitted, displayed or printed in whole or in part, except where required or permitted by law, and in accordance with the standards outlined in this policy.

Background Issues:

Scope

The policy applies to the SSN whether maintained, used or displayed wholly or in part, and in any data format, including but not limited to oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or other medium as determined.

References

- Illinois Personal Information Protection Act (PIPA)
- Gramm-Leach-Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)

Definitions

1. Social Security Number (SSN) may be interpreted to include Taxpayer Identity Number (TIN).

2. Individual Workstations: Includes but is not limited to desktops, laptops, tablets, smart phones and PDAs.
3. Removable or Transportable Media: Includes but is not limited to paper forms, reports, cassettes, CDs, USB tokens, flash drives, hard drives and zip drives.
4. Data Steward: NOTE - A coordinated effort is underway to establish this and other relevant definitions. The policy statement will be updated as the definition is established.
5. Enterprise Systems: The term is applicable to any infrastructure as a means of describing its importance to the college's mission and how it should be administered, protected and funded. From a functional viewpoint, an Enterprise System will be either (a) the only delivery platform for an essential service, or (b) a platform for a service to a very broad constituency spanning organizational boundaries. An enterprise system is most frequently administered and protected by an institutional unit with expertise in both the technology and the business functions delivered.

"Enterprise System Status," January 2006, T.E. Board/ISA

Standards

1. Going forward, the college does not permit the use of a SSN as the primary identifier for any person or entity in any system, except where the SSN is required or permitted by law, and permitted by college policy.
2. Where permitted by law and college policy, the SSN may be stored as a confidential attribute associated with an individual or may be used as an optional key to identify individuals for whom a primary identifier is not known.
3. Individuals shall not be required to provide their Social Security number, verbally or in writing, at any point of service, nor shall they be denied access to those services should they refuse to provide a SSN, except where the collection of SSN is required by law or otherwise permitted by college policy. Individuals may volunteer their Social Security number if they wish, as an alternate means for locating a record.
4. Except where the SSN is required by law, the college ID (EMPLID) replaces use of the SSN and will be used in all future electronic and paper data systems and processes to identify, track, and service individuals associated with the college. The college ID will be permanently and uniquely associated with the individual to whom it is originally assigned.
5. All newly developed or acquired application software will not store SSN as a data element until a business requirement is submitted and approved by the Data Steward and/or other authorities as deemed appropriate.
6. Servers housing databases or records containing SSNs should be of single purpose, with access restricted to system administrators, protected by an approved firewall appliance, and should not be used by individuals to access the Internet or access e-mail.
7. Where possible, all records containing an SSN should be stored on network drives with access limited to those individuals or entities that require access to perform a legitimate college job function. Individual workstations, laptops and other personal computers (PDAs) should not be used to store records containing SSNs.

8. All removable or transportable media (e.g., paper forms, reports, cassettes, CDs, USB drives, etc.) containing SSNs must be secured when not in use. Reasonable security measures depend on the circumstances, but may include locked file rooms, desks and cabinets.
9. Subject to applicable document retention policies or unless required by law, when no longer required, paper documents and electronic media containing SSNs will be destroyed or disposed of using methods designed to prevent subsequent use or recovery of information.
10. SSNs will be released to entities outside the college only where permitted or required by law, or with the express written permission of the individual or entity, or where approved by Prairie State College Cabinet.
11. The college will limit access to records containing SSN to those individuals requiring access as determined by job function. Individuals permitted access to SSN will be instructed on the appropriate handling and protection of this data by their management or designated representative.

Procedure

Individual business units are responsible for the development, documentation and implementation of applicable procedures to effectuate this policy. Procedures are subject to review by the college policy committee.

Compliance

All parties as delineated under Audience are required to comply with this policy no later than sixty days after approval (see "Date Effective.") Individuals who discover or strongly suspect the unauthorized release of SSN or related information, or a violation of this policy must promptly notify their management and any of the following:

- PSC Help Desk - (708) 709-7999
- E-mail: helpdesk@prairiestate.edu
- College Ethics and Compliance Officer

Approved Uses of SSN

The primary uses and reasons for the continued capture, storage, retention and processing of SSN data are identified and documented in the ‘Approved Uses of SSN’. Typically, processes that access historical SSN data, or require or permit continued use of SSN data, are described here. Additional processes may be added as approved by the college.