Policy on the Protection of Social Security Numbers

Suffolk County Community College collects, maintains and secures social security numbers (SSNs) or taxpayer identification numbers (TINs), when they are the same as SSNs, for students, faculty, administrators, staff, alumni and other individuals associated with the College, who are required to provide such confidential personally identifiable information numbers.

This policy covers the use, display, storage, retention, and disposal of SSNs in print or electronic form and is applicable to all individuals who access, use, or control information technology and/or hard copy records containing SSNs. All such individuals shall employ deliberate and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of the SSNs they handle, store, and/or transmit or to which they otherwise have been given or have gained access.

Policy Objectives

This Policy will achieve the following:

1. Ensure that the necessary awareness, procedures and training exist for all members of the College community in order to comply with this Policy;
2. Require that all individuals affected and governed by this Policy take personal responsibility for adhering to it;
3. Reduce reliance for identification purposes on SSNs in favor of the College ID as the primary identifier for persons associated with the College;
4. Establish a consistent policy towards and treatment of SSNs;
5. Eliminate unnecessary storage and use of SSNs in College documents, practices and systems;
6. Ensure that access to SSNs for the purpose of conducting College business is granted only to the extent necessary;
7. Enhance and preserve individual privacy for members of the college community through the confidential handling of SSNs;
8. Ensure that no new systems or technology will be purchased or developed by the College that uses the SSNs as its primary key to the database, except where required by law;
9. Ensure that any request for SSNs of employees, faculty, staff, students or alumni is for a legitimate purpose; and
10. Ensure that SSNs are redacted from any document or form requested or distributed when they are not relevant to the request.

Collection, Use and Release of Social Security Numbers

The College collects SSNs when required to do so by law or when no other identifier serves a legitimate business purpose. Unless required by law, individuals need not provide their SSN, orally or in writing, at any point of service, nor are they to be denied access to those services should they refuse to provide an SSN.

SSN collection must be approved by the appropriate College official. When an SSN is requested, the College must inform the individual by what authority and what uses will be made of the SSN. Similarly, whenever an SSN is requested on a College form or other document, the written or electronic form used to request the number will clearly identify the reason for the request.

SSNs will not be used by the College to identify individuals except as required by law or for a legitimate business purpose. SSNs will not be stored in any form outside of the College's enterprise resource systems (e.g., Banner, Operational Data Store –ODS, Xtender-Document Imaging, etc.) without the specific approval of the appropriate College official.

SSNs will be released by the College to persons or entities outside of the College only in the following circumstances:

- As required by law;
- When permission is granted by individual;
- When an external entity is acting as the College's authorized contractor or agent, attests that no other methods of identification are available and ensures that reasonable security measures are in place to prevent unauthorized dissemination of SSNs to third parties; or
- When the College General Counsel has approved the release.

Procedures

The Information Security (ISec) Committee is responsible for overall SSN security oversight. In addition to the procedures set forth in this Policy, the ISec Committee will establish additional procedures, as needed, for the use, display, storage, retention, and disposal of any document, item, file, or database which contains SSNs in print or electronic form.

The following College officials are responsible for SSN management for their respective areas of operations:

1. Alumni: Vice President for Institutional Advancement
2. Continuing education and workforce development: Vice President for Workforce and Economic Development
3. Employees and prospective employees: Assistant Vice President for Employee Resources
4. Faculty and visiting scholars: Vice President for Academic and Student Affairs
5. Finance: Vice President for Business and Financial Affairs
6. Institutional Effectiveness: Vice President for Planning and Institutional Assessment
7. Legal: College General Counsel
8. Students: Associate Vice President for Student Affairs

Access

Access to SSNs must be requested by an individual's supervisor or area administrator. When approval is granted, supervisors and administrators will submit access requests to the appropriate College official for authorization. Supervisors and administrators are also responsible for maintaining their area's secure work processes for SSNs and requesting the removal of access to SSNs when an individual's employment or responsibilities change.

Access to SSNs will be at one of the following three levels:

- Level 1 – Full read/write and search capabilities, limited to specific administrative staff within departments as required for County, State or Federal agencies.
- Level 2 – View and update to verify and/or correct a record.
- Level 3 – Enter-only capability for individuals assigned responsibility for creating records.

The access levels to SSNs will be limited and reviewed quarterly by the appropriate College officials, as identified above. An employee's access will be immediately terminated upon change of duty/assignment or separation from the College.

Use

Individuals who have permission to work with SSNs are not permitted to download files containing them to portable media (e.g., flash drives, memory cards, CD/DVDs, etc.), or to store or process files on laptops unless the file or the laptop's hard drive is encrypted. In addition, files should only remain on College office PCs or network folders during the time they are being processed. The release or posting of personal information, such as grades, keyed by the SSN or any portion thereof, is prohibited.

Release and Transmission

The release and transmission of SSNs, either internally or externally, must be approved by the appropriate College official, as identified above. Electronic transmission must be secure and should use Secure File Transfer Protocol (SFTP). If SFTP is not available, files may only be transmitted using email if the file is encrypted and password protected. In addition, only College email accounts are to be used to send and receive these files. Transmission methods must be approved by the College Associate Dean for Computer and Information Systems.

Hard copy transmission must be completed by U.S. Mail, Federal Express, UPS or other secure and confidential carrier.

Receipt of SSNs from External Sources

Individuals who receive paper documents or electronic transmissions from external sources that contain SSNs must forward such documents or transmissions to the College Registrar, Central Records Office, Human Resources or Payroll, as appropriate. Neither the original nor copies of such documents or transmissions are to be maintained by any other offices.

Compliance

Individual(s) who inadvertently gain access to an electronic file or database that contains SSNs or College IDs for which they have not been authorized shall report it immediately to the College Associate Dean for Computer and Information Systems. Individual(s) who inadvertently gain access to a paper file or database that contains SSNs or College IDs for which they have not been authorized shall report it immediately to their supervisor, who, in turn, shall report it to the Vice President for Planning and Institutional Assessment.

Violations of any part of this policy resulting in the misuse of, unauthorized access, or unauthorized disclosure or distribution of SSNs will be subject to College disciplinary procedures, up to and including the termination of employment or contract with the College, or in the case of a student violating any parts of this Policy, in suspension or expulsion from the College. When appropriate, law enforcement will be contacted.

Approved by Executive Council
November 3, 2009