Handling of

Personally Identifiable Information (PII) For South Suburban College Employees

Protection of Personally Identifiable Information (PII)

South Suburban College recognizes that certain information maintained by the College constitutes **Personally Identifiable Information (PII)** and requires enhanced safeguards.

Definition

For purposes of this policy, PII includes, but is not limited to:

- Social Security numbers
- Driver's license or state identification numbers
- Financial account or payment card information
- Student education records protected under FERPA
- Financial aid information protected under GLBA
- Health information protected under HIPAA
- Biometric identifiers
- Date of birth when combined with other identifying data
- Any information that can reasonably be used to identify an individual

PII may exist in electronic, paper, audio, visual, or other formats.

Responsibilities for Handling PII

All employees, contractors, and authorized users who access PII must:

- Access PII only when required to perform official job duties
- Use the minimum necessary information to accomplish the task
- Store PII only in approved College systems
- Transmit PII only through secure, encrypted methods
- Protect physical documents containing PII from unauthorized access
- Immediately report suspected exposure, loss, or unauthorized disclosure

PII must not be:

- Stored on unapproved personal devices
- Transmitted via unsecured email or messaging platforms
- Downloaded to local devices unless explicitly authorized
- Shared with unauthorized individuals

Data Classification and Controls

The College maintains a data classification framework to identify and protect sensitive information, including PII.

Systems containing PII must implement appropriate safeguards, including:

- Role-based access controls
- Multifactor authentication where applicable
- Encryption in transit and at rest when feasible
- Logging and monitoring of access
- Secure disposal procedures

Access to systems containing PII may be reviewed periodically to ensure continued business need.

Incident Reporting and Response

Any suspected compromise, unauthorized access, or loss of PII must be reported immediately to:

- The Information Technology Department
- The employee's supervisor
- Human Resources (if applicable)

The College will investigate reported incidents in accordance with its Incident Response Plan and may initiate required notifications under applicable law.

Failure to report known or suspected breaches of PII may result in disciplinary action.

Retention and Disposal

PII shall be retained only for as long as required by:

- Legal obligations
- Regulatory requirements
- Operational necessity

When no longer required, PII must be securely destroyed in accordance with College's record retention schedules and secure disposal standards.