Prairie State College

Adoption Date: 12/09/2009
Revision Date : xx/xx/xx

Information Security Policy

The following plan contains a collection of policy statements and a description of Prairie State College's approach to information security.

Contents

1. Objective and Scope

This plan describes the administrative, operational, and technical security safeguards that must be implemented for systems that create, maintain, house, or otherwise use public, confidential, and restricted information.

There are many layers of security involved, each managed in concert with the rest to provide "Defense in Depth":

1. Physical access to systems
2. Server or host controls
3. Client or workstation controls
4. Data access controls (confidentiality)
5. Policy & Procedures
6. Network controls
7. Employee practices

Data Executives are responsible for taking the necessary steps to identify internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of institutional data. Risks may include, but are not limited to:

- Unauthorized access to public, confidential, or restricted information
- Compromised system security as a result of access by an intruder
- Interception of data on the network
- Physical loss of data center or computer equipment
- Errors or corruption introduced into systems
- Accidental deletion or modification of institutional data

2. Administrative Controls

2.1 Roles and Responsibilities:

Responsibility for Prairie State College's information security program is delegated to the following groups and individuals:

Data Executive - The enterprise executive having policy-level responsibility for a particular set of information assets.

Information Technology Security Officer – The official responsible for directing implementation of the enterprise information security program is The Executive Director of Information Technology Resources (or his/her designee.)

Data Manager - The dean, director or manager within a department (or his/her designee) accountable for managing information assets.

Data Custodian - The technical or functional official (and his/her staff) that has operational-level responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of hardware and software platforms.

Authorized Data User – Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Data Users (Users). Users include, but are not limited to, faculty and staff members, trainees, students, vendors, volunteers, contractors, or other affiliates of Prairie State College.

2.2 Incident Response

Information Technology Resources (ITR) is responsible for incident response, in conjunction with law enforcement, or other governmental agencies and/or vendors as required. Incidence response procedures are described in depth in the Prairie State College Incident Response Plan.

2.3 Acceptable Use of Information Systems

Prairie State College's acceptable use policy is contained in the Use Of Information Resources Including World Wide Web and Internet Policy (C-21). This policy describes the requirements for appropriate use of technology.

2.4 Planning for Security

A control review should be performed before implementation of computer systems which house or handle *Confidential* or *Restricted* institutional information. This may include:

- A technical security evaluation to ensure appropriate safeguards are in place and operational
- A risk assessment, including a review for regulatory, legal, and policy compliance
- A contingency plan, including the data recovery strategy

3. Operational Controls

3.1 General Principles

- Access to Prairie State College *Confidential* and *Restricted* information assets may only be granted to Authorized Data Users on a need-to-know basis. The appropriate *Data Manager* must approve and verify such access.
- All Users shall receive education on the expectations, knowledge, and skills related to information security.
- Every User must maintain the confidentiality of Prairie State College information assets even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is *public*.
- No User should place *Restricted* information including social security numbers, credit card numbers, or drivers license numbers onto personally owned media or storage devices (e.g., PDA's, floppy disks, case logs, note cards) or maintain a personal database.
- Storage of any other *Confidential* or *Restricted* information, such as student grades, on personally owned media or storage devices or in personal databases is discouraged. In cases where such storage cannot be reasonably avoided, all care must be taken to prevent unauthorized deletion, modification, or disclosure.
- Each User is personally responsible for any breaches that occur as a result of his/her actions.
- Everyone has an obligation to report instances of non-compliance to their supervisors, the Executive Director of Human Resources, or the Executive Director of Information

Technology Resources.

- Users who access data for which they do not have a need to know and/or commit breaches of confidentiality may be subject to disciplinary action up to and including discharge, termination of contract/relationship, and/or liability to civil and criminal penalties.
- Everyone must comply with all applicable board policy, federal, and state regulations (e.g. FERPA) governing the access any use of data.

3.2 Information Access

3.2a Physical Access Control

- The level of physical access control for any area that contains institutional information is determined by the level of risk and exposure. Data centers and other locations where *Restricted* information is housed must be protected at all times by physical access controls such as keys, access cards, and/or burglar alarms.
- Physical access to data center areas must be monitored and logged through a sign-in sheet, electronic logging, or other tracking mechanism. Visitors and other maintenance personnel will be escorted by authorized operations staff when accessing the data center.
- Electronic or hardcopy media that contains *Restricted* information must be secured during storage, transportation, and disposal.

3.2b Electronic Access Control

Access will be limited by the Identification and Authentication policies in section 4 of this document. In addition,

- Users' immediate supervisors must inform ITR and Human Resources when User accounts become inactivate or when access is no longer required.
- Users' immediate supervisors will work with Human Resources to ensure the timely revocation of access privileges and return of institutionally owned materials (e.g., keys, ID Cards), for terminated employees and contractors.
- Inactivity time-outs must be implemented, where technically feasible, for terminals and workstations that access *Restricted* information. The period of inactivity shall be no longer than 30 minutes in publicly accessible areas.

3.2c Access to Data for Automated Operations (Generic Access)

Generic access to information stored in databases is allowed only for non-interactive tasks. A non-interactive task is one that is scheduled to run automatically or one that is triggered by a series of events. A User does not directly initiate the task, nor is a User the direct recipient of the information. This includes automatic downloads and other linkages for data transfer.

- Requests for generic access to information stored in databases for automated operations are made to the Data Manager. If approved, such changes will be executed by a programmer employed by ITR, and security practices utilized in the solution will be reviewed by the ITR System Administrator.

- Generic account passwords must be protected from unauthorized disclosure. Hard coded passwords that reside on a client machine or in an application must be afforded reasonable protection commensurate with risk and the available platform or application security features.
- Information access via generic accounts is extremely rare and must be limited to the specific task required.

3.2d Prairie State College Systems Administered by Contractors

An on-site *Data Custodian* must be identified to oversee administrative duties performed by contractors to ensure their compliance with security policies and standards. Contractor activities will be controlled and monitored as follows:

- Contractor User accounts must not allow more system or network privileges than necessary to meet contract requirements.
- Secure authentication of contractors is required.
- Logging and auditing of system accesses and activity is required.

3.2e Audits

- A *Data Custodian* must be able to audit access and access attempts to *Restricted* information. To the extent technologically practical, *each Data Custodian* shall maintain ongoing internal audit processes that record system activity such as log-ins, file accesses, and security incidents.
- The *Data Manager* and/or *Data Custodian* shall periodically review the audit records for evidence of violations or system misuse. Investigation will be conducted when unauthorized accesses and attempts are identified.
- All Users shall be made aware that access audits may be conducted. If evidence of improper data access is discovered, it may result in disciplinary action.

3.3 Communication Security

Institutional information transmitted outside the organization requires additional safeguards. Security provisions employed will depend upon the identified risk and threats, regulatory requirements, and the technical mechanisms available.

- The *Data Manager* is responsible for making decisions regarding appropriateness of external transmission and access.
- The Information Security Officer will review and approve technical security mechanisms and services for remote access and external transmission.
- Electronic communication and exchange of *Restricted* institutional information that occurs over open networks such as the Internet must include strong authentication, and may require encryption (with effective administration of keys and passwords for

encryption), depending on the nature of the communication, and associated risk assessment.

- Encryption must be employed for all external transmissions of *Restricted* institutional information via electronic mail, except as authorized by the subject of the data.

3.4 Information Integrity Controls

Information must remain consistent, complete and accurate. Integrity errors and unauthorized or inappropriate duplications, omissions and intentional alterations will be investigated and reported to the *Information Technology Security Officer* and the *Data Executive* of the affected data.

3.4a Separation of Duties and Functions

To protect the integrity of data, tasks involved in critical business processes must be performed by separate individuals. Where feasible, responsibilities of programmers, system administrators and database administrators must not overlap.

3.4b Systems and Application Software

- System and application software must be tested before installation in a production environment.
- System and application software must be protected from unauthorized changes.

3.4c Change Controls

Configuration management ensures that changes do not introduce any new vulnerability to systems or processes, and that changes do not remove important existing features. A system for change control management must be implemented for systems handling *Confidential* information, to monitor and control hardware and software configuration changes. For more details, see the Information Technology Change Management Policy.

3.4d Anti-Virus Controls

- All systems connected to the network will have virus protection where technologically feasible.
- The most recent version of anti-virus software must be implemented and maintained with current virus signature/patterns.

3.4e Patches

- Critical operating system patches must be installed on all systems as soon as possible after their general release.
- Critical application patches, should be installed to the extent possible on all systems as soon as feasible.

However, installation of patches may be delayed for the following reasons:

1. To backup the system prior to installation.
2. To test prior to moving into a production environment.
3. To verify compatibility with other installed applications.

3.5 Preventive Measures

Processes are necessary to prevent loss of vital information, to provide backup and recovery, and provide continuous operation consistent with the business needs of the institution.

3.5a Prevention

Annual testing of preventive methods as they apply to fire, utility services and other environmental hazards must occur.

3.5b Backup

- Backups must be retained for 30 days.
- At least three versions of the data must be maintained.
- At a minimum, one fully recoverable version of all critical data must be stored in a secure, off-site location.
- All critical information used on workstations should be placed on networked file server drives to allow for backup.
- Backup and recovery documentation will be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
- Recovery procedures will be tested on an annual basis.

4. Technical Controls

4.1 Identification

The standard format for Login Identifiers (user names) for faculty or staff is first initial and last name. In cases where this would result in duplicates, first initial, middle initial, and last name, or first two letters of first name and last name. Student user names consist of the first initial and last name appended with a sequence number.

Users who are both student and staff or faculty members are handled on a case by case basis, but the following rules generally apply:

1. Students or former students that have student accounts who are then hired as employees will normally be given an additional Staff/Faculty account.
2. Staff or Faculty members taking classes normally have their existing accounts modified to allow access to the services available to students.

4.2 Authentication

At a minimum a valid user name and password will be required for authentication in order to create, modify, or use information that is *Confidential* or *Restricted*. All such systems will adhere to the minimum acceptable password standards, as described below:

Minimum Password Standards

1. A unique user name and initial password is issued for each User of the system.
2. User-initiated password changes must be supported.
3. Sharing of individual account passwords is not allowed. This does not apply to generic group accounts, where the password is managed within a work group.
4. A password must be changed if it is shared in the course of getting help with a problem, or if it is believed an unauthorized user has used an account or may have seen or captured a password.
5. Passwords should be changed at significant events or changes of status, such as a semester change. All passwords should be changed at least twice in a calendar year.
6. Administrator intervention is required to reset/change passwords that are forgotten, corrupted, or otherwise unknown to the User. Alternatively, an institutionally approved challenge-response self service application may be used.
7. Proof of identity for password resets may be:

    a. Personal information held in central database records: last name, birth date, and last 4 digits of social security number
    b. Department, supervisor, or liaison identification
    c. A photo ID or human factor such as a biometric scan
    d. Satisfactory challenge-responses in a self service application

8. Accounts will be restricted from logins if the administrator cannot identify the User with one of these methods, until a positive verification can be made.
9. A minimum of one previously used password will be checked at change time to prevent reuse.
10. Passwords must be stored in a hashed/encrypted format, and will be transmitted over open networks in an encrypted format.
11. Password controls will be employed to ensure that robust passwords, at least 8 characters in length, containing at least two letters and 2 non-letters, are used.

4.3 Access Control

4.3a Data Classification

Access to institutional data varies according to the sensitivity of such data and use shall be limited to those defined for the classification to which it was assigned. Where the data is deemed to be of a *Confidential* or *Restricted* nature, access and use shall be limited to the purpose for which it was authorized. There are three levels of confidentiality which apply to institutional data:

- **Public:** Access to *Public* institutional data may be granted to any requester. *Public* data is not considered *Confidential* or *Restricted*. Examples of *Public* data include published “white pages” directory information, and academic course descriptions. The integrity of *Public* data must be protected, and the appropriate owner must authorize replication of the data. Even when data is considered *Public*, it cannot be released (copied or replicated) without appropriate approvals.
- **Confidential:** Access to *Confidential* data must be requested from, and authorized by, the *Data Manager* who is responsible for the data. Data may be accessed by users as part of their job responsibilities (role-based access). The integrity of this data is of primary importance, and the confidentiality of this data must be protected. Examples of *Confidential* data include financial, project, human resources, budget information, and sensitive student information such as student ID numbers and grades.
- **Restricted:** Access to *Restricted* data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the College who require such access in order to perform their job, or to those individuals permitted by law. The confidentiality of this data is of primary importance, although the integrity of this data must also be ensured. Access to *Restricted* data must be requested from, and authorized by, the *Data Manager* who is responsible for the data. Examples of *Restricted* data include student financial aid data, research data, student or employee Social Security numbers, student or employee driver license numbers, or any credit card number. Access to this data may be further legally restricted by federal or state law.

4.3b Access Control Principles:

- The integrity of institutional data must be protected from unauthorized modification, destruction, or disclosure. Permission to access institutional data should be granted to all eligible Prairie State College employees for legitimate institutional purposes.
- Accessing *Confidential* or *Restricted* institutional data, without proper authorization is prohibited. Where access to institutional data has been authorized, use of such data shall be limited to the purpose for which access to the data was authorized.
- Secondary use of institutional data, without adhering to the restrictions, is also not permitted.
- Prairie State College employees must take action to resolve or report to their management instances in which institutional data is at risk of unauthorized modification, disclosure, or destruction.
- Data Managers must ensure all decisions regarding the collection and use of institutional data are in compliance with the law and with Prairie State College policy and procedure. Data Managers must also ensure appropriate security practices are used to protect institutional data, including appropriate auditing mechanisms for monitoring data access.
- All requests for access to *Restricted* institutional data will be documented. Authorization for access to *Restricted* institutional data comes from the *Data Manager*, and is made in conjunction with an authorization from the requestor’s department head or other authority.

- Users will respect the confidentiality and privacy of individuals whose records they access, observe any ethical restrictions that apply to the data they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

4.4 Auditing:

- A *Data Custodian* must be able to audit access and access attempts to *Restricted* information. To the extent technologically practical, each *Data Custodian* shall maintain ongoing internal audit processes that record system activity such as log-ins, file accesses, and security incidents.
- The *Data Manager* and/or *Data Custodian* shall periodically review the audit records for evidence of violations or system misuse. Investigation will be conducted when unauthorized accesses and attempts are identified.
- All Users shall be made aware that access audits may be conducted. If evidence of improper data access is discovered, it may result in disciplinary action.

5. Security Design Considerations:

5.1 Implementation

- Highly Redundant – Wherever possible single points of failure should be avoided

  a. Hardware/equipment
  b. No "single person" system administration dependency

- Physical security

  a. Secure location
  b. Conditioned power & UPS
  c. Environmental controls (HVAC)

- Very granular authorization/access controls available
- Enable enterprise-wide services delivery (directory enabled applications)

5.2 People

- Technical system administrators

  a. Collaboration, robust solutions
  b. Cooperation, division of labor
  c. Responsive to changes
  d. Training/expertise requirements

- Improved User experience

a. Availability of applications
b. Reliability of services
c. Consolidated login (simplified sign-on)

5.3 Policy

1. Collaborative policy development to drive the technologies adopted
2. Ability to reach broader compliance with security/privacy regulations
3. Security procedures well thought out and communicated