BERKELEY COLLEGE

DATA SECURITY POLICY

BERKELEY COLLEGE
DATA SECURITY POLICY

TABLE OF CONTENTS

Chapter	Title	Page
1	Introduction	1
2	Definitions	2
3	General Roles and Responsibilities	4
4	Sensitive Data Classification and Control	6
5	Data Access Control	7
6	Password Control	9
7	Storage of Sensitive Data	10
8	Distribution and Transmission of Sensitive Data	11
9	Network Security	12
10	Mobile Device Security	13
11	Remote Access	14
12	Physical Security	15
13	Third Party Access	16
14	Disposal of Sensitive Data	17
15	Sensitive Data Security Incidents	18
16	Sensitive Data Awareness	19
17	Periodic Policy Review	20

APPENDICES

Appendix A – Categories of Restricted Data

CHAPTER 1 – INTRODUCTION

Accurate, timely, relevant, and properly protected information is a critical asset of Berkeley College.

The College recognizes that failure to implement adequate security controls over sensitive information could potentially lead to:

- Irretrievable loss of important data;
- Serious financial consequences;
- Damage to the reputation of the College; and
- Legal penalties.

Therefore, the College is committed to ensuring that all access to and uses of sensitive information is performed in a secure manner. Measures must be in place to minimize the risk to the College from unauthorized disclosure of sensitive data, whether accidental or deliberate. To comply with data protection laws, sensitive information must be collected and used appropriately, stored safely and not disclosed to any other person unlawfully.

The object of this Data Security Policy is to define the security controls necessary to safeguard the confidentiality and integrity of sensitive College information. This policy provides a framework in which security threats to College information systems can be identified and managed on a risk basis and establishes terms of reference which ensure uniform implementation of data security controls throughout the College.

This Data Security Policy applies to all associates and anyone else authorized to access College Data (as defined in Chapter 2). Failure to comply with these policies may result in loss of data access privileges and possible disciplinary action.

CHAPTER 2 - DEFINITIONS

For purposes of this policy, the following terms shall be defined as indicated below:

Access Administrator: An individual or department with primary responsibility for administering access rights for Users to one or more data systems, including granting new access rights, modifying a User’s existing access rights and reducing or eliminating a User’s access rights. A list of Access Administrators and the system(s) they administer is maintained by the Human Resources Department.

College: Berkeley College.

College Data: Data which is collected, maintained, or utilized by the College for the purpose of carrying out institutional business.

College Network: The system of personal computers, servers, storage devices, printers, telecommunication devices and other related equipment owned by the College and used to process, transmit, receive, store and otherwise manage electronic College Data.

Data: Factual material or information.

Data Steward: An individual or department with primary responsibility for determining the purpose and function of a Data resource. One becomes the Data Steward either by designation or by virtue of having acquired, developed, or created information resources for which no other party has stewardship. A list of Data Stewards is maintained by the Human Resources Department.

Internal Data: College Data which is considered neither “Public Data” nor “Restricted Data”. This includes student directory information that has not been restricted, as well as statistical, procedural, and other information gathered for internal reference and planning that is considered proprietary but its disclosure would not result in a substantial loss to the College, a violation of law, significant negative publicity or other serious consequences.

Managers: Members of the College community who have management or supervisory responsibility.

Mobile Device: Any computer, personal digital assistant, telephone or other device which is designed to be portable and can store Data or connect to a computer network or the Internet.

Portable Digital Media: Any digital media which is designed to be portable, such as CDs, DVDs, tapes, flashdrives, floppy disks, memory sticks and portable hard drives.

Public Data: Data which is easily accessible by the general public and requires no further authorization for release. This includes information not generally considered harmful or an invasion of privacy if disclosed.

Restricted Data: College Data which is accessible only for specific uses by specific authorized individuals, and available for release to other persons under limited circumstances requiring formal approval. Information should be classified as “Restricted Data” if disclosure to an unauthorized individual could result in a substantial loss to the College, a violation of law, significant negative publicity or other serious consequences. Categories of "Restricted Data" are set forth in Appendix A.

Sensitive Data: Data which is either Restricted Data or Internal Data.

Sensitive Data Security Incident: An occurrence in which it may be reasonably suspected that Sensitive Data has been compromised.

Strong Password: A password at least 8 characters in length which consists of a combination of alphabetic, numeric and special (!@#$%^&*<>) characters.

Third Party: Any individual, contractor, vendor or agent which is not an associate or student of the College.

User: Anyone who has access to College Data.

CHAPTER 3 – GENERAL ROLES AND RESPONSIBILITIES

Purpose.

This chapter defines general responsibilities of the College community for protecting sensitive information.

Policy.

1. **Users.** Users are responsible for protecting Sensitive Data to which they have access. Their responsibilities cover both computerized and non-computerized information and information technology devices in their possession. Users are expected to learn and comply with all College policies relating to the protection of Sensitive Data.

2. **Data Stewards.** Data Stewards have the responsibilities of Users and in addition are responsible for the following:

    a. ***Establishing security policies and procedures.*** Data Stewards should establish specific data security policies and procedures for their information where appropriate. Stewards are responsible for the procedures related to the creation, retention, distribution and disposal of information. These must be consistent with this policy, and applicable records retention policies, as well as with other College policies, contractual agreements, and laws. Stewards may impose additional requirements that enhance security.

    b. ***Assigning classifications.*** Data Stewards shall be responsible for assigning each category of their designated Data to a sensitivity classification in accordance with Chapter 4.

    c. ***Determining authorizations.*** Data Stewards determine who is authorized to have access to their information. They shall make sure that those with access have a legitimate need to know the information and understand the security requirements for that information.

3. **Managers.** Managers have all the responsibilities of Users and may in some cases also serve as Data Stewards. In addition, they share responsibility for data security with the Users they manage and supervise.

4. **Access Administrators.** Access Administrators are responsible for controlling access to data systems by administering access rights under the direction of Data Stewards and the Human Resources Department.

5. **Information Systems Department**. The Information Systems Department is responsible for:

    a. Securing the College Network Infrastructure and protecting the College Network from external threats.

    b. Establishing security standards and protocols for Users including encryption techniques and procedures for secure disposal of digital media.

    c. Determining secure methods of remote and Third Party access to the College Network.

6. **Human Resources Department**. The Human Resources Department is responsible for:

    a. Working with Data Stewards to manage data access rights.

    b. Maintaining master lists of access rights and Access Administrators.

    c. Distributing this policy to all associates and tracking their acceptance.

    d. Coordinating periodic classes about data security and tracking completion by associates.

7. **Compliance Department**. The College Compliance Department (in liaison with external legal counsel if necessary) is responsible for interpreting the laws that apply to this policy and ensuring that this policy is consistent with those laws and other College policies.

CHAPTER 4 – SENSITIVE DATA CLASSIFICATION AND CONTROL

Purpose.

The purpose of this chapter is to establish sensitive information classifications and to provide for the identification and management of sensitive information.

Policy.

1. All College Data shall have designated Data Stewards.

2. Data Stewards shall be responsible for assigning each category of their designated Data to one of the following sensitivity classifications: (a) Restricted Data, (b) Internal Data or (c) Public Data.

3. Data that is aggregated shall be classified as to the most secure classification level of any individual component.

4. Data Stewards shall implement policies and security measures as necessary to safeguard the Sensitive Data for which they are responsible.

CHAPTER 5 – DATA ACCESS CONTROL

Purpose.

The purpose of this chapter is to ensure that proper controls are in place to establish and maintain the appropriate access rights for all internal or external data systems used at the College.

Policy.

1. No User shall have access to Sensitive Data unless there is a legitimate business purpose for such access; and the level of access given to a User shall be the minimum required for such User to perform such business purpose.

2. Each Data Steward is responsible for determining the appropriate level of access rights to Sensitive Data for which the Data Steward is responsible.

3. Each Data Steward is responsible for designating Access Administrators who are responsible for administering access to the data system(s) for which the Data Steward is responsible. Each data system should have at least two Access Administrators (one primary and one or more secondary).

4. An Access Administrator shall not grant a User new access rights, modify a User's existing access rights, or reduce a User's access rights unless approved in advance by the appropriate Data Steward(s) or the Human Resources Department in accordance with this chapter.

5. Managers are responsible for ensuring that associates they supervise have proper access rights in order to perform their job responsibilities. In the event that an associate requires new access rights, modification of existing access rights or a reduction in access rights, the Manager must promptly submit a request for change to the appropriate Data Steward(s). Once approved by the Data Steward(s), the request for change shall be forwarded to the appropriate Access Administrator(s) to implement the change.

6. The Human Resources Department may approve new access rights in lieu of Data Steward(s) where such access rights are included in approved job descriptions. When time is of the essence, the Human Resources Department may authorize Access Administrators to reduce or eliminate an associate's access rights.

7. The Human Resources Department shall maintain an up-to-date master list of Access Administrators. Any new Access Administrator or any change in or separation of an existing Access Administrator must be promptly reported to the Human Resources Department by the Access Administrator's Manager.

8. The Human Resources Department shall maintain an up-to-date master list of access rights granted to each associate.

9. The Information Systems Department is responsible for assigning and maintaining access to the College Network infrastructure.

10. Appropriate audit tracking capabilities should be enabled on each data system as determined by the Data Steward(s) in consultation with the Information Systems Department.

CHAPTER 6 – PASSWORD CONTROL

Purpose.

The purpose of this chapter is to ensure that proper password controls are in place to protect sensitive information.

Policy.

1. Strong Passwords are required for any systems which provide access to Restricted Data.

2. Strong Passwords are recommended for any systems which provide access to Internal Data.

3. Users must not share passwords with anyone, including Managers and members of the Information Systems Department.

4. If a User knows or has reason to believe a password has been disclosed or otherwise compromised, the password must be immediately changed or inactivated.

5. If passwords are documented on paper, such paper must be stored in a secure locked location. Passwords which are stored electronically must be encrypted.

6. Passwords must be changed every 90 days.

7. Any system which provides access to Sensitive Data must be configured to lock out a user after three consecutive unsuccessful password attempts, if this feature is available on such system.

8. Web browsers must not be set to remember or otherwise store passwords.

CHAPTER 7 – STORAGE OF SENSITIVE DATA

<u>Purpose</u>.

The purpose of this chapter is to provide for secure storage of sensitive data.

<u>Policies</u>.

1. **Restricted Data**. Restricted Data must be securely stored at all times to prevent access by unauthorized individuals.

    a. Restricted Data in electronic format which is not stored on the College Network or another College-approved secure network must be encrypted.

    b. Any Portable Digital Media or a Mobile Device which contains Restricted Data must never be left unattended and must be securely stored in a locked drawer or cabinet when not in use.

    c. Paper containing Restricted Data must never be left unattended and must be stored in a locked cabinet when not in use.

2. **Internal Data.** Internal Data shall be stored so as to provide a reasonable level of protection against unauthorized access. The same standards for storage of Restricted Data should be employed for Internal Data whenever feasible.

CHAPTER 8 – DISTRIBUTION AND TRANSMISSION OF SENSITIVE DATA

Purpose.

The purpose of this chapter is to provide for secure distribution and transmission of sensitive data.

Policy.

1. **Restricted Data.** Restricted Data must not be distributed or made available to persons who are not authorized to access the information. Restricted Data that is transmitted electronically, transported physically or spoken in conversation must be appropriately protected from unauthorized interception.

   a. Restricted Data in electronic format which is transmitted by any means other than the College Network or another College-approved secure network must be encrypted.

   b. Distributing Restricted Data in paper form should be avoided unless there is a valid business reason for doing so.

   c. Restricted Data which is distributed from one person to another in paper form or stored on Portable Digital Media should either be marked as "RESTRICTED" or enclosed in a sealed envelope marked "CONFIDENTIAL".

   d. Restricted Data should be distributed using a trusted delivery method such as by hand or by College interoffice mail. Restricted Data which must be delivered by courier should be sent certified mail-return receipt requested or by a recognized commercial courier (such as UPS or Federal Express) which provides delivery and receipt tracking.

   e. When Restricted Data is distributed from one person to another, the obligation is on the sender to confirm receipt by the intended recipient.

   f. Telephone or in-person conversations involving Restricted Data should take place in an area where such conversations can not be overheard by unauthorized individuals.

2. **Internal Data.** Internal Data should not be distributed or made available to persons who have no legal, business or other legitimate reason to access the information. The same standards for distribution and transmission of Restricted Data should be employed for Internal Data whenever feasible.

CHAPTER 9 - NETWORK SECURITY

Purpose.

The purpose of this chapter is to define roles and responsibilities for ensuring the security and integrity of the College Network.

Policy.

1. The Information Systems Department is responsible for protecting the College Network from outside threats such as intrusion, probing, viruses, spyware and denial-of-service attempts.

2. The Information Systems Department has the authority to evaluate the seriousness and immediacy of any threat to the College Network and to take action to mitigate that threat.

3. The Information Systems Department is responsible for maintaining procedures to protect Sensitive Data that reside on network servers.

4. Users are responsible for complying with all rules, regulations and policies established to protect the security and integrity of the College Network.

CHAPTER 10 – MOBILE DEVICE SECURITY

Purpose.

The purpose of this chapter is to protect sensitive information accessible from Mobile Devices.

Policy.

1. Mobile Devices which allow access to systems containing Sensitive Data must be password protected in accordance with Chapter 6.

2. Once a User has logged into a Mobile Device, the device must not be left unattended. When finished using a Mobile Device, a User must log out and the device must remain in possession of the User until it can be securely stored.

3. Sensitive Data should not be stored on a Mobile Device unless there is a legitimate academic, administrative or business reason for doing so.

4. When a Mobile Device is permanently transferred from one User to another, any Sensitive Data on the device must be securely erased before transfer.

CHAPTER 11 – REMOTE ACCESS

Purpose. The purpose of this chapter is to define standards for securely connecting to the College Network from a computer or other device located outside of the College Network.

Policy.

1. A User shall be granted remote access to the College Network only for legitimate academic, administrative or business purposes and only after prior approval by senior management of the College.

2. The College Network may be remotely accessed only by using methods of connection approved by the Information Systems Department.

3. Users are responsible for safeguarding the remote access credentials granted to them in accordance with this policy. These credentials may consist of username and password combinations, digital certificates or other software or hardware.

4. All computers or other devices to be used for remote access to the College Network must meet the standards established by the Information Systems Department and must be available for inspection upon request by a representative of the Information Systems Department in order to verify compliance with this policy.

5. After accessing Sensitive Data remotely from a public device, the User must clear cache and delete all temporary files in order to remove Sensitive Data stored on the device.

CHAPTER 12 – PHYSICAL SECURITY

Purpose.

The purpose of this chapter is to ensure that appropriate physical access controls are in place to protect sensitive information.

Policy.

1. **Physical Entry Controls.** Areas containing Sensitive Data in any form or access to any component of the College Network must be protected by appropriate physical entry controls to ensure that only authorized personnel are allowed access. Visitors to secured areas should be supervised by authorized personnel.

2. **Server Rooms**. College Network server rooms must be locked at all times. Campus Security should be able to monitor and log access to these locations. Visitors to server rooms must be accompanied by authorized staff or other designee of the Information Systems Department.

3. **Individual Offices and Work Areas.** Individual offices and work areas utilized by Users with access to Sensitive Data should be secure.

   a. Doors should be locked when Users are not present.

   b. Sensitive Data should not be viewable by passersby or unauthorized guests.

      i. Computer monitors must be carefully positioned so that viewing is restricted to the authorized User.

      ii. When leaving a computer unattended where it might be accessed by unauthorized individuals, the User should either log out of all networks and applications or utilize a password-protected screensaver.

      iii. Papers containing Restricted Data must be covered or put away when unauthorized individuals are present.

   c. Any media containing Restricted Data, whether electronic or non-electronic, must be in a locked drawer, cabinet or storage area when not in use.

4. **Equipment Security.** Equipment components of the College Network, including individual computers, should be secured using a locking mechanism where feasible.

5. **Secure Disposal of Equipment**. All equipment containing media should be checked to ensure that any Sensitive Data is securely erased prior to disposal.

CHAPTER 13 – THIRD PARTY ACCESS

Purpose.

The purpose of this chapter is to define standards for Third Parties seeking to access the College Network in order to minimize the potential exposure to the College from risks associated with Third Party access.

Policy.

1. Third Party access to the College Network may be made for legitimate academic, administrative or business purposes only.

2. Requests to allow a Third Party access to the College Network must be authorized by the Information Systems Department and the relevant Data Steward(s) prior to access being granted.

3. The requester is responsible for assuring that the Third Party agrees in writing to comply with all College data security policies and the requester remains responsible for the actions of the Third Party when accessing the College Network.

4. In order to ensure individual accountability on the College Network, each Third Party granted access must be given a unique user identification and password. The Third Party will at all times be held responsible for any activities which occur on the College Network using this unique user identification.

CHAPTER 14 – DISPOSAL OF SENSITIVE DATA

Purpose.

The purpose of this chapter is to provide standards for secure disposal of any media which contains sensitive information.

Policy.

1. **Disposal of Restricted Data.** When there is no legal, business or other legitimate reason to store Restricted Data, such Restricted Data must be disposed of as follows:

    a. Paper containing Restricted Data must be shredded.

    b. Any media containing Restricted Data in electronic format must be securely erased or physically destroyed.

2. **Disposal of Internal Data.** When there is no legal, business or other legitimate reason to store Internal Data, such Internal Data should be disposed of as follows:

    a. Paper containing Internal Data should be shredded if feasible, otherwise it must be recycled.

    b. Any media containing Internal Data in electronic format should be securely erased or physically destroyed if feasible, otherwise erased.

3. **Transfer of Computers and Other Devices.** Whenever a computer, Mobile Device or other equipment which has the capacity to store data is transferred from one User to another, all data stored on the device must be securely erased.

4. **Responsibilities.**

    a. Data Stewards shall be responsible for establishing timeframes and guidelines for when Data is to be disposed of in accordance with this policy.

    b. Campus Operating Officers shall be responsible for maintaining shredding and recycling facilities at their campus locations.

    c. The Information Systems Department shall be responsible for establishing procedures for securely erasing data as required by this policy.

CHAPTER 15 - SENSITIVE DATA SECURITY INCIDENTS

Purpose.

The purpose of this chapter is to provide steps to take when sensitive information may be compromised.

Policy.

1. All observed or suspected Sensitive Data Security Incidents should be promptly reported to the Information Systems Helpdesk (Data Security Incident) which will notify the Vice President of Information Systems, the Director of Internal Audit, the Chief Compliance Officer, the Data Steward(s) and Campus Operating Officer of the area(s) affected and the Manager of the associate reporting the incident. Users should not attempt to investigate or resolve an incident on their own.

2. The Vice President of Information Systems, Director of Internal Audit and Chief Compliance Officer (the "Investigative Team") will investigate the incident and, when appropriate, take steps to contain any loss of data and remedy the suspected cause(s) of such incident.

3. If, after investigation, the Investigative Team determines there is a reasonable likelihood that Restricted Data may have been disclosed to unauthorized individual(s), the Incident Response Team will be notified. The Incident Response Team consists of: the Vice President of Information Systems, the Chief Compliance Officer, the Chief Financial Officer, the Director of Media Relations, the Director of Internal Audit, the Associate Vice President, Operations and a representative of the Provost's office.

4. The Incident Response Team will review the conclusions of the Investigative Team and will present a recommended response to the President. The Emergency Management Master Plan will be invoked if appropriate.

CHAPTER 16 – SENSITIVE DATA AWARENESS

Purpose.

The purpose of this chapter is to ensure that all members of the College community are informed and aware of the importance and legal obligation of protecting sensitive information.

Policy.

1. All associates are responsible for reviewing this Data Security Policy and affirmatively agreeing to comply with it. The Human Resources Department shall be responsible for distributing this Data Security Policy and tracking acceptance by associates.

2. During orientation, all new full and part-time associates, temporary workers and volunteers should be instructed on the importance of information security and their roles in protecting Sensitive Data.

3. Classes (online or in-person) shall be held periodically to continue to educate associates about this policy and the importance of sensitive data security. Successful completion of these classes shall be tracked by the Human Resources Department.

4. Managers shall ensure that associates under their supervision are aware of this Data Security Policy and other relevant information security policies, procedures, and guidelines, and have access to current versions. If modifications to policies are distributed, managers must inform their respective communities within seven days unless told otherwise.

5. Managers shall hold awareness and education sessions on an annual basis to review information security basics and current information security policies with associates under their supervision.

6. Third Parties authorized to access Sensitive Data must be informed of their responsibilities under this Data Security Policy. College information security awareness and educational materials shall be made available for use by authorized Third Parties.

CHAPTER 17 – PERIODIC POLICY REVIEW

Purpose. The purpose of this chapter is to define the process for periodic review and amendment of this Data Security Policy.

Policy.

1. A Data Security Policy Review Committee made up of the Incident Response Team (as defined in Chapter 15) and other representatives of the various College constituencies shall meet annually each Spring to review this policy and recommend any changes.

2. The chairperson of the Data Security Policy Review Committee shall be the Vice President of Information Systems.

3. The recommendations of the Data Security Policy Review Committee shall be submitted to the President for approval.

APPENDIX A

Categories of Restricted Data

Identity Data
Age/Date of Birth
Anonymous Donor Information
Bank/Financial Account Numbers
Citizenship/Nationality/Visa Status
Credit/Debit Card Numbers
Driver's License Numbers
Home Address
Home Telephone Number
Medical Records
Passport Numbers
Passwords
Social Security Numbers

Associate Data
Identity Data (listed above)
Compensation
Disciplinary Actions
Employee Benefits Elections
Employment Applications
Faculty Transcripts
Faculty Evaluations
Family Member/Beneficiary Information
Grievances
Performance Evaluations
Student Instructional Reports (SIRS)
Whistleblower Records
Worker's Compensation Claims

Student Data
Identity Data (listed above)
Academic Status
Admissions Application Records
Class Level
Class Schedule
Conduct/Misconduct Records
Course Evaluations
Disabilities
Ethnicity
Fees Assessed or Paid
Financial Aid Records
Financial Statements (Student or Parent/Guardian)
Gender
Grades (including GPA)
Health Care Providers
Instructors
Letters of Recommendation

Loan Collection Records
Parent/Guardian Name and Address
Residency Status
Selective Service/Veteran’s Administration Status
Special Programs
Student ID Numbers
Transcripts

Business and Financial Records
Audit/Investigative Workpapers and Reports
Bank/Financial Account Records
Data Subject to Confidentiality Agreements
Financial Statements
Injury and Damage Claims
Litigation Records
Marketing Plans
Proprietary Vendor Information
Tax Returns
Trade Secrets

Facilities
Architectural Records and Floor Plans
Building Systems Equipment Locations
Hazardous Materials Locations and Details
Utility Valve Locations