Procedure 9.0501

Information Classification Procedure

Contents

Introduction

Purpose

In order to preserve the appropriate confidentiality, integrity and availability of Beaufort County Community College's (BCCC) information assets, the College must make sure they are protected against unauthorized access, disclosure or modification. Information assets include, but are not limited to, all documents, materials, records, data and information that represent material value to the College and are produced, managed, or for which the College is otherwise responsible for as part of the day-to-day operation of the College. This is not just critical for assets covered by the Family Educational Rights and Privacy Act (FERPA), but also for all business conducted across the College, including, but not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- North Carolina State Laws and Regulations
- Payment Card Industry Data Security Standard (PCI-DSS)

Information assets are made up of different types of information and different types of information require different security measures depending upon their sensitivity. The College's information classification standards are designed to provide information owners with guidance on how to classify information and then use them accordingly.

Scope

This guide applies to all College information, irrespective of the location of the information or the type of device on which they reside. It should consequently be used by all staff, students, other members of the College and third parties who interact with information assets held by, and on behalf of, the College.

Any legal or contractual stipulations, not inconsistent with federal, state, or local laws, over information classification supersede these standards.

Assumptions

The legal definitions specified by FERPA and PCI Data Security Standard (PCI DSS) continue to be relevant concerning personally identifiable information requiring the appropriate levels of protection.

Information owners have sufficient technical knowledge to implement the controls and standards as specified.

Responsibilities

Members of BCCC:

THE College community consists of all employees of the College, College associates, and agency staff working for the College, third parties and collaborators on College projects are users of College information assets. They are responsible for assessing and classifying the information assets they work with, and applying the appropriate controls.

College community members must respect the security classification of any information as defined, and must report any concerns regarding information assets to the Information Security Manager as quickly as possible.

Information Owners

In order to ensure that all information is properly classified, it must have a designated owner to conduct the inventory, assign information to the appropriate category and determine the minimum level of protection. Those who create or are able to modify information share ownership of the information. Information Owners are responsible for assessing the information and classifying its sensitivity. They should then apply the appropriate controls to protect that information.

Information Technology:

Information Technology staff is responsible for providing the mechanisms or instructions for protecting electronic information while it is resident on any BCCC-owned or controlled system.

Records Management Staff:

Records management staff are responsible for providing the instructions for the protection and preservation of records, whether physical or electronic.

Records management staff is composed of an individual from each division, e.g. Academics, Con-Ed, etc. The identified divisional individual is responsible for the records management conformance within their division.

Information Security Advisory Board

The Information Security Advisory Board is responsible for the advising on and recommending information security standards on data classification.

The Information Security Advisory Board will include representatives from Senior Staff and other units as directed by the president.

Information Classification Definitions

Level 3 - Confidential

Level 3 information assets include confidential business or personal information, for which unauthorized disclosure would result in significant financial loss to the College, impair its ability to conduct business, or result in a violation of contractual agreements or federal or state laws or regulations.

Level 3 information assets are intended for very limited use and must not be disclosed except to those who have explicit authorization to view or use.

There are often governing statutes, regulations, standards, or agreements with specific provisions that dictate how level 3 information assets must be protected.

Regulations and laws that affect Level 3 information assets include, but are not limited to, the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS).

Level 3 information assets include, but are not limited to:

- social security numbers
- payment card numbers
- medical records, and
- restricted information protected by non-disclosure agreements

Level 2 - Restricted/Sensitive
Level 2 information assets include confidential business or personal information for which unauthorized disclosure could have a serious adverse impact on the College, individuals or affiliates.

Level 2 information assets are intended for a very specific use and should not be disclosed except to those who have explicit authorization to view or use.

There are often general statutory, regulatory or contractual requirements that require protection level 2 information assets.

Regulations and laws that affect information assets in Level 2 include, but are not limited to the Family Educational Rights & Privacy Act (FERPA)

Restricted and sensitive includes, but is not limited to:

- student data that is not designated as directory information, e.g. grades, classes and dates attended
- passport data
- personal financial information
- personally identifiable information (PII) such as name, birthdate, address, employee ID, etc. where the information is held in combination and could lead to identity theft or other misuse
- certain research data (e.g., proprietary or otherwise protected)

Level 1 - Internal
Level 1 information assets include information that is not openly shared with the general public but is not specifically required to be protected by statute or regulation.

Unauthorized disclosure would not result in direct financial loss or any legal, contractual, or regulatory violations, but might otherwise adversely impact the College, individuals, or affiliates.

Level 1 information assets are intended for use by a designated workgroup, department, or group of individuals within the College.

Note: While some forms of internal data can be made available to the public, it is not freely disseminated without appropriate authorization.

Level 1 information assets include, but is not limited to:

- budget and salary information
- personal cell phone numbers
- departmental policies and procedures
- internal memos
- incomplete or unpublished research

Level 0—Public

Level 0 information assets are purposefully made available to the public.

Disclosure of Level 0 information assets in approved form requires no authorization and may be freely disseminated without potential harm to the College.

Public information assets include, but is not limited to:

- advertising
- product and service information
- directory listings
- published research, presentations or papers
- job postings
- press releases
- course catalogs
- class schedules

Examples

Security Level	Definition	Examples	Analysis
3. Confidential	Normally accessible only to specified and / or relevant members of BCCC staff	Sensitive personal data: • racial/ethnic origin, • political opinion, • religious beliefs, • trade union membership • physical/mental health condition, • sexual life, • criminal record (including when used as part of primary or secondary research data) Salary information. Individuals' bank details. Draft research reports of controversial and financially significant subjects. Passwords. HR system data.	Data usually associated with standards such as HIPPA and PCIDSS. Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.

Security Level	Definition	Examples	Analysis
2. Restricted	Normally accessible only to specified and / or relevant members of BCCC staff or the student body	Reserved committee business. Draft reports, papers and meeting minutes. Strategic and financial information. Systems configuration and access procedures.	Data usually associated with FERPA. Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
1. Internal Use	Normally accessible only to members of the BCCC staff or the student body	Internal correspondence. Final working group papers and minutes. Committee papers. Information held under license. School policy and procedures.	Subject to scrutiny in relation to appropriate exemptions/ public interest and legal considerations

Security Level	Definition	Examples	Analysis
0. Public	Accessible to all members of the public	Annual accounts; Minutes of statutory and other formal committees. Pay scales. Staff Directory. Information available on the BCCC website or through other BCCC's Publications. Course information.	Freely available on the NC State government website, the BCCC website or through the BCCC's Publication Scheme.

Explicit information ownership and other rights of access to information
The College recommends that departments, functions and research projects explicitly designate information owners.

Other users may have rights of access to data according to the terms of engagement under which the data was gained or created.

Granularity of classification
The sets of information being classified should, in general, be large rather than small. Smaller units require more administrative effort, involve more decisions and add to complexity, thus decreasing the overall security.

Information Retention
There may be minimum or maximum timescales for which information has to be kept. These may be mandated in a research or commercial contract. Other forms of information retention may be covered by state or federal regulations: see NCDOR Retention Schedule for guidance.

Data Handling Examples by Classification Level

	Level				
SERVICE	0	1	2	3	COMMENTS
BCCC Owned Workstations, Laptops, Tablets, other devices	✓	✓			No level 2 or 3 data can be stored here. Mobile devices must have additional security configurations in place if storing level 1 data.
Publicly Accessible Kiosks and Workstations	✓				No level 1, 2, or 3 data can be stored here.
Personally Owned Workstations, Laptops, Tablets, other devices	✓				No level 1, 2, or 3 data can be stored here.
IT-Provided Network Drives (U: Z: Intranet SharePoint.)	✓	✓	✓		No level 3 data can be stored here. Level 2 data can be stored here only if additional security is in place such as limited access and/or encryption.
BCCC Email	✓	✓	✓		No level 3 data can be sent via email. Level 2 data is permissible if designated email recipients are authorized to view the data and no recipients' addresses are outside the College email system.
BCCC One Drive	✓	✓	✓		No level 3 data can be stored here. Level 2 data can be stored here only if additional security is in place such as limited access.
Public Cloud Storage Sites (e.g., OneDrive, Google Drive)	✓				No level 1, 2 or 3 data can be stored here.
BCCC websites (including public SharePoint, departmental websites, WIKIs, etc.)	✓				No level 1, 2 or 3 data can be stored here.

	Level				
SERVICE	0	1	2	3	COMMENTS
College learning management system (e.g. Blackboard)	✓	✓	✓		No level 3 data can be stored on the College learning management system. Level 2 data is permissible if designated viewers/recipients are authorized to view the data and no recipients are from outside the College system.
Computer Information System (e.g. Colleague)	✓	✓	✓	✓	*We need a description of what can be stored here.*
Third party learning management systems (e.g. *MyMathLab*)	✓	✓	✓		No level 3 data can be stored on third party learning management systems. Level 2 data is permissible if designated viewers/recipients are authorized to view the data and no recipients are from outside the College system.
Portable Electronic Storage Media, such as USB devices, CD/DVD, or external hard drives.	✓	✓			No level 2 or 3 data can be stored here. Portable storage media must have additional security configurations in place if storing level 1 data.

Users must contact the appropriate information asset owner and/or data security officer to identify the classification level of any service or application not listed above before posting or storing sensitive information in those locations. If you have any questions, please contact the designated information security officer.

Appendix A

Disclaimers

All documents should specify the classification as a standardized footer corresponding to the type and level of information.

Confidential

This document is confidential and proprietary to Beaufort County Community College and only authorized for those employees who have a business need for this information. Disclosure of this document in any manner to a third party is strictly forbidden.

Restricted

This document is restricted and only intended for use by employees of Beaufort County Community College. Disclosure of this document in any manner to a third party must be authorized.

Internal
This document is for internal Beaufort County Community College use only.

Public
This document is for Public use. NOTE: This disclaimer does not have to appear on any document or information asset deemed to be Public Information.

Appendix B
Data Security Incident Response Plan
Data security can be compromised in a variety of ways;

- Malware infection allowing unauthorized remote access into the system or unauthorized retrieval of data.
- Unintended disclosure on a public website or through physical or electronic mail.
- Payment card fraud involving skimming devices at point of sale terminals
- Lost or stolen paper documents or computing equipment (laptop, PC, or backup media).

In the event that paper or electronic records containing sensitive data are potentially exposed to unauthorized persons, the following protocol shall be executed.

Affected Unit:

1. Immediately contain and limit the exposure of data. Isolate compromised systems from the network (e.g., unplug the cable). Preserve electronic evidence. Do not shut down, reboot, access or otherwise alter the machine.
2. Alert the general counsel, the Information Services Security Team, and appropriate data owner(s).
3. Conduct a thorough investigation of the suspected exposure and maintain a log of all actions taken.
4. Provide the data owner(s), Information Services Security Team and General Counsel with an incident report identifying all information at risk and the source and timeframe of the compromise.
5. Notify affected parties if directed by General Counsel.
6. Remediate as directed by Information Services Security Team and the Data owner(s).

Information Services Security Team: (electronic records only) (ISO, Network Administrator, Computer Services Coordinator)

1. Gather information from affected unit to determine what sensitive data was exposed and when.
2. Create incident ticket and alert the appropriate data owner(s).

3. Determine root cause. Forensics on cloned hard drive, system log review, analysis of systems running in memory.

4. Determine data exfiltration. Network and system log review.

5. Remediate and return system to operation. Recommend how affected unit should clean the system.

6. Report all findings to Data Breach Response Team

7. Review and revise Information security program for adequacy of policy, standards and controls.

Data Security Incident Response Team: (Dean/Dir of the affected unit, data owners(s), ISO, affected unit VP, General Counsel, Media Relations and Public Safety)

1. Consider evidence provided by the affected unit, the data owner and ISO, and determine whether or not the following actions are warranted:

2. Engage local law enforcement, SBI, FBI, CIA.

3. Notify affected parties.

4. Notify other third parties for breaches involving; credit cards, educational records, health records, research subject data, donor information, or other record.

Data owner:

Records	Data Owner
Student records	Registrar
Employee records	Director Human Resources
Credit card or bank account data	VP Administrative Services VP of Continuing Education Foundation Director
Human Subject Data	VP Institutional Effectiveness and Research

1. Notify and report to other parties as required by rule or law.

2. Work with Media Relations and General Counsel on affected parties notification text and scripts.

3. Prepare a post mortem report with action log and remediation plan for affected unit.

The Data Breach Response Team will evaluate and refine the data breach response plan based on lessons learned in responding to potential breaches.

References

Legal References: *Enter legal references here*

SACSCOC References: *Enter SACSCOC references here*

Cross References:

History

Senior Staff Review/Approval Dates: *10/31/2016*

Board of Trustees Review/Approval Dates: *Enter date(s) here*

Implementation Dates: *Enter date(s) here*