|  |  |
| --- | --- |
|  | **COLLEGE of CENTRAL FLORIDA ADMINISTRATIVE PROCEDURE** |
|  | |
| **Title: Data Loss Prevention** | |
| **Page 1 of 5** | **Implementing Procedure For Policy # 3.24** |
| **Date Approved: 5/29/14** | **Division: Administration and Finance/Information Technology** |

# Purpose

Data Loss Prevention (DLP) encompasses the processes and rules used to detect and prevent the unauthorized transmission or disclosure of confidential information. The purpose of this procedure is to establish a framework of controls for classifying and handling college data based on the data’s level of sensitivity, storage location, value, and criticality to the college. The control elements of DLP help to ensure data is utilized in its intended manner.

数据丢失预防(DLP)包括用于检测和防止机密信息的未经授权的传输或泄露的过程和规则。本程序的目的是建立一个控制框架，根据数据的敏感性、存储位置、价值和对学院的重要性来分类和处理学院数据。DLP的控制元素有助于确保数据以其预期的方式被利用。

Confidential data can reside on or in a variety of mediums (pictures, paper documents, shred bins, physical servers, virtual servers, databases, file servers, personal computers, point-of-sale devices, USB drives and mobile devices) and can move through a variety of methods (human, network, wireless, etc.). The college relies on a variety of DLP strategies and solutions to prevent data loss. The college’s DLP strategies and solutions are reevaluated regularly to ensure their relevancy and effectiveness.

机密数据可以驻留在各种介质上(图片、纸质文档、碎片桶、物理服务器、虚拟服务器、数据库、文件服务器、个人计算机、销售点设备、USB驱动器和移动设备)，并可以通过各种方法(人工、网络、无线等)进行移动。学院依靠多种DLP策略和解决方案来防止数据丢失。学院的DLP策略和解决方案定期重新评估，以确保其相关性和有效性。

This security procedure applies to all college employees and users of the college’s computer systems. Individuals working for institutions affiliated with the college are subject to the same rules when they are using the college’s information technology resources or have any means of access to college data that has been classified as confidential or private.

本安全程序适用于所有学院员工和学院计算机系统的用户。在学院所属机构工作的个人在使用学院信息技术资源或以任何方式获取学院机密或私人数据时，也应遵守同样的规定。

# Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the college should that data be disclosed, altered or destroyed without authorization. Classification of data will aid in determining baseline security controls for the protection of the data. All institutional data is classified into one of three sensitivity levels (tiers), or classifications:

在信息安全的背景下，数据分类是根据数据的敏感程度以及数据被披露、篡改或销毁对学院的影响进行分类。数据分类将有助于确定保护数据的基线安全控制。所有机构数据都被划分为三个敏感级别(层次)之一，或分类:

## Tier1-Confidential Data

Data is classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the college or its affiliates. Unauthorized access to or disclosure of confidential information could constitute an unwarranted invasion of privacy and cause financial loss and damage to the college’s reputation and the loss of community confidence. Examples of Confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied.

当未经授权的披露、更改或破坏数据可能对学院或其附属机构造成重大风险时，数据将被列为机密。未经授权访问或披露机密信息，可能构成对隐私的无正当理由的侵犯，并造成经济损失和损害学院的声誉，以及社区信心的丧失。机密数据的例子包括受州或联邦隐私条例保护的数据以及受保密协议保护的数据。应该应用最高级别的安全控制

Access to Confidential 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 (“need-to-know”). Access to Confidential data must be requested for an individual and approved by the individual’s Vice President, Provost or Executive Director. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data.

## Tier 2-Internal/Private Data

Data is classified as Internal/Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the college or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data. A reasonable level of security controls should be applied to internal data.

Access to Internal/Private data must be requested for an individual and approved by the individual’s Vice President, Provost or Executive Director. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data. Access to Internal/Private data may also be authorized to groups of persons by their job classification or responsibilities (“role-based” access), and may also be limited by one’s department.

Internal/Private Data is moderately sensitive in nature. Often, Tier 2 Internal/Private data is used for making decisions, and therefore it’s important this information remain timely and accurate. The risk for negative impact on the college should this information not be available when needed is typically moderate. Examples of Internal/Private data include official college records such as financial reports, some research data, and budget information.

## Tier 3-Public Data

Data is classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the College and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public data should be protected. The impact on the institution should Level 3 Public data not be available is typically low, (inconvenient but not debilitating).

## Data Collections

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student’s name, address and social security number, the data collection should be classified as Confidential even though the student’s name and address may be considered Public information unless specifically marked as Do Not Publish.

数据所有者可能希望对具有共同用途或功能的数据集合分配单一分类。在对数据集合进行分类时，应该使用任何单个数据元素的最严格分类。例如，如果数据收集包含学生的姓名、地址和社会安全号码，那么数据收集应该被列为机密，即使学生的姓名和地址可能被视为公共信息，除非特别标明为“不公开”

## Restricted Data

“Restricted data” is a particularly sensitive category of Tier 1-Confidential data. Restricted data is defined as ‘any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transmission’.

“受限制数据”是一类特别敏感的一级机密数据。受限制数据的定义是“任何受法律或政策保护的机密或个人信息，无论在存储或传输中，都需要最高级别的访问控制和安全保护”。

Restricted data includes, but is not necessarily limited to:

* Personally Identifiable Information (PII)
* Private Educational Records protected under FERPA
* Credit card data regulated by the Payment Card Industry (PCI)
* Electronic Protected Health Information (ePHI) protected by Federal HIPAA legislation or Florida medical privacy laws
* Information specifically identified by contract as restricted
* Other information for which the degree of adverse effect that may result from unauthorized access or disclosure is high

受限数据包括但不一定限于:

* ▪个人识别信息(PII)
* ▪私人教育记录受FERPA保护
* 信用卡数据受支付卡行业(PCI)监管
* ▪电子健康信息保护(ePHI)受到联邦HIPAA立法或佛罗里达州医疗隐私法的保护
* ▪合同中明确规定的信息受限制
* ▪其他因未经授权访问或披露而可能产生严重不利影响的信息

## Restricted Data - Personally Identifiable Information (PII)

Unencrypted electronic information that includes an individual’s first name or initial and last name, in combination with any one or more of the following:

* Social security number
* Driver license number
* Financial account number, credit card number, or debit card number in combination with any security code, access code, or password

## Restricted Data - Private Educational Record (protected under FERPA)

Unencrypted electronic information that includes any one or more of the following:

* Name of the student’s parent or other family member
* Address of student’s family
* Personal identifier, such as the student’s social security number
* A list of personal characteristics that would make the student’s identity easily traceable
* Disciplinary status
* Financial aid, tuition, payments, account balances
* Grades, exam scores, or GPA (grade point average)
* Class roster
* Applications and admissions information
* Schedules
* Evaluations, forms, memos, or correspondence to and about the student
* Birth date
* Gender
* Citizenship
* Marital status

The student can create and manage their Personal Identification Number on the MyCF portal. College personnel will first verify that the PIN provided is the student’s current personal identification number before proceeding to discuss any of the student’s FERPA restricted data. The PIN cannot be used to authorize access to student records for anyone other than the student. In order to give permission to another individual to discuss student records, the student must complete and submit the Student Authorization for Access to Educational Records..

## Restricted Data - Payment Card Information (PCI)

Credit card account number with any of the following:

* Cardholder name
* Service code
* Expiration date

# Data Handling Requirements and Safeguards 数据处理要求和保障措施

Nearly 100% of college employees work on virtual desktop (VDI) terminals and their data files are stored on the college network. Automated data backups of all databases and file stores are run nightly. Networked data is stored off-site in a secure location.

几乎100%的高校员工在VDI终端上工作，他们的数据文件存储在高校网络中。所有数据库和文件存储的自动数据备份每夜运行。网络数据被储存在一个安全的位置。

For each restricted data classification, the data handling requirements and restrictions are defined to appropriately safeguard the information. All employees must adhere to the following requirements and restrictions regarding the storage and handling of unencrypted restricted data:

对于每个受限制的数据分类，定义了数据处理要求和限制，以适当地保护信息。所有员工必须遵守以下关于存储和处理未加密的受限制数据的要求和限制:

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Storage and Handling** | **PCI** | **PII** | **FERPA** |
| Network Shared Drive | No | Requires authorization | Requires authorization |
| Workstation  (*college owned and managed computer*) | No | Requires special authorization and should be rare | Requires authorization |
| Copying/Printing | No | Should only be printed for legitimate need.  Limited to employees authorized to access the data and who have signed a confidentiality agreement.  Print should not be left unattended on a printer/fax or in a public area.  Must be sent via Confidential envelope; data mus be marked  ‘Confidential’. | Should only be printed for legitimate need.  Limited to employees authorized to access the data and who have signed a confidentiality agreement.  Print should not be left unattended on a printer/fax or in a public area.  Must be sent via Confidential envelope; data mus be marked  ‘Confidential’. |
| Mobile computing devices (*laptops, tablets*) | No | No | Requires authorization.  Requires password protection |
| Removable media (*CDs, USB drives*) | No | Requires special authorization and should be rare.  Requires password protection. | Requires authorization. Requires password protection and encryption |
| Home and travel computer (*college owned and managed computer*) | No | Requires special authorization and should be rare.  Requires password protection. | Requires authorization. Requires password protection. |
| College Email communication | No | No | No |
| Electronic File Transfer | No | Requires secure FTP | Requires secure FTP |
| Cloud based commercial server (*hosted off campus, Dropbox*) | No | No | No |

|  |  |  |  |
| --- | --- | --- | --- |
| Personal email | No | No | No |
| Personally-managed computer (*home computer*) | No | No | No |
| Personal Smart Phone | No | No | No |

# Data Disposal Requirements and Safeguards

Paper documents that include confidential or private data and are ready for disposal must be properly shredded. Documents that are awaiting shredding must be stored in a secure location.

Electronic data files that contain confidential or private data should be deleted and completely removed from the trash, if applicable, as soon as they are no longer necessary.

Electronic devices that may have contained confidential or private data and are ready for disposal must be drilled or destroyed.

# Data Discovery

Data discovery is one of the key elements of a DLP program. Regardless of the amount of security controls that have been implemented, it is likely that confidential data may be at risk. The college relies on several strong discovery tools to conduct data discovery and to remediate potential data leaks. A data discovery assessment will be conducted regularly.

## Securing Data in Motion

Email is a primary form of college communications Email may at times include confidential data despite the restriction that unencrypted restricted data cannot be included within an email communication. To enforce compliance requirements for such ‘data in motion’, CF uses Cisco’s IronPort email security appliance. It provides more than 100 predefined DLP policies to detect sensitive data, numerous methods to handle DLP violations, and capabilities for reporting and auditing email security. If a sensitive message requires encryption, the message can be automatically quarantined or encrypted using the Cisco IronPort Email Encryption feature – an agentless encryption mechanism that does not require PKI certificates, key management, or any recipient training.

## Securing Data in Use and Data at Rest

CF uses Jenzabar CX/JX for the college’s Enterprise Resource Planning (ERP) system. The ERP data is stored within an Informix database and contains confidential data for students, employees and vendors. Auxiliary systems store data within SQL Server databases and may also contain sensitive data. Access to the confidential or sensitive data stored within these college databases is restricted to employees who need the data to perform their duties. CF uses network security, system security and secure data transmission procedures to prevent intentional or unintentional data leakage from the databases.

Employee generated data is unstructured and can be difficult to secure. There is a rapid and seemingly endless growth of employee generated data. A data discovery assessment will be conducted regularly to identify and protect confidential data when it has been stored in an unstructured environment. The college will use data discovery software to provide visibility into the content of data across all file systems, detect sensitive data, identify when the data was

stored, when the data was last accessed and who has access to the data. As a result, the confidential data will be deleted if it is no longer needed or encrypted if it must be retained.

# Employee Training and Awareness

Employees are instrumental to the success of the college’s data loss prevention (DLP) plan. Every employee must have a clear understanding of their role in protecting college data and they must be fully aware of the consequences that may result from a data breach. College employees are regularly exposed to training and reminders regarding data loss prevention, including:

* Broadcast IT Security email messages
* Employee IT Security training
* FERPA training
* IT Security messages on network time-out screens
* Red Flag Training

# Violations

Anyone who knows or has reason to believe that another person has violated this procedure shall report the matter promptly to his/her supervisor, department head or the Chief Information Officer. After a violation of this procedure has been reported or discovered, the issue will be handled as soon as possible to reduce harm to the college and its affiliates. Violators of this procedure may be subject to disciplinary action, up to and including the termination of employment depending on the severity of the violation or data breach.