Data Protection Policy 9.1.1.B - Data Classification and Data Types

Effective Date: 5/30/2014
Prior Effective Date: 7/1/2009

Data Classification and Data Types
Various data have different levels of sensitivity and their access is covered by different laws. The three types of classification used in this document are: Restricted, Controlled, and Public. The data trustee is ultimately responsible for deciding how to classify their data (see Roles and Responsibilities for list of data trustees). The restricted data category encompasses the most sensitive data. The list below is not meant to be complete. If you have any questions about how to classify data for these purposes, please contact the Office of Information Security at 513-558-ISEC (4732) or infosec@uc.edu for a recommendation.

Restricted Data: Any breach of data in this category must be reported to the IT@UC Office of Information Security and the unit head.
  • Personal identity information (PII) that consists of an individual’s name, including the last name along with the individual’s first name or first initial, in combination with and linked to any one or more of the following data elements:
    ▪ Social security number or partial social security number
    ▪ Driver’s license number
    ▪ State identification card number issued by the registrar of motor vehicles or a deputy registrar under section 4507.50 of the Ohio Revised Code, or an equivalent state identification card number issued by a similar agency in another state
    ▪ SSID
    ▪ Financial account number
    ▪ Credit card number
    ▪ Debit card number
    ▪ Electronically stored biometric information
    ▪ Protected health information e.g. HIPAA data
  • Data from research involving human subjects
  • ISO Number
  • Transcripts, defined as any cumulative listing of a student’s grades
  • Data that the university classifies or determines to be highly sensitive

Controlled Data: Breaches of data in this category should be reported to the unit head, who depending on the severity of the breach, may forward the information to the IT@UC Office of Information Security. Included in this category are:
  • Graded work, grade book, etc.
  • Data from research germane to intellectual property that is not categorized as “restricted”
  • Data whose integrity must be maintained
  • Other data as designated by the university

Public Data: Data that is readily available to the public. This data requires no confidentiality or integrity protection.
**Data Type:** Social Security Number (SSN)

**Classification:** Restricted

**Law:** Ohio Rev. Code 1347.15, FERPA, HIPAA

**Specific Examples of Restricted SSN Data:**
The Social Security Administration (SSA) issues three types of Social Security cards depending on an individual’s citizen or noncitizen status and whether or not a noncitizen is authorized by the Department of Homeland Security (DHS) to work in the United States. They include:

1. The first type of card shows the individual’s name and Social Security number only. This is the card most people have and reflects the fact that the holder can work in the U.S. without restriction. The SSA issues this card to:
   - U.S. citizens; or
   - Noncitizens lawfully admitted to the United States for permanent residence and noncitizens with DHS permission to work permanently in the United States (e.g., refugees and asylees).

2. The second type of card bears, in addition to the individual's name and Social Security number, the legend: "NOT VALID FOR EMPLOYMENT." The SSA issues this card to lawful noncitizens who do not have DHS permission to work, but are required by law to provide a Social Security number to get general assistance benefits that they have qualified for previously.

3. The third type of card bears, in addition to the individual’s name and Social Security number, the legend "VALID FOR WORK ONLY WITH DHS AUTHORIZATION." The SSA issues this card to people with DHS permission to work temporarily in the United States.

**Required Security Measures:**
- **Social security numbers or partial social security numbers** must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
- **Social security numbers or partial social security numbers** must never be stored on a non-university owned or operated computer or storage device.
- **Social security numbers or partial social security numbers** must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

**Recommended Security Precautions:**
- Whenever possible all UC-owned desktop computers and servers that contain SSN data are encrypted.
- Internal forms should be revised to eliminate unnecessary references to SSN.
- Paper copies of all documents with SSN should be stored in locked filing cabinets and should be shredded when discarded.

**Required Actions When Data is Compromised:**
Breaches or data that is lost or stolen must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.
**Data Type:** HIPAA

**Classification:** Restricted

**Law:** HIPAA, Ohio Rev. Code 1347.15 (if SSN is involved, see above)

**Specific Examples of Restricted HIPAA Data:**
- Patient Names
- Street address, city, county, zip code
- Dates (except year) for dates related to an individual
- E-mail, URLs, & IP #'s
- Social security numbers or partial social security numbers
- Account/Medical record #'s
- Health plan beneficiary numbers
- Certificate/license #'s
- Vehicle id’s & serial #' s
- Device id’s & serial #’ s
- Biometric identifiers
- Full face images associated with HIPAA records
- Any other unique identifying number, characteristic, or code
- Payment Guarantor's information

For more information, see the HIPAA web page. Health Insurance Portability and Accountability Act

**Required Security Measures:**
- **HIPAA data** must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
- **HIPAA data** must never be stored on a non-university owned or operated computer or storage device.
- **HIPAA data** must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

**Recommended Security Precautions:**
- Whenever possible all UC-owned desktop computers and servers that contain HIPAA data are encrypted.
- Paper copies of all documents with HIPAA data should be stored in locked filing cabinets and should be shredded when discarded.

**Required Actions When Data is Compromised:**
Breaches or data that is lost or stolen must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.
**Data Type:** FERPA

**Classification:** Restricted and Controlled

**Law:** FERPA (if SSN is involved, see above)

**Specific Examples of Restricted FERPA Non-Directory Data:**
- Transcripts, defined as any cumulative listing of a student’s grades
- Student Financial Services information
- Credit Card Numbers
- Bank Account Numbers
- Wire Transfer information
- Payment History
- Financial Aid / Grant information
- Student Tuition Bills

**Specific Examples of Controlled FERPA Non-Directory Data:**
- Graded work, grade book, etc.

  *Note that the following FERPA data may ordinarily be revealed by the university without student consent unless the student designates otherwise. If the student designates otherwise, then that data becomes classified as controlled. Separately, if any the following data is linked to any of the above specific examples of restricted or controlled FERPA data, then all data elements become either restricted or controlled depending on the classification above.*

- Name
- Date of birth
- Place of birth
- Directory address and phone number
- Electronic mail address
- Mailing address
- Campus office address (for graduate students)
- Secondary mailing or permanent address
- Residence assignment and room or apartment number
- Dates of attendance, i.e. specific quarter or semesters of registration
- Enrollment status
- UC degree(s) awarded and date(s)
- Major(s), minor(s), and field(s)
- University degree honors
- Institution attended immediately prior to UC
- ID card photographs for university classroom use
- UCID (unique identifier for all students)

**Required Security Measures:**
- **Restricted FERPA non-directory data** must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
- **Restricted FERPA non-directory data** must never be stored on a non-university owned or operated computer or storage device.
- **Restricted FERPA non-directory data** must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.
Recommended Security Precautions:
- Whenever possible all UC-owned desktop computers and servers that contain controlled FERPA non-directory data are encrypted.
- Faculty members utilize the grade book function on the university’s Blackboard course management system.
- UC employees are advised against storing controlled FERPA non-directory data on a PC or server not owned by the university. If the employee decides to store controlled FERPA non-directory data on a PC or server not owned by the university they must ensure that the appropriate physical and logical controls are in place to protect the data.
- It is recommended that whenever possible removable media containing controlled FERPA non-directory data be encrypted and stored in a secure, locked location. The university strongly discourages storing unencrypted controlled FERPA non-directory data on removable media.
- Paper copies of all documents with restricted or controlled FERPA non-directory data should be stored in locked filing cabinets and should be shredded when discarded.

Required Actions When Data is Compromised:
Breaches or data that is lost or stolen of restricted FERPA non-directory data must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.

Breaches or data that is lost or stolen of controlled FERPA non-directory data must be reported to the unit head, who depending on the severity of the breach, may forward the information to the IT@UC Office of Information Security.
Data Type: FERPA Directory Data

Classification: Controlled

Law: FERPA

Specific Examples of Controlled FERPA Directory Information:
Note that the following data may ordinarily be revealed by the University for Directory Information Purposes without student consent unless the student designates otherwise. If the student designates otherwise, then the following data elements must be treated as controlled data.

• Name
• Directory address and phone number
• Dates of attendance, i.e. specific quarters or semesters of registration
• Enrollment status, i.e. college, class (frosh, sophomore, etc...)
• UC degree(s) awarded and date(s)
• College and class
• Major(s), minor(s), and field(s) of study
• University degree honors and awards

Recommended Security Precautions:
• If the student designates not to reveal, then FERPA directory data may be disclosed only to UC employees and non-employees with a business need to know.
• Paper copies of all documents with FERPA directory data should be disposed of in a secure manner but need not be shredded.

Required Actions When Data is Compromised:
No action is required.
**Data Type:** Donor Information

**Classification:** Restricted

**Law:** HIPAA, Ohio Rev. Code 1347.15, PCI

**Specific Examples of Restricted Donor Information:**
- Name
- Credit Card Numbers
- Bank Account Numbers
- Social Security Numbers or partial Social Security Numbers
- Amount/what donated
- Telephone/Fax#
- Employment information
- Family information (spouse(s) / children / grandchildren)
- Medical History (alumni/family who have major medical procedures performed at University Hospital)

**Required Security Measures:**
- **Restricted Donor Information** must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
- **Restricted Donor Information** must never be stored on a non-university owned or operated computer or storage device.
- **Restricted Donor Information** must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

**Recommended Security Precautions:**
- Whenever possible all UC-owned desktop computers and servers that contain Donor Information data are encrypted.
- In the case of Credit Card information all 12 of the Payment Card Industry compliance steps should be followed: [https://www.pcisecuritystandards.org/security_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php).
- Paper copies of all documents with donor information should be stored in locked filing cabinets and should be shredded when discarded.

**Required Actions When Data is Compromised:**
Breaches or data that is lost or stolen must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.
Data Type: Faculty/Staff Housing

Classification: Restricted

Law: PCI, GLB

Specific Examples of Restricted Faculty/Staff Housing Data:
- Name / Spouse
- Credit rating / history
- Financial worth
- Income levels and sources, etc.

Required Security Measures:
- **Restricted Faculty/Staff Housing data** must be encrypted if stored or used on portable storage devices, removed from a secure university location, or if electronically transmitted.
- **Restricted Faculty/Staff Housing data** must never be stored on a non-university owned or operated computer or storage device.
- **Restricted Faculty/Staff Housing data** must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

Recommended Security Precautions:
- Whenever possible all UC-owned desktop computers and servers that contain Faculty/Staff Housing data are encrypted.
- In the case of Credit Card information all 12 of the Payment Card Industry compliance steps should be followed: [https://www.pcисecuritystandards.org/security_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php).
- SSNs should not be kept as part of this information. UCID's should be used instead.
- Paper copies of all documents with faculty/staff housing information should be stored in locked filing cabinets and should be shredded when discarded.

Required Actions When Data is Compromised:
Breaches or data that is lost or stolen must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.
Data Type: Research Information

Classification: Restricted

Law: HIPAA, Ohio Rev. Code 1347.15 (if SSN is involved), ITAR, EAR

Specific Examples of Restricted Research Information:
- Human subject information
- Lab animal care information
- Proprietary data as classified by an industry sponsor
- UC Proprietary or 3rd Party information
- Not in the public domain or being published information

Required Security Measures:
- Restricted Research Information must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
- Restricted Research Information must never be stored on a non-university owned or operated computer or storage device.
- Restricted Research Information must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.
- Restricted Research Information owned by an industry sponsor and classified as restricted data, for example proprietary data for the purpose of protecting from other industry competitors, must be contractually outlined between the university and sponsor as to all required security measures.

Recommended Security Precautions:
- Whenever possible all UC-owned desktop computers and servers that contain Research Information are encrypted.
- Research Information should be accessible only by those with a need to know.
- Paper copies of all documents with research information should be stored in locked filing cabinets and should be shredded when discarded, especially for human research data that contains personally identifiable information.

Required Actions When Data is Compromised:
Breaches or data that is lost or stolen must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine further notification requirements.
Data Type: Export Controlled Information

Classification: Restricted

Law: ITAR, EAR

Specific Examples of Export Controlled Information
- Any information that is labelled Export Controlled
- ITAR USML Category or EAR CCL ECCN
- Proprietary or 3rd Party information
- Not in the public domain or being published

Required Security Measures:
- Export Controlled data must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
- Export Controlled data must never be stored on a non-university owned or operated computer or storage device.
- Export Controlled data must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

Recommended Security Precautions:
- All UC-owned PCs that contain export controlled information must be secured with the appropriate physical and logical security controls to protect the data.
- Whenever possible all UC-owned desktop computers and servers that contain Export Controlled data are encrypted.
- Paper copies of all documents with Export Controlled data should be stored in locked filing cabinets and should be shredded when discarded.

Required Actions When Data is Compromised:
Breaches or data that is lost or stolen must be reported to the unit head and to the University’s Information Security Department via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.
Data Type: Employee Information

Classification: Restricted

Law: Ohio Rev. Code 1347.15, GLB

Specific Examples of Restricted Employee Information:
- Social Security Number or partial Social Security Number
- Name
- Date of birth
- Home address or personal contact information
- Benefits information
- Performance reviews
- Worker’s compensation or disability claims

Required Security Measures:
- Restricted Employee Information must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
- Restricted Employee Information must never be stored on a non-university owned or operated computer or storage device.
- Restricted Employee Information must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

Recommended Security Precautions:
- Whenever possible all UC-owned desktop computers and servers that contain Employee Information are encrypted.
- Employee information should be accessible only by those with a need to know.
- Paper copies of all documents with employee information should be stored in locked filing cabinets and should be shredded when discarded.

Required Actions When Data is Compromised:
Breaches or data that is lost or stolen must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.
**Data Type:** Business Information

**Classification:** Restricted

**Law:** Ohio Rev. Code 1347.15, GLB, PCI

**Specific Examples of Restricted Business Information:**
- Credit card numbers
- Bank account information
- Purchasing card (P-card) numbers
- Social Security or other Taxpayer ID numbers
- Contract information (between UC and third parties)

**Required Security Measures:**
- **Restricted Business Information** must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
- **Restricted Business Information** must never be stored on a non-university owned or operated computer or storage device.
- **Restricted Business Information** must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

**Recommended Security Precautions:**
- Whenever possible all UC-owned desktop computers and servers that contain Business Information are encrypted.
- In the case of Credit Card information all 12 of the Payment Card Industry compliance steps should be followed: [https://www.pcisecuritystandards.org/security_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php).
- Paper copies of all documents with business information should be stored in locked filing cabinets and should be shredded when discarded.

**Required Actions When Data is Compromised:**
Breaches or data that is lost or stolen must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.
Data Type: Management Data

Classification: Controlled

Specific Examples of Management Data:
- Faculty and staff reviews and evaluations

Recommended Security Precautions:
- All UC-owned PCs that contain management data must be secured with the appropriate physical and logical security controls to protect the data.
- UC employees are advised against storing management data on a PC or server not owned by the university. If the employee decides to store management data on a PC or server not owned by the university they should ensure that the appropriate physical and logical controls are in place to protect the data.
- It is recommended that whenever possible media containing management data be stored in a secure, locked location. The university strongly discourages storing unencrypted management data on removable media.
- Management data should be accessed by personnel with a need to know.
- Paper copies of all documents with management data should be stored in locked filing cabinets and should be shredded when discarded.

Required Actions When Data is Compromised:
No action is required.
Data Type: Legal Information

Classification: Restricted

Law: HIPAA, FERPA, PCI, GLB, Ohio Rev. Code 1347.15, ITAR, EAR

Specific Examples of Restricted Legal Information:
• Anything / Everything in the Office of the General Counsel

Required Security Measures:
• Restricted Legal Information must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
• Restricted Legal Information must never be stored on a non-university owned or operated computer or storage device.
• Restricted Legal Information must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

Recommended Security Precautions:
• All UC-owned PCs that contain restricted legal information, such as but not limited to, any and all data found in the office of general counsel, must be secured with the appropriate physical and logical security controls to protect the data.
• Whenever possible all UC-owned desktop computers and servers that contain legal information are encrypted.
• Paper copies of all documents with general restricted data should be stored in locked filing cabinets and should be shredded when discarded.

Required Actions When Data is Compromised:
Breaches or data that is lost or stolen must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.
Data Type: ISO Number

Classification: Restricted

Law: Ohio Rev. Code 1347.15, GLB

Specific Examples of ISO Usage:
- Bearcat Card
- Campus Recreation Center
- Parking and Housing
- Administration and operation of the Card Access/Badge system including creating ISO number replacement for lost badges Contract information (between UC and third parties)
- Remote student printing service
- Swipe UC IDs for Patron record checkouts in the libraries
- Campus dining and meal plans
- UC Bookstore
- Time clock in/out
- GradesFirst
- Tutor Trac
- DAAP System
- eProfessional
- Blackboard
- UCFi1eSpace
- Data Warehouse
- Identity Management

Required Security Measures:
- ISO must be encrypted if stored or used on portable storage devices, if removed from a secure university location, or if electronically transmitted.
- ISO must never be stored on a non-university owned or operated computer or storage device.
- ISO must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

Recommended Security Precautions:
- Whenever possible all UC-owned desktop computers and servers that contain ISO are encrypted.
- Paper copies of all documents with ISO should be stored in locked filing cabinets and should be shredded when discarded.

Required Actions When Data is Compromised:
Breaches or data that is lost or stolen must be reported to the unit head and to the IT@UC Office of Information Security via e-mail at infosec@uc.edu, who will determine notification and follow up requirements.
Related Links
The Data Protection Policy and all its subparts:
- Minimum Safeguards
- Data Classification and Data Types - (This Document)
- Roles and Responsibilities
- Acceptance of Risk Policy and Risk Acceptance Form
- Compliance and Remediation
- Summary of Applicable Laws
  (More detail on the applicable laws available on the IT@UC Office of Information Security website.)
- University Approved Cloud Storage

Contact Information
IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

History
Issued: 7/1/2009
Revised: 5/30/2014