Schedule A - Specific Fields

Specific *Confidential* Data Fields

Most educational and business records at Pepperdine University fall into the *Confidential* classification. While not an exhaustive list, below are listed some known *Confidential* data fields.

Educational Records

FERPA Covered Student Records. As defined by the U.S. Department of Education, "the Family Educational Rights and Privacy Act is a Federal law that protects the privacy of student education records." The specified privacy is preserved by applying Confidential data classification controls to these records Complete information can be found at the U.S. Department of Education website at http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

- Grades / Transcripts
- Class lists or enrollment information
- Student Financial Services information
- Athletics or department recruiting information
- Payment history
- Financial Aid / Grant information / Loans
- Student tuition Bills
- Date of birth
- Place of birth

Exception: The following FERPA data fields may ordinarily be revealed by the University without student consent and are classified Public, **unless** the student specifies they may not be revealed – questions about use of this data should be directed to the Registrar.

- Name
- Campus ID (as long as it cannot be used to gain access to password or PIN)
- Directory address and phone number
- Electronic mail address
- Permanent and/or mailing address
- Campus office address
- Residence assignment and room or apartment number
- Specific quarters or semesters of registration
- Degree(s) awarded and date(s)
- Major(s), minor(s), and field(s)
- University degree honors
- ID card photographs for University classroom use

Business Records

Employee Information

- Performance reviews
- Worker's compensation or disability claims
- Name in association with:
  - Salary or payroll information

- Date of birth
- Home address or personal contact information
- Benefits information

Management data

- Detailed annual budget information
- University investment information
- Non-anonymous faculty course evaluations
- Bank account numbers

General Information

- Email used to carry out University duties or conduct University business
- Information shared with legal counsel
- Internal departmental memos and other correspondence for internal-use-only

Specific RESTRICTED Data Fields

A small subset of data requires encryption or has a reasonable expectation that loss may result in large fines or disclosure costs; typically this type of data is classified RESTRICTED. Below is a comprehensive list of known RESTRICTED data fields:

Information Controlled by Law, Contract or Policy

- Credit Card Numbers
- Debit Card Numbers
- PIN Numbers
- Social Security Numbers
- Drivers License Numbers
- Authentication Secrets:
  - Biometric data used for authentication
  - Account passwords or lists of passwords
  - Secret cryptographic keys

HIPAA – Protected Health Information: As defined by the U.S. Department of Health and Human Services, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects individuals from the "wrongful disclosure of individually identifiable health information". In summary, HIPAA prohibits institutions from releasing patient information that can be traced back to a specific individual. Complete information can be found at the official HIPAA website http://www.hhs.gov/ocr/hipaa/. The following data, in relation to one's status as a patient, is considered **RESTRICTED** information.

- Patient names
- Street address, city, county, zip code
- Dates (except year) for dates related to an individual
- Telephone/Facsimile numbers
- Electronic mail, URLs, & IP addresses
- Account/Medical record numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identification & serial numbers
- Device identification & serial numbers
- Biometric identifiers
- Full face images
- Any other unique identifying number, characteristic, or code
- Payment Guarantor's information
- Records of past, present or future physical or mental health or condition

- Records of the provision of health care to the individual
- Records of the past, present, or future payment for the provision of health care to the individual

Specific Public Data Fields

Some data is published, as needed, publicly. These are examples only:

- Campus maps
- Business contact data (e.g., directory information)
    - Phone number
    - Email address
- Event and class schedules
- Campus-wide ID (CWID) - Created by Registrar as unique value equivalent to name - e.g. class roster use OK.

Alphabetical Table of Fields

Data Field	Classification	Note
Athletics Information	*Confidential*	
Authentication Secret such as: Account Passwords List of Passwords Secret Cryptographic Keys	**RESTRICTED**	
Bank Account Number	*Confidential*	Account and Routing Numbers
Biometric Data	**RESTRICTED**	When used for authentication
Budget Information	*Confidential*	
Campus Map	Public	
Campus-wide ID (CWID)	Public	Alternate for person's name
Course Enrollment Information	*Confidential*	
Course Schedule	Public	
Credit Card Number	**RESTRICTED**	
Debit Card Number	**RESTRICTED**	
Departmental Memo	*Confidential*	
Directory Information	Public	
Drivers License Number	**RESTRICTED**	
Email Address	Public	
Email Message Data	*Confidential*	Email for University duties
Employee Disability Claim	*Confidential*	
Employee Name in Association with Benefits Information Date of Birth Driver's License Number Home Address Personal Contact Information Salary or Payroll Information	*Confidential*	
Employee Performance Review	*Confidential*	
Employee Social Security Number	**RESTRICTED**	
Employee Worker's Compensation Claim	*Confidential*	
Health Center Information	**RESTRICTED**	See "Patient Health Information" below.
Legal Counsel Communication	*Confidential*	
Medical Records	**RESTRICTED**	See "Patient Health Information" below.
Password(s)	**RESTRICTED**	
Patient Health Information (PHI) including, but not limited to: Account Information Beneficiary Information Biometric Identifiers Condition/Diagnosis Records Email Address Guarantor's Information Health Plan Information Identification Number(s) Medical Record(s)	**RESTRICTED**	HIPAA prohibits institutions from releasing patient information that can be traced back to a specific individual.

Name(s) Payment Records Personal Contact Information Photographs Other Identifying Information Treatment Records		
PIN Number	**RESTRICTED**	Financial access or other PINs
Social Security Number	**RESTRICTED**	
Student Birth Date and Place	*Confidential*	
Student Financial Aid Information	*Confidential*	
Student Grades	*Confidential*	
Student Name in Association with Campus Address Degree(s) and Date(s) Awarded Email Address ID Card Photo Major(s), Minor(s) Field(s) Permanent and/or Mailing Address Personal Contact Information Residence Assignment Semester Registration Information University Honors	Public unless student requests to opt out, then *Confidential.*	These data fields may ordinarily be revealed by the University without student consent, unless the student designates otherwise.
Student Payment History	*Confidential*	
Student Social Security Number	**RESTRICTED**	
Student Tuition Bill Information	*Confidential*	
Student Transcripts	*Confidential*	
University Investment Information	*Confidential*	

Schedule B - Controls

Simplified table of Classifications and Controls

Classification	Control
Public	None
Confidential	Passwords
RESTRICTED	Encryption

The above table summarizes policy sections 4 & 5.

Controls Matrix by Classification and Process

Classification / Process	RESTRICTED	*Confidential*	Public
Acquisition	Must be: ● Legal to acquire ● Actively used	Must be: ● Legal to acquire ● Actively used	Must be: ● Legal to acquire
Access	Limited to those with University duties that require access and for whom it is legally appropriate to have access	Limited to those with University duties that require access and for whom it is legally appropriate to have access	Not limited: ● Publish as appropriate
Network Transmission	Data or entire transmission must be encrypted outside datacenter	As required on internal and external networks	As required on internal and external networks
Data Processing	Systems must use appropriate safeguards to prevent loss/disclosure	Systems must use appropriate safeguards to prevent loss/disclosure	As required on any system
Communication	Methods must prevent disclosure to unauthorized persons	Requires appropriate safeguards against disclosure	As required to all persons
Storage	Must be one of: ● Strong encryption using strong password or private key ● University central administrative database	Storage in a secure location with controls in place to limit access to those with University duties that require access	As required
Retention, Disposal, Transfer	According to Records Management Policy and Computer Disposal Policy		

The above table displays a matrix of the 5.0 Controls section of the Information Classification and Protection Policy.

Schedule C - Specific Technologies

Central Administrative Databases

*Central administrative databases are approved for unencrypted storage of **RESTRICTED** information.*

The current systems designated as the central administrative databases are:

- Peoplesoft System
- Centralized Document Management (Etrieve or Nolij)
- Accellion Attachments

Passwords

*Passwords are **RESTRICTED** data and must be encrypted in transit and at rest.*

The current University password standards for end users are published at:

- http://mypassword.pepperdine.edu

University clear text passwords may not be submitted to third party services for retransmission & authentication at the University, even over Transport Layer Security (TLS). This process necessarily involves passing the password in such a way that a bad actor or error at the third party would have access to the clear text password. Third parties must either use a supported single sign-on (SSO) option (e.g. CAS) or provide a system to be hosted and operated by Information Technology (IT) in an IT operated datacenter.

Access Controls for Confidential Information

Access to *Confidential* and **RESTRICTED** information in electronic records shall be controlled as follows:

- Use appropriate system or network permissions for the individual or group to restrict access to persons who need to know the data
- Authenticate access using one of the following sets of credentials:
    - University NetworkID and Password.
    - Other unique ID and a password that meets University password standards.
    - University NetworkID and Password along with a second authentication factor.
    - Best practice use of an approved University-supported single sign-on system.

Mobile Devices – tablets and smartphones

RESTRICTED information is NOT to be stored or transmitted via mobile devices. The necessary exceptions are the storage of the owner's password(s) in the operating system or in password managers recommended by the Information Security Office (see ISO website). Access to the mobile device and the password manager MUST be password protected (see password standards page for guidance).

Confidential information requires password-protected access. Since most mobile devices store and replay passwords automatically, *Confidential* information on mobile devices needs to be protected with a PIN or Password lock on timeout of 15 minutes or less. Use of profiles that allow the device to be remotely wiped via a manufacturer or University service are strongly encouraged to protect *Confidential* information on the device. Best practice includes: 1) using a password rather than a PIN and 2) setting the device to

auto-wipe on 10 consecutive failed accesses.

G Suite & Network File Shares

RESTRICTED information is NOT to be stored in G Suite or on network File Shares without approved additional encryption. Departments needing to file share RESTRICTED data should contact the information security office for consulting and encrypted drive (N: Drive) evaluation.

General Data Privacy Regulation (GDPR)

This EU law is being monitored closely at the time of publication. Currently, GDPR does not alter classifications of individual data fields. However, it may affect what data is legal to collect. University departments are advised to participate fully in upcoming data privacy reviews and follow advice of University counsel on changes to data collection and retention.

Technologies for Encrypted Network Transmission

Restricted information may NOT be transmitted on any network, outside an IT data center, without encryption.

Approved encrypted network transmission methods include:

- Encrypted Virtual Private Network (VPN) transmissions between secure computers
- Transport Layer Security (TLS) transport for network protocols
- Secure Shell (SSH v2) and related protocols, SFTP, SCP
- Remote Desktop Protocol (RDP) using encryption. The use of RDP for accessing servers without using certificates identifying those servers is deprecated.
- Secure email attachments server, attachments.pepperdine.edu – NOTE: this is only an approved method to secure the attachment; it does not secure the message text.
- Encrypted PDF files, using strong encryption. Password for said files is **RESTRICTED** data.

Technologies for Storage Encryption

Storage of **Restricted** information outside the central administrative databases requires approved strong encryption protected by a password or passphrase that meets University password standards.

Approved strong encryption methods include:

- Pretty Good Privacy (PGP or GPG) file encryption, where the key is secured by a password that meets University password standards for strength and storage.
- Encrypted Workstations with IT approved, centrally managed encryption and with a signed security agreement.
- IronKey or Kanguru USB flash drives protected by a password that meets University password standards.
- Enterprise backup encryption used by IT where the keys to the data are controlled in University datacenters.
- NOT APPROVED due to lack of central IT support: technologies not on above list.
- NOT APPROVED due to lack of enterprise management and password controls are: personally installed encryption technologies, including: Bitlocker, FileVault, TrueCrypt.

The use of other encryption technologies for safeguarding **Restricted** information is prohibited. The use of other encryption technologies for University business is deprecated because of the cost of supporting multiple & non-enterprise technologies and because IT cannot support data recovery or decryptions on other technologies in the event of investigation, data loss or employee departure.

For consulting on access control, and encrypted transmission and storage methods, please contact the Information Security Office.

Schedule D - Classification Examples

Classification Principle

The classification of the document or the system resolves to the highest classification of data fields therein.

Control Principle

The control to be applied to a document or system is the control that applies to the highest classification of data in the document or system.

Classification Examples

A staff member's email account contains a mixture of University community event announcements (Public data) and messages used to conduct University business (*Confidential data)*.

- Classification: *Confidential*
- Control: The email access must be secured with a password. The mailbox owner and delegates need their own separate passwords to access the messages.

A datacenter server contains a database a database with salaries (*Confidential* data) and Social Security Numbers (RESTRICTED data).

- Classification: RESTRICTED
- Control: All network transmissions must be encrypted to and from the server. The database may be encrypted or the SSN data field may be encrypted using University approved encryption.

A print out of a application for financial assistance contains the student's name (Public data), GPA (Confidential data) and Social Security Number (RESTRICTED data).

- Classification: RESTRICTED
- Control: Print out must be locked or supervised at all times.

Information Classification and Protection Policy Schedules

Policy Change Log		
Change Date	Change Description	Change By
4/16/2007	First draft approval and publication	K. Cary
10/31/2007	New revisions considering Phil Philips' feedback (provided 8/22/2007)	D. Gianforte
11/01/2007	New revisions considering K. Cary feedback	D. Gianforte
12/01/2007	Revisions based on Info Security Task Force feedback (my deliverables)	D. Gianforte
12/13/2007	Revisions based on Info Security Task Force feedback (classification reorder)	D. Gianforte
1/14/2007	Revisions based on Outside Council feedback	D. Gianforte
2/18/2008	Revisions based on latest Task Force feedback, new alphabetical schedule	D.G. / K.C.
8/22/2008	Revisions to wording based on General Counsel input at UMC approval	D.G. / K.C.
9/8/2008	Amend missing classification last row Schedule A alphabetical, make schedule C "transmission" match section 5.3 of the policy, complete missing sentence schedule D.	K. Cary
1/19/2009	Removed Drivers License Number from *Confidential* fields (it is **RESTRICTED**)	K. Cary
07/23/12	Updated Schedule C to reflect current technologies.	K. Cary
12/04/12	Updated Schedule C to reflect current technologies.	K. Cary
06/13/14	Updated Schedule A to reflect additional fields. Updated Schedule B with simplified controls table. Updated Schedule C to reflect current technologies. Increased consistency throughout.	K. Cary
7/22/14	Prepared for publication incorporating corrections from Registrar's office and Accellion info.	K. Cary
6/26/15; 7/15/15	Examples of popular unapproved encryption; Corrections from Finance on Bank Numbers; explicitly denies non-enterprise encryption	K. Cary
11/9/18	Formatting & clarification. Updates to data fields and control technology. Addition of schedule D (Classification Examples).	K. Cary A. Regan