University of California Hastings College of the Law

Information Security Program

I. Introduction and Purpose

In 1999, Congress passed the Gramm-Leach-Bliley Act ("GLBA"). One of the goals under GLBA is to assist financial institutions in protecting the security of individuals' non-public financial information. Although Hastings College of Law ("Hastings") is an educational institution, it is required to comply with GLBA regulations by adopting a program establishing guidelines to safeguard the security of personal financial information of its students, employees, donors, and others. Starting in 2018, GLBA (Gramm-Leach-Bliley Act) information security safeguards will be audited to ensure administrative capability for any institution receiving Title IV funds.

The purpose of the Hastings Information Security Program is to comply with the GLBA and to support the implementation of state and federal privacy protection laws with reference to

Confidential, Restricted and Sensitive (hereinafter "CRS") Information, computerized and in print), collected, processed and/or maintained by Hastings.[1] Under this Program, department managers with functional responsibilities requiring the collection or management of Confidential Information are required to take appropriate steps to protect such data within their departments and to notify individuals and designated Hastings personnel when an individual's Confidential Information has been disclosed through a breach of security.

This Program is designed to:

- Ensure the security and protection of CRS Information in Hastings' custody pertaining to employees, students, donors, clients, and others, whether in electronic, paper, or other forms against careless, accidental or intentional disclosure to unauthorized persons;
- Protect against any anticipated threats or hazards to the security or integrity of such Confidential Information;
- Protect against unauthorized access to or use of such Confidential Information; and,
- Provide appropriate measures in response to incidents which threaten the security of CRS Information.

The unauthorized modification, deletion, or disclosure of CRS Information can compromise the integrity of Hastings' programs, violate individual privacy rights, and is expressly forbidden. **Careless, accidental or intentional disclosure of CRS Information may result in corrective action up to and including, dismissal, expulsion, disciplinary action and/or legal action by the College.**

II. Scope

This Program applies to all nonpublic, personal CRS Information which may be contained in Hastings records that is collected, processed and/or maintained by Hastings in the ordinary course of business.

[1] In addition to the mandates of the GLBA, this Program is written to address a myriad of state and federal laws designed to protect the privacy of confidential personal information and sensitive information maintained by Hastings as a state agency in automated files or data systems against unauthorized disclosure. Such laws include The California Information Practices Act of 1977 (IPA), The California Computer Data Access and Fraud Act of 1987, and The Health Care Portability and Accountability Act of 1996 (HIPAA).
This Program does not address procedures to protect the privacy of student education records under the Family Education Rights and Privacy Act of 1974 ("FERPA"). FERPA regulations are contained in the Hastings College of the Law Student Record Procedures.

This Program applies to all members of the Hastings community including but not limited to Hastings organizations, employees, students, faculty, contractors and vendors retained by Hastings (hereinafter "Service Providers") and Hastings auxiliary organizations having Access to CRS Information collected processed and/or maintained by Hastings.

III. Definitions

Access means a personal inspection or review of the CRS Information or a copy of the CRS Information, or an oral or written description or communication of the CRS Information.

Confidential Information (as defined in Section 1798.2 of the California Civil Code) includes personal data collected and/or maintained by Hastings that includes an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security Number; (2) Driver's license number or California Identification Card number; (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Confidential Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Confidential Information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

CRS Information is "Confidential, Restricted, or Sensitive" information or data in printed or electronic format. See separate definitions for each type.

Custodian of Records are those department managers specifically designated by the Hastings General Counsel to accept and respond to a subpoena, court order, request for records under applicable provisions of federal and state laws, or other compulsory legal process, which involves the release of CRS Information.

Customer is an individual Consumer who has a financial relationship with Hastings. A Consumer is one who obtains or has obtained a financial product or service from Hastings that is to be used primarily for educational, personal, family, or household purposes. For example, students' who receive financial aid are Consumers who have a financial relationship with Hastings. Students, faculty, staff, and any other person who use their credit cards to purchase products or services from Hastings have a financial relationship with Hastings.

Disclosure means to permit access to or to release, transfer, disseminate, or otherwise communicate all or any part of CRS Information by any means, orally, in writing, or by electronic or any other means to any person or entity.

Financial Information includes but is not limited to credit card sales records, personal travel profiles, student loan records, and risk management claims records.

Handled means the access, collection, distribution, process, protection, storage, use, transmittal or disposal of information containing CRS Information.

Information Confidentiality and Security Agreement is a document (Appendix C) that all employees must sign, before they are granted access to CRS Information.

Information Proprietor is a department manager, or his or her chosen designee, who has either created or been given the responsibility for the existence, security and management of a database containing CRS Information within his or her own department.

Information Security Program Coordinator is the individual responsible for implementing the provisions of this Program. The Hastings General Counsel is designated as the Hastings Information Security Program Coordinator.

Permitted Disclosures means legally permissible disclosures of CRS as provided in The California Information Practices Act of 1977 (IPA) as provided in Appendix A2.[2] Most relevant to College operations is the exception which permits disclosure of personal information to those officers, employees, attorneys, agents, or volunteers of the agency which have custody of the information if the disclosure of the information is relevant and necessary in the ordinary course of the performance of their official duties and is related to the purpose for which the information is acquired.

Personal and public information means the information that *personally identifies or describes* an individual. Section 1798.29 of the California Civil Code, which enacts the security breach notification requirement of the IPA, defines the specific personal information that is subject to that section of the IPA. This "notice-triggering information" (name plus Social Security Number, driver's license or California identification card number, financial account number with a security code, medical information or health insurance information) should be classified as restricted information.

---

[2] The California Information Practices Act was enacted in 1977 to protect individual's privacy rights in "personal information" contained in state agency records. The Act reflects the Legislature's determination that the right to privacy is in jeopardy and that the maintenance and dissemination of private information should be subject to strict limits. The Act prohibits disclosure of personal information except in certain limited circumstances as provided in Appendix A.

Restricted Information describes any confidential or personal information that is protected by law or policy such as those referenced above and that requires the highest level of security protection, whether in storage or in transit. At UC Hastings, the term *restricted* also applies to personal information that is not Confidential according to the above definition and for which access is controlled by the College and may require authorization (e.g. student grades, employment documents, faculty evaluations).

Sensitive Information includes non-personal, institutional information that is not intended for distribution to the general public and whose integrity must be protected. Examples of sensitive information are College and departmental budget information and faculty meeting notes.

Service Provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to CRS Information through its provision of services directly to Hastings. For example, the College's auditors are Service Providers because they have access to CRS Information retained by Hastings as a function of the external audit review process.

Third Party means any individual (or individual on behalf of an organization) who is not an employee of Hastings.

IV. Functional Roles and Responsibilities

1) Information Security Program Coordinator

The General Counsel is designated the Information Security Program Coordinator ("ISPC"). The ISPC working closely with the Associate Dean for Library and Technology (Director of Information Technology "DIT") is responsible for implementing the provisions of this Program. The ISPC shall oversee the implementation of the Program by:

- Evaluating the effectiveness of the safeguards currently utilized by Hastings for controlling external risks to the security and confidentiality of CRS Information collected, processed and maintained by Hastings;
- Revising the Information Security Program as appropriate;
- Preparing and implementing policies to the Program that will be submitted to the Chancellor and Dean and Senior Staff for approval;
- Preparing an annual report on the status of the Information Security Program;

- Updating the Information Security Program as necessary;
- Maintaining the Information Security Program;
- Providing assistance to Custodians of Records in responding to third-party requests for CRS Information; and,
- Ensuring that Custodians of Records designations are current.

2) Director of Information Technology

The DIT shall work closely with the ISPC, department managers and all Hastings employees to maintain the security of databases utilized by Hastings in the collection, processing, and/or maintenance of CRS Information. These databases may exist on hard drives, including personal laptops, magnetic tapes, optical disks, diskettes, personal digital assistants (Pads), etc.

The DIT shall perform the following functions:

- Maintain and regularly update a record of personal laptop computers of Hastings Faculty and employees who utilize them to connect to the Hastings network to access or download CRS Information;
- Protect against unauthorized use of such records or information which could result in substantial harm or inconvenience to any customer;
- Report breaches in a timely manner and initiate remediation protocols immediately;
- Protect against anticipated threats or hazards to the security or integrity of such records;
- Assist department managers in taking inventory of the types of CRS Information that is stored on staff computers and Hastings network servers, collected, processed and maintained by Hastings within their department;
- Enable Encrypting File system on all computers on campus where feasible, including personal laptops that have access to CRS Information to add an extra layer of security for drives, portable drives, folders or files that contain CRS Information;
- Assist department managers in identifying reasonably foreseeable internal and external risks to the security and confidentiality of CRS Information;
- Provide assistance to Hastings department managers and Hastings employees where appropriate regarding the requirements of the Information Security Program;
- Provide assistance with training for those Hastings employees who have

access to CRS Information; deactivate e-mail and computer accounts upon an employee's separation of employment from the College;
- Identify appropriate password management conventions, including mandating and enforcement of strong password creation, password encryption and other security measures; and,
- Post the Information Security Program and subsequent modifications on the Hastings website and update it regularly.

2) Department Managers

Each department manager is responsible for ensuring that the guidelines set forth in this Program are followed for all databases containing CRS Information managed within their department. A distinction is made between the department that has a responsibility for the existence of a particular database and the department that has responsibility for operational support. The department that created or was given responsibility for the existence of the database as part of its business function is the "Information Proprietor" of the database and therefore has responsibility for its security and management, including required notification procedures. The department manager, who is the information proprietor, may delegate the role of "Information Proprietor" to a supervisor within the same department.

Department managers shall perform the following functions:

- Assist the DIT by taking inventory of and classifying the types of CRS that is stored on staff computers and Hastings network servers, collected, processed and maintained by Hastings within the department.
- Work with the DIT to identify the risks to the CRS Information ensuring appropriate security controls are in place to reduce risks and to protect the confidentiality of CRS Information collected, processed and/or maintained in their departments;
- Provide security of the repository where CRS Information is collected, processed and/or maintained within their departments;
- Protect the privacy rights of Hastings employees, students, and others as related to CRS Information that is maintained within their departments;
- Promote and encourage good security procedures and practices to protect private records within their departments;
- Identify and monitor risks to the security of CRS Information in their departments;
- Develop plans and procedures to preserve CRS Information within their departments in case of natural or manmade disasters;

- Ensure that employees in their departments who may have access to the Hastings network have read and signed the Information Confidentiality and Security Agreement in Appendix C;
- Perform ongoing assessments of employees in their departments to ensure that employees follow written procedures for information security, revoking system access when appropriate;
- Consult with the ISPC on requests for Confidential Information maintained by their departments prior to releasing such Confidential Information;
- Assist the ISPC and DIT in the preparation of an annual report that critically evaluates the adequacy of existing safeguards, compliance with the College safeguarding policies and procedure and that suggests the implementation of additional safeguards, if appropriate; and,
- Assist the ISPC and DIT with identifying and classifying automated filing systems, data systems and paper records that contain CRS Information to identify appropriate levels of precautions to protect these resources from unauthorized use, access, disclosure, modification, manipulation, loss, or deletion;
- At least once a year, review the status of each individual for whom an account has been established to determine whether authorization for access to CRS Information is still valid. Work with the IT Department to lock out or remove the accounts of those individuals who no longer meet authorization criteria.

3) Custodians of Records

Custodians of Records are certain department managers designated by the General Counsel who are charged with the responsibility for:

- Accepting all third-party requests for Hastings Records and information;
- Notifying the General Counsel of all subpoenas or other requested CRS Information;
- Releasing requested records and CRS Information in response to legally valid subpoenas, Public Record Acts requests, etc., as determined by the General Counsel; and,
- Notifying the ISPC of any such releases.

The Custodian of Records and department managers typically will be the first to notice an anomaly or security breach and may be in the best position to take steps to mitigate any further losses with respect to the unauthorized disclosure of CRS Information. The Custodian

of Records, department manager, must alert the ISPC and the DIT of reasonably suspected security breaches.

4) Employees and Affiliates

Employees and affiliates who have access to CRS Information are responsible for the security of computers and devices that they use or manage and shall:

- Participate in training regarding access and use of CRS Information;
- Sign an Information Confidentiality and Security Agreement (Appendix C); and,
- Comply with Hastings information security policies and procedures consistent with this Program, including taking appropriate steps to secure CRS information that they create, possess, manage or have access to in connection with their employment or research.

V. Risk Assessment

Confidentiality, integrity, and availability are the three primary security objectives cited in federal regulation regarding IT security.[3] These objectives describe the paramount goals for ensuring the protection of information and resources from unauthorized access, use, disclosure, disruption, modification, or destruction.

Confidentiality: preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The assigned level of confidentiality is used in determining the types of security measures required for its protection from unauthorized access or disclosure. These objectives describe the paramount goals for ensuring the protection of information and Resources from unauthorized access, use, disclosure, disruption, modification, or destruction.

Integrity: guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. The level of impact of unauthorized modification or destruction of information resources determines the importance of maintaining the integrity of a Resource.

Availability: ensuring timely and reliable access to and use of information. The overall importance of availability of a Resource is based on its criticality to the functional operation of a Campus or department or to the priority of that function in continuity plans and disaster

[3] *See* 44 U.S.C. sect. 3541, *et. seq,*.

recovery strategies. Emergency management planning must take into account the availability requirements of a particular Resource to determine its inclusion in emergency and disaster recovery planning.

The objective of risk assessment pursuant to the categories defined above is to develop contingencies for managing risks to the security of CRS Information. Risk assessments should consider the impact of potential harm that failure to achieve any of these security objectives would have on University operations, functions, image or reputation, assets, or the privacy of individual members of the University community.

A framework for categorizing impact into three potential levels of risk is offered by federal standards:

- Low: The event could be expected to have a limited adverse effect or negative outcome to the University or result in limited damage to College operations or assets, requiring minor corrective actions or repairs.
- Moderate: The event could be expected to have a significant adverse effect on the University or cause a significant degradation in its mission capability, place the College at a significant disadvantage, or result in major damage to College assets, or reputation requiring extensive corrective actions or repairs.
- High: The event could be expected to have a severe or catastrophic effect on College operations, assets, or individuals and could be expected to cause a loss of mission capability for a period that poses a threat to human life, results in a loss of major assets, or would result in severe financial impact or impact to the reputation of the College.

Reasonable, foreseeable internal and external risks to the security and integrity of CRS Information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information have been identified at Hastings.

An analysis of Security Objectives (confidentiality, integrity, availability) and the Security Impact (low, moderate, high) for information assets, in the context of the operational goals of the unit, shall determine which security measures should be implemented. For example, information assets with a low level of confidentiality but requiring a high degree of integrity and availability will require security measures that will ensure protection of the resource and its availability, but may require different levels access control measures. Some assets with a high degree of confidentiality may not require the same level of availability. Selected security measures for resources will differ depending on the outcome of the risk assessment.

VI. Management and Control of Risks

Hastings has developed the following general policies, practices and principles necessary to reasonably safeguard CRS Information:

A. Collection

CRS Information shall not be collected unless it is appropriate and relevant to the purpose for which it will be collected. It must be collected, to the extent practicable, from individuals directly and not from other sources. Where information is obtained from other sources, a record must be maintained of those sources from which the CRS Information was obtained.

B. Storage of CRS Information

1. Confidential Information

   Electronic files containing Confidential Information may be stored only on servers (clouded or on premise) managed by the IT Department. Specifically, Confidential Information may not be stored outside the IT Department, on servers managed outside the IT Department, on desktops and laptops, or on any type of portable electronic storage device with the exception of system backups generated by the IT Department.

   Confidential Information may not be transmitted electronically unless the information is encrypted.

   Paper files containing Confidential Information must be stored in a locked filing cabinet in a locked room, or on a temporary basis only, in a locked desk in a locked room.

2. Restricted Information

   It is recommended that electronic files containing Restricted Information be stored only on servers (on campus or in the cloud) managed by the IT Department.

   With the exception of Library servers, all servers containing Restricted Information must be managed by the IT Department.

   Electronic files containing Restricted Information may be stored on a

desktop or laptop computer only if the system is password protected. It is recommended that these files also be encrypted and be removed once they are no longer needed.

Restricted Information may be transmitted electronically only if access is password protected or data is encrypted.

Paper files containing Restricted Information must be stored in a locked desk or locked filing cabinet.

Portable storage devices containing Restricted Information must be stored in a locked desk or locked cabinet and the device must be password protected or have the Restricted Information data encrypted.

3. Sensitive Information

Electronic files containing Sensitive Information may be stored on a desktop or laptop computer only if the system is password protected.

Sensitive Information may be transmitted electronically only if access is password protected or data is encrypted.
It is recommended that paper files containing Sensitive Information be stored in a locked room, locked desk, locked cabinet, or other secure location.

It is recommended that portable storage devices containing Sensitive Information be stored in a locked room, locked desk, locked cabinet, or other secure location.

See the table in Appendix B for more detail.

C. **Exceptions to the Policy**

Any exception to these policies for the handling and storage of Confidential, Restricted, and Sensitive information must be approved and tracked by the Information Security Program (ISP) Coordinator.

D. Data Classification

Data classification is a key element for identifying appropriate levels of safeguards to

protect the security and integrity of computerized CRS Information. Data classification is essential to risk management. To that end, the State mandates that each year, Hastings shall certify that it has identified those automated files and data systems containing CRS Information utilized by the College in the ordinary course of business and that the College has adopted appropriate precautions to preserve their integrity and security.

E. Access

No Hastings employee shall be granted Access to centralized electronic data systems containing CRS Information in the custody of Hastings without review and written approval of their department manager for that department. The approval of Access to CRS Information will be based on several factors including the determination that access is required for the employee to perform a critical Hastings function that is part of the employee's job duties and responsibilities and assurance that all requirements contained in the Information Security Program designed to protect individual privacy and safeguard CRS Information will be met.

Employees with access to CRS Information complete a background check prior to being hired. Upon hiring, Hastings will provide employees approved for security access appropriate training regarding Hastings information security policies and procedures after which they shall be required to complete an Information Confidentiality and Security Agreement (Appendix C). A copy of the signed Information Confidentiality and Security Agreement will be retained in the individual's official personnel file.

Employees with approved access to electronic information will be assigned one or more accounts to access Hastings electronic information resources by the Information Technology Department. Hastings will deactivate email and all other computer accounts when an employee separates from the College. An employee approved for access to electronic information does not need to complete an additional CRS Information Access and Compliance Form for Access to non-electronic information. Any change in an employee's status or position, for example a lateral move to a different Hastings department, will trigger a review of the employee's approved access, and the employee's CRS Information Access and Compliance Form will be updated to reflect any changes.

Access to Hastings' computer systems and networks is provided through the use of individually assigned unique computer passwords. Passwords are automatically generated by the DIT to protect access to CRS Information. Passwords should be shared with other individuals only when the access provided by such passwords is limited to a specific electronic information resource, when such sharing is essential to

the continuity of an authorized business practice associated with that information resource, and when the other User is authorized to at least the same level of access privilege. Passwords to Essential or Restricted databases containing CRS Information including student data, personnel data, and/or fiscal data, such as provided by Colleague Systems, shall not be shared. When there is a need for shared passwords, the appropriate department manager and the DIT shall be responsible for authorizing and setting up specific accounts for that purpose. Each individual is responsible for all computer activity performed under his/her assigned password.

C. E-mail Usage Policy

CRS Information may be collected and/or maintained through the use of the College's electronic mail system, email. To help protect against security breaches, the Hastings Information Technology Department adopted an Acceptable Use Policy and Policy on Spam related to the use of Hastings e-mail and other computer resources. Consistent with these policies, Hastings employees should be cognizant that the Hastings e-mail system is for conducting business by or on behalf of the College although employees may send or receive personal messages via email and the College reserves the right at all times to access employee email messages. Employees should not access the email of any other employee without that employee's express permission, unless otherwise authorized by the Chancellor and Dean or the General Counsel.

D. Training

The ISPC, in conjunction with the DIT and Personnel Department shall coordinate the provision of training to all department managers and supervisors who have access to CRS Information concerning the Program requirements and their responsibilities under the Program.

All other Hastings employees having access to CRS Information will receive training from their department or administrative unit regarding Hastings Information Security Policy and Procedures relevant to that department, including this Information Security Program and the Privacy and Safeguarding Plan for their department or administrative unit.

E. Physical Security of Records

Each department shall ensure that all printed material containing CRS Information is protected against destruction, loss, or damage from potential environmental hazards such as fire, or water damage, to the extent possible. All members of the Hastings community are encouraged to assist the College in the protection of physical records by

reporting hidden or undiscovered environmental hazards to either department managers, the Facilities Department and/or the ISPC when appropriate.

F. Record Retention

The maintenance of records beyond the retention requirements set forth in the *University of California Records Disposition Schedule,* of which Hastings follows, presents a significant risk to the security and integrity of CRS Information. Due to space limitations, student, employee, financial or other records are sometimes stored in remote locations and periodic inspections to ensure record security must be conducted and documented. Longer retention must be is specifically approved by the appropriate department manager or Hastings General Counsel. All records containing CRS Information should be destroyed within three (3) months following the required period of retention.

G. Record Destruction

Record destruction is the responsibility of department managers. All records containing CRS Information shall be destroyed when retention is no longer legally required. Destruction mechanisms must prevent unauthorized access to CRS Information (e.g., shredding, erasing, modifying the personal information in records to make it unreadable or undecipherable through any means).

Prior to the survey and disposal of a campus computer or the transfer of a computer from one campus user to another user, the computer's hard drive shall be wiped clean of recoverable data using a low- level formal utility or other means to remove the operating system, software applications installed on the computer and any personal files which were stored on the computer.

Upon termination of Hastings employment, all network access, file access and e-mail accounts shall be disabled immediately. Department managers are authorized to extend an individual's e-mail account for up to six (6) weeks after termination after consulting with the General Counsel's Office. The Hastings General Counsel must approve any additional extension beyond the six-week period.

H. Department Privacy and Safeguarding Plan

The development and implementation of written department privacy and safeguarding plan is the responsibility of each department manager working closely with the DIT. While there is no prescribed document format, at a minimum, the plan must be dated and signed by the appropriate department manager, reviewed by the DIT and the ISPC, and must include:

1. Name of the office, department, or operation where CRS Information and/or is handled;
2. Identification of CRS Information handled;
3. Number of individuals with access to CRS Information;
4. Administrative controls implemented to minimize the number of individuals with access to CRS Information;
5. Description of physical security of records methods;
6. Discussion of records retention and destruction methods;
7. Discussion of training content, frequency, delivery method, etc.;
8. Discussion of business continuity plans; and,
9. Discussion of incident response procedures.

I. Service Provider Requirements

All new contracts with service providers entered into after the date of the adoption of this Program must include a privacy clause which requires the Service Provider to implement appropriate measures to safeguard CRS Information, to refrain from sharing any such information with any other party, and to comply with Hastings information security policies and procedures including those set forth in this Program.

At the discretion of the General Counsel, contracts with Service Providers may include the requirement that in addition to the insurance requirements for service agreements, the Service Provider must be bonded and must maintain personal liability insurance which, among other things, protects against allegations of violations of privacy rights of individuals as a result of improper or insufficient care on the part of the Service Provider.

VII. Required Disclosure of Security Breach

A security breach occurs when unencrypted CRS Information is reasonably believed to have been acquired by an unauthorized person. Good faith acquisition of personal information by a Hastings' employee or agent of Hastings for College purposes does not constitute a security breach, provided that the personal information is not used or subject to further unauthorized disclosure. If personal information in the Hastings database is encrypted, a breach occurs only if an access method was used, or is reasonably believed to have been used, that resulted in decryption; or if the data was compromised on a desktop or other platform that has acquired a clear text copy of that data.

Hastings is required to disclose any breach of system security to individuals whose unencrypted CRS Information was, or is reasonably believed to have been acquired by an unauthorized

person. Any Hastings employee, student, faculty, staff, consultant or any other person having access to Hastings CRS Information shares in the responsibility to immediately notify the department manager that is the proprietor of the disclosed information, or the ISPC of a security system breach.

VIII. Individuals' Rights

Individuals have the right to inquire and be notified about whatever CRS Information Hastings maintains concerning them. An opportunity to inspect any such CRS Information must be afforded within thirty (30) days of any request. If the record containing the CRS Information also contains CRS Information about another individual, that information must be deleted from the record before it is disclosed. Individuals may request copies of records containing any CRS Information about them, and those copies must be provided within fifteen (15) days of the inspection. Hastings may charge a reasonable per page cost for making any copies. Individuals may request that their CRS Information be amended and, if the request is denied, the individual may request a review of that decision by the General Counsel.

IX. Periodic Evaluation and Revision

Hastings shall periodically evaluate, test, and adjust its Information Security Program and departmental security policies and procedures, to validate that equipment and systems function properly and produce the desired results. Information security shall be included in all internal audits. Each year, an annual review of the Information Security Program shall be completed to ensure that it remains appropriate and relevant.

X. Incident Response Plan

The purpose of the Incident Response Plan is to minimize the effects of a breach in security.

When the breach is discovered, the Computer Emergency Response Team (CERT) responds immediately and takes the necessary steps to close the breach. This may include disconnecting the affected systems, tracking the perpetrators, restoring service, etc. CERT consists of the network administrator, the DIT, and administrators of the system(s) affected. Responding to the incident should also be accompanied by gathering information (logs, running processes, etc.) and investigating the incident. As soon as possible, the systems need to be restored. This may involve using backup hardware, patching or reinstalling the system. The incident needs to be reported to

the appropriate groups – local or federal authorities, incident response teams, and, impacted individuals.

Title IV schools must report on the day of detection when a data breach is even suspected. Information regarding the breach to the Education Security Operations Center (ED SOC) with the below data:

- Date of breach (suspected or known)
- Impact of breach (number of records, etc.)
- Method of breach (hack, accidental disclosure, etc.)
- Information Security Program Point of Contact – email and phone)
- Remediation Status (complete, in process – with detail) & next steps as needed

Security Awareness Training Program

The Human Resources department shall be in charge of making all employees aware of cardholder data security. Security awareness also includes, but is not limited to, the following topics: guarding passwords, strong passwords, unauthorized software, illegal software, backup, email attachments, maintaining confidentiality of cardholder data, password protection, and data storage. The training shall be done within 90 days of a person's hire. Retraining shall be done yearly.

XI. Appendix A: Permitted Disclosures

Hastings may not disclose CRS Information except in certain limited circumstances. The more common exceptions permit disclosure in the following circumstances:

- To the individual to whom the information pertains;

- Where the individual to whom the information pertains has given voluntary written consent to disclose the information to an identified third party no more than thirty (30) days before the third party requested it, or within the time limit agreed to by the individual in the written consent;

- To an appointed guardian or conservator of a person representing the individual provided it can be proven with reasonable certainty through Hastings forms, documents or correspondence that the person is the authorized representative of the individual to whom the information pertains;

- To persons within Hastings who need the information to perform their functions;

- To another government agency when required by law;

- In response to a request for records under the California Public Records Act (unless the Public Records Act provides an exception);

- Where there is advance written assurance that the information is to be used for purposes of statistical research only and where the information will be released in a form that does not identify any individual and such request is approved by the General Counsel;

- Where Hastings has determined that compelling circumstances exist which affect the health or safety of the individual to whom the information pertains, and notification is transmitted to the individual at his or her last known address, and disclosure does not conflict with other state or federal laws;

- Pursuant to a subpoena, court order, or other compulsory legal process if, before disclosure, Hastings notifies the individual to whom the record pertains, and if the notification is not prohibited by law and such request is approved by the General Counsel;

- Pursuant to a search warrant;

- To a law enforcement or regulatory agency when required for an investigation of unlawful activity of or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law.

XII. Appendix B: Guide for Handling and Storage of Confidential, Restricted, and Sensitive Information

P- Preferred
A - Acceptable
U - Unacceptable
UG - will grandfather Library and Bookstore for restricted and sensitive information
UE - unacceptable with designated exceptions
AT - temporary basis only
NR - not recommended

Form of Data	Storage Option	Confidential	Restricted	Sensitive
Electronic	IT-Managed Central Server in designated directories	P	P	P
Electronic	Server in the Library	U	A	A
Electronic	Server in the individual department	U	UG	UG
Electronic	Desktop with neither password protection nor encryption	U	U	U
Electronic	Desktop with password protection only	U	A	A
Electronic	Desktop with password protection and encryption	UE	A	A
Electronic	Laptop with neither password protection nor encryption	U	U	U
Electronic	Laptop with password protection only	U	A	A
Electronic	Laptop with password protection and encryption	UE	A	A
Electronic	Home computer	U	U	U
Paper	Individual staff or faculty desks - unlocked in unlocked room	U	U	U
Paper	Individual staff or faculty desks - locked in unlocked room	U	A	A
Paper	Individual staff or faculty desks - unlocked in locked room	U	U	A
Paper	Individual staff or faculty desks - locked in locked room	AT	A	A
Paper	Unlocked file cabinet in unlocked room	U	U	U
Paper	Locked file cabinet in unlocked room	U	A	A
Paper	Unlocked file cabinet in locked room	U	U	U

Paper	Locked file cabinet in locked room	A	A	A
Electronic	Email files with neither password protection nor encryption	U	U	U
Electronic	Email files with password protection only	U	A	A
Electronic	Email files with password protection and encryption	U	A	A
Electronic Portable Media	Individual staff or faculty desks - unlocked in unlocked room	U	U	U
Electronic Portable Media	Individual staff or faculty desks - locked in unlocked room	U	A	A
Electronic Portable Media	Individual staff or faculty desks - unlocked in locked room	U	U	A
Electronic Portable Media	Individual staff or faculty desks - locked in locked room	U	A	A
Electronic Portable Media	Unlocked file cabinet in unlocked room	U	U	U
Electronic Portable Media	Locked file cabinet in unlocked room	U	A	A
Electronic Portable Media	Unlocked file cabinet in locked room	U	U	A
Electronic Portable Media	Locked file cabinet in locked room	U	A	A
Electronic Portable Media	On person, at home, mobile	U	U	NR

XIII. Appendix C: Information Confidentiality and Security Agreement

To Be Signed by Employees (Staff, Faculty, Temps, Visitors, Etc.) or Outside Entities (Contractors, Vendors, Consultants, Agencies, etc.)

UC Hastings College of the Law ("Hastings") regards security and confidentiality of data and information to be of utmost importance. Further, it is the intent of this policy to ensure that confidential information, in any format, is not divulged outside of Hastings without explicit approval to do so by the Chancellor and Dean of the College. As such, the College requires all users of data and information to follow the procedures outlined below:

Policy on Confidentiality of Data
Each individual granted access to data and hard copy information holds a position of trust and must preserve the security and confidentiality of the information he/she uses. Users of College data and information are required to abide by all applicable Federal and State guidelines and College policies regarding confidentiality of data, including, but not limited to the Family Education Rights and Privacy Act (FERPA); Gramm Leach Bliley (GLB); and The Health Insurance Portability and Accountability Act of 1996 (HIPAA). All users of College data and information must read and understand how the FERPA, GLB and HIPAA policies apply to their respective job functions. All users with access to Colleague or other college computer systems acknowledge that they have read and agree to abide by the College's Acceptable Use Policy found at http://www.uchastings.edu/infotech under the sub-heading policies (also herein attached).

Any individual with authorized access to Hastings' computer information system, records or files is given access to use the College's data or files solely for the business of the College and must not divulge this information outside of the College except for approved College business requirements approved by the Chancellor and Dean of the College such as procurement of insurance and financial/banking requirements. Specifically, with respect to College records or information, individuals must:

1. Access data solely in order to perform his/her job responsibilities.
2. Not seek personal benefit or permit others to benefit personally from any data that has come to them through their work assignments.
3. Not make or permit unauthorized use of any information in the College's information system or records.
4. Not enter, change, delete or add data to any information system or files outside of the scope of their job responsibilities.
5. Not include or cause to be included in any record or report, a false, inaccurate or misleading entry known to the user as such.

6. Not alter or delete or cause to be altered or deleted from any records, report or information system, a true and correct entry.
7. Not release College data other than what is required in completion of job responsibilities.
8. Not exhibit or divulge the contents of any record, file or information system to any person unless it is necessary for the completion of their job responsibilities.

It is the individual's responsibility to report immediately to his/her supervisor any violation of this policy or any other action, which violates or compromises the confidentiality of data.

Security Measures and Procedures

All users of College information systems are supplied with individual user account(s) to access the data necessary for the completion of their job responsibilities. Users of the College information systems are required to follow the procedures outlined below:

1. All transactions, processed by a user ID and password, are the responsibility of the person to whom the user ID was assigned. The user's ID and password must remain confidential and must not be shared with anyone.
    a. Using someone else's password is a violation of policy, no matter how it was obtained.
    b. Your password provides access to information that has been granted specifically to you. To reduce the risk of shared passwords – remember not to post your password on or near your workstation or share your password with anyone.
    c. It is your responsibility to change your password immediately if you believe someone else has obtained it.

2. Access to any student or employee information (in any format) is to be determined based on specific job requirements. The appropriate Dean and/or Department Director/Manager is responsible for ensuring that access is granted only to authorized individuals, based on their job responsibilities. Written authorization must be received by the IT Department prior to granting system access.

    You are prohibited from viewing or accessing additional information (in any format) unless you have been authorized to do so. Any access obtained without authorization is considered unauthorized access.

    In order to prevent unauthorized use, the user shall log off of all applications that are sensitive in nature, such as employee/student personal information, when leaving their workstation. An alternative is to establish a workstation password or to lock your session. This is especially important during breaks, lunch and at the end of the workday.

Note: If you require assistance in establishing your workstation password, please access the screensaver documentation.

3. Passwords should be changed periodically and/or if there is reason to believe they have been compromised or revealed inadvertently. IT will change a password immediately if it has been compromised or revealed inadvertently.

4. Upon termination or transfer of an employee, Human Resources will notify the IT Department, who in turn will deactivate or modify the employee's network and systems accounts, and change all passwords.

5. Generally, students and temporary employees should not have access to the College record system. Written approval by the Dean and/or Department Director/Manager in charge of the respective area is needed if it is determined that access is required. The student or temporary employee is to be held to the same standards as all College employees, and must be made aware of their responsibilities to protect student and employee privacy rights and data integrity. Written authorization must be received by the IT Department prior to granting system access.
6. You agree to properly secure and dispose of any output or files you create in a manner that fully protects the confidentiality of records.
7. Confidential data files should be permanently maintained on network servers. Use of local hard drives or laptop computers or other storage media for maintaining confidential data must be approved by the appropriate Dean and/or Department Director/Manager.

Additionally, I understand that if granted access to process transactions via Colleague data entry screens, any information I enter or change will be effective immediately. Accordingly, I understand that I am responsible for any changes made using my ID. I agree not to share my ID or password with any other individuals and will notify Human Resources immediately if I believe my password has been compromised.

I understand that my access to College data and information systems is for the sole purpose of carrying out my job responsibilities and confidential information is not to be divulged outside of The College, except as previously stated. Breach of confidentiality, including aiding, abetting, or acting in conspiracy with any other person to violate any part of this policy, may result in sanctions, civil or criminal prosecution and penalties, employment and/or College disciplinary action, and could lead to dismissal, suspension or revocation of all access privileges. I understand that misuse of College data and information and any violation of this

policy or the FERPA, HIPAA or GLB policies are grounds for disciplinary action, up to and including dismissal. This agreement shall not abridge nor supersede any rights afforded faculty members under the Faculty Handbook.

I have read and agree to comply with the UC Hastings College of the law Information Confidentiality and Security Agreement and the Hastings Acceptable Use Policy (attached).

Name (please print): _____
Title and Department: _____
Signature: _____
Date: _____

XIV. Appendix D: Hastings Computer Resources Acceptable Use Policy

The following acceptable use policy covers use of E-mail and other Hastings computer resources. Use of such resources constitutes acceptance of this policy.

Hastings College of the Law provides computing resources, including E-mail, in support of the College's mission of teaching, research, and community service. Use of Hastings computing resources constitutes acceptance of this policy and agreement to comply with this policy. In addition, you should be aware that there is no guarantee of privacy or confidentiality with regard to E-mail/Internet communications.

Users of Hastings computing resources must respect the rights of other users, including the rights of copyright holders, abide by the security needs of the systems, and conform their behavior to all relevant laws, regulations, and contractual obligations of the College. In addition, all College regulations and policies apply, including the Student Code of Conduct, Academic Regulations, and the Staff Personnel Manual. Misuse of Hastings computing, networking, or information resources may result in disciplinary action. Additionally, misuse can be prosecuted under applicable state and federal statutes defining computer crime.

Confidential Information may be collected and/or maintained through the use of the College's electronic mail system, e-mail. Hastings employees should be cognizant that the Hastings e- mail system is for conducting business by or on behalf of the College although employees may send or receive personal messages via e-mail and the College reserves the right at all times to access employee e-mail messages. Employees should not access the e-mail of or use the e-mail credentials of another employee unless otherwise authorized by the Chancellor and Dean or the General Counsel.

Access to Hastings' computer systems and networks is provided through the use of individually assigned unique computer passwords. Passwords should be shared with other individuals only when the access provided by such passwords is limited to a specific electronic information resource, when such sharing is essential to the continuity of an authorized business practice associated with that information resource, and when the other User is authorized to at least the same level of access privilege. Passwords to Essential or Restricted databases containing Confidential Information including student data, personnel data, and/or fiscal data, such as provided by Datatel Systems, shall not be shared. When there is a need for shared passwords, the appropriate department manager and the DIT shall be responsible for authorizing and setting up specific accounts for that purpose. Each individual is responsible for all computer activity performed under his/her assigned password.

Policy on Spam

We have provided email services at Hastings to facilitate official communications between the school, its departments (including student organizations), faculty, staff, and students. Any email message that is unofficial and unsolicited is considered "spam" and represents an inappropriate use of Hastings computer resources.

Announcements from Hastings offices (the Records Office, Career Services, Student Services, the Academic Dean's Office, your faculty advisor), and any student group to which you belong that uses email is a legitimate means of communication.