Information Security Program
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 Datatel 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.

- ❖ Using someone else's password is a violation of policy, no matter how it was obtained.
- ❖ 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.
- ❖ 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.
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.
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 Datatel 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): _____

Department or Firm: _____

Signature: _____

Date: _____

Appendix D: Hastings Computer Resources Acceptable Use Policy

The following Acceptable Use Policy covers use of email and other Hastings computer resources. Use of such resources constitutes acceptance of this policy:

"Hastings College of the Law provides computing resources, including email, 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 email/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. Network Working Group RFC 1855, which provides netiquette guidelines, is incorporated by reference as part of this policy and is available at the Circulation Desk in the Law Library."

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" (see Dean Scallen's essay below on "The World of Spam") and represents an inappropriate use of Hastings computer resources.

The World of Spam According to Dean Scallen

Spam is the electronic equivalent of junk mail - mail you did not ask for and that you are not interested in receiving. Now, you may not like receiving your Visa bill, but hey, you asked for it by charging on that card. You also may not be interested in or have asked for notes from the I.R.S. or the DMV or the California Courts, telling you to show up for jury duty - but tough - these are official communications from authorized governmental agencies.

What kinds of email can you expect to receive? Announcements from Hastings offices (the Records Office, Career Services, Student Services, the Academic Dean's Office, your faculty advisor), the Hastings Bookstore, and any student group to which you belong that uses email as a means of communication.

If you hate junk mail that you receive via the U.S. Post Office, you can file a form with the Post Office that will prevent them from delivering it to you. There are few such mechanisms for email. You can ask a student group to take you off its distribution list, but then you would miss the important announcements relating to that student interest group. Spam clutters up your email box. Some people

get a lot of email, and they really don't want to spend time opening up stuff they didn't ask for and are not interested in (and they often have to open it to tell what it really is - at least with junk snail mail you have a major hint because it is sent via third class or bulk rate mail).

So, be a good citizen; don't send Spam, whether it be the email version or the Hormel version - the former makes people mad and the latter will smell after a day out of the can.