



**CENTRAL ADMINISTRATION INFORMATION TECHNOLOGY
Required Practices for Enterprise Security**

	Harvard Enterprise Security Policy	Central Administration Required Practice
1.1	<p>High Risk - SSN, Credit Card, Bank Account Information CA units must not store High Risk Confidential Information (HRCI) in any way relating to Harvard or Harvard sponsored activities on any individual user computer or portable storage device. Similarly units must not permit vendors or contractors to store SSNs.</p>	<p>Such information may be stored on protected servers or secure shared file systems. Central Admin staff members are responsible for on-going, active searching for the existence of high risk confidential data that may reside on their Harvard University personal computing and data storage devices and for prompt remediation of any/all found instances of such data.</p> <p>Central Administration Best Practice for implementing this requirement is IdentityFinder. See www.identityfinder.com</p>
	<p>CA units wishing to work with HRCI or to contact with a vendor to work with HRCI must obtain prior approval from the University CIO.</p>	<p>Central Administration units must contact the University Help Desk for instructions on obtaining access to HRCI.</p>
1.2	<p>High Risk - Human Subject Information CA units must ensure that all research that includes human subjects is approved by a Harvard Institutional Review Board (IRB) and all personally identifiable data collected for, used in, or produced by research involving human subjects is protected from inadvertent or inappropriate disclosure.</p>	<p>Central Administration units must notify the University Information Security Officer and the University Chief Information Officer prior to submission to the IRB.</p>
2.1	<p>Obtaining Harvard Confidential Information CA units must contact the University Help Desk for access to the core databases containing confidential information about Harvard people and to discuss data policy and handling requirements before development.</p>	<p>Harvard maintains central databases containing information on faculty, students, and staff. Local applications or directories must contact the Help Desk for access to these databases in order to maintain data integrity and consistency.</p>
2.2	<p>Protecting Confidential Information on Networks CA units must ensure that all confidential information is encrypted when transported across any network. Users must understand that normal email can not be considered a secure way to transport sensitive or confidential information, particularly outside of the local email server. Versions of email that encrypt the messages and attachments are used wherever a substantial amount of sensitive or confidential information is involved.</p>	<p>Except in extraordinary and rare circumstances, unencrypted email cannot be used for transport of confidential information. If there is no other method to meet a critical business requirement, units must submit a written request including the business justification and technical protection measures that will be employed to the Security Officer (scott_bradner@harvard.edu). He will review the request and forward to the Harvard CIO (dan_moriarty@harvard.edu) with a recommendation as to whether the request should be approved or not.</p>



CENTRAL ADMINISTRATION INFORMATION TECHNOLOGY
Required Practices for Enterprise Security

2.3	Making Confidential Information Available through Directories CA units must ensure that directory applications providing access to information collected by Harvard about individuals adhere to privacy preferences established by the individuals and maintained by Directory Services, including FERPA block requests.	<p>In some cases, otherwise public directory information must not be disclosed because the individual has requested confidentiality.</p> <p>Any online or published directory must adhere to privacy preferences as recorded in the ID Management system. Use LDAP in real time to access privacy preferences in the ID Management System.</p>
2.4	Identifying Users with Access to Confidential Information System owners must be able to identify users of systems that contain or access confidential information. Passwords must meet industry standards and not be shared.	<p>The password setting process must reject simple or guessable passwords, for example, passwords shorter than 8 characters, common names and words in various languages, sequences of numbers, or passwords that do not include at least one non-alphabetic character. Using the PIN or LDAP server will meet these requirements.</p>
2.5	Inhibit Password Guessing There must be a mechanism to limit the number of repeat attempts to log into an application with confidential information.	<p>A log should be kept of the timing (but not of the passwords that were attempted) of all failed logins. System administrators should be notified in cases where the number of failed attempts exceeds the threshold.</p> <p>Locking out users should take place after no fewer than six failed attempts, in order not to penalize users with complex passwords. For example, ten failed attempts is a reasonable number after which to lock out failed attempts. Alternately, significantly slow the process of login after no more than ten failed attempts.</p>
2.6	Limit Application Availability Time There must be a mechanism to time out a user's access to applications that deal with confidential information.	<p>The normal timeout should be no longer than 30 minutes. In non-enclosed office environments, where access to computers may not be controlled at all times, timeout should be set to 5 minutes or less.</p>
2.7	Limit User Access to Confidential Information CA units must ensure that only users with a specific business reason can access such applications. Access rights to servers with confidential information must reflect a user's university status.	<p>Granting access based on a specific business reason is a local management decision. The Harvard Auth Proxy service may be used to limit the access of employees whose jobs have changed or left Harvard.</p>
2.8	Confidential Information on Harvard Computing Devices CA units must ensure that Harvard confidential information is protected if it resides on a Harvard user's computer or portable storage device. Loss of a computer or device must not put Confidential Information at risk of disclosure. See also Policy 1.1 which prohibits storing HRCI on such computer or device.	<p>High Risk Confidential Information must <i>never</i> be downloaded or stored on any individual user computer. No Harvard Confidential Information can be stored on a computer not owned and maintained by Harvard. If Central Administration employees need to work at locations other than Harvard, the work must be done on a Harvard owned and managed computer and must have disk encryption installed and activated, and auto login to the computer and the disk encryption must be disabled.</p>



CENTRAL ADMINISTRATION INFORMATION TECHNOLOGY
Required Practices for Enterprise Security

		<p>Central Administration users must use PGP Whole Disk encryption software on all laptop computers and desktop computers that store confidential information. The PGP software encrypts the contents of the laptop or desktop computer hard drive and protects the data in the event the machine is lost or stolen while powered down.</p> <p>The use of fully encrypted USB devices is a required standard to protect Harvard Confidential Information being stored on portable data storage devices. Central Admin users refer to http://www.uis.harvard.edu/support_services/standards.pdf</p>
2.9	Internet access to Confidential Information CA units must ensure that no confidential information is saved on any computer able to be directly accessed from the Internet or open portions of Harvard's internal network.	<p>If access to Confidential Information is provided or requested via web or other Internet server, such servers must be stateless and must not store any such information on any disks that the servers can directly access (including remotely mounted disks).</p> <p>There must be a firewall between any such server and the Internet or open portions of Harvard's internal network. There must be a firewall between the user-accessible server and the database server.</p>
2.10	Confidentiality Agreements Some University employees who have access to confidential information are required by law or Harvard process to sign a confidentiality agreement.	<p>The University Confidentiality agreement is available at http://www.security.harvard.edu/protected_files/confidentiality_agreement.php</p>
2.11	Harvard University ID (HUID) Numbers Access to lists and databases of HUIDs should be restricted to person who have specific need for access.	
3.1	FERPA Directory Information CA units must ensure that they use the University common definitions of FERPA directory elements in order to promote a consistent understanding of what data elements about students might be considered public.	<p>The list of University common directory elements may be found at http://www.security.harvard.edu/for_students/ferpa_info.php No directory element that is not on the list may be published.</p>
3.2	FERPA Blocks CA units must ensure that they observe students requests that their directory information not be publicly displayed.	<p>Use LDAP to access FERPA flag in real time for directory information; use university-approved forms and procedures.</p> <p>Also, see 2.3 above. The FERPA flag is one of the privacy preferences referenced.</p>



CENTRAL ADMINISTRATION INFORMATION TECHNOLOGY
Required Practices for Enterprise Security

4.	Accepting Payment Cards CA units must only allow acceptance of credit cards as payment in accord with the Harvard Credit Card Merchant Handbook.	Harvard Cash Management approval must be obtained in order to institute any planning for a credit card payment system.
5.1	Physical Environment Whether in Harvard offices or at off-site locations, all confidential information in paper or magnetic media form must be properly protected. Computers containing confidential information must be physically secure. Physical access to any facility that is sensitive for any reason should be appropriately secure.	Confidential paper records should be kept in locked file cabinets except when actually being used. FAX machines used to receive confidential information should be in locked protected areas. A locked room should not be considered a secure location if the room is cleaned at night by a janitorial crew. Computers that contain confidential information should be located in computer facilities where the access is controlled and monitored or, in rare cases, secured in locked cages in other locations. Physical access to any facility that is sensitive or contains sensitive information should be protected by appropriate means of control. Note: HUPD and the Facilities Security Task Force will be publishing a set of physical security requirements for different types of facilities and alternative methods of implementation.
5.2	Recording Information About the activities of individuals CA units that maintain logs or generate records of actions of individuals must adopt written policies on the protection, retention, and access policies for such logs and records.	A statement of what information is being collected about an individual, why that information is being collected, how long that information will be kept and who will have access to the information must be developed for each such collection of information. This includes logs produced by building access control systems, web servers or other computer applications and surveillance camera recordings. Such statements should be made available to the individuals who are the subjects of the information collecting activity by posting them, by distributing them or by making them available upon request. In most cases conspicuous signs should note the presence of surveillance cameras. If there is no intent of deterrence, there is no requirement to post this notice.



**CENTRAL ADMINISTRATION INFORMATION TECHNOLOGY
Required Practices for Enterprise Security**

6.1	<p>Contracts CA units must ensure that vendors dealing with Harvard confidential information have a written contract covering their services including the proper contract language requiring the protection of Harvard's information. CA units working with vendors for the collection of HRCI must obtain prior approval from the University CIO.</p>	<p>See http://www.security.harvard.edu/for_vendors/index.php</p>
7.1	<p>Computer Operation CA units must ensure that the computer environment is secure, patches are up to date and the machines are operated in a way to minimize the chance of a security breach; only required applications are enabled on a computer.</p>	<p>For Central Administration departments the standards, policies and procedures implemented and followed by UIS Desktop and LAN Services comprise the base set of requirements for desktop/laptop/PDA computer operation.</p> <p>http://www.uis.harvard.edu/support_services/policies.php</p> <p>http://www.uis.harvard.edu/support_services/standards.pdf</p> <p>For securing the physical environment, see 5.1 above.</p>
7.2	<p>Computer Setup CA units must ensure that the computer environment is properly protected by filters to protect the applications.</p>	<p>See http://www.security.harvard.edu/tech_security/comp_setup.php</p>
7.3	<p>Target Computers Computers that may be broken into because of the information they contain or the resources they control need special protection.</p>	<p>In cases where connection to the network is a business requirement, target systems should be physically secure and connected to special network segments that are dedicated to such systems</p> <p>For systems containing High Risk Confidential Information or building access control or building system control information, special protections are required. See Discussion at Policy 7.3 at http://www.security.harvard.edu/policy/index.php</p>
7.4	<p>Network Take-down and Vulnerability Scanning Network managers are authorized by the University to run vulnerability scans. Network operators should monitor network activity for signs of attach and take action in the absence of action by the computer operator.</p>	<p>In Central Administration, University Information Systems (UIS) monitors the network and will disconnect a computer suspected to be compromised.</p>
8.	<p>IT Service Resumption The security and availability of confidential information must be assured in case of a declared disaster. Each business area</p>	



CENTRAL ADMINISTRATION INFORMATION TECHNOLOGY
Required Practices for Enterprise Security

	using confidential information must develop and document a business continuity plan containing disaster recovery timeline, methodology, documentation, procedures, and action steps.	
9.	Federal and Regulatory CA units must adhere to state and federal and regulatory statutes in addition to Harvard policies. Massachusetts law imposes specific requirements for the proper destruction of electronic and paper records containing HRCI and reporting improper access to or use of such records.	
9.1	Disposition and Destruction of Records Electronic or physical records containing confidential information must be properly disposed of.	Contact University approved vendor Data Shredder for secure paper destruction. Scott Hovan 800-622-1808 Data Shredder Find out more about Harvard's partnership with Data Shredder http://vpf-web.harvard.edu/ofs/procurement/ven_par_dsr.shtml
9.2	Reporting Security Breaches Known or suspected breaches in the security of Harvard Confidential Information must be reported to the University Office of General Counsel.	For loss of a laptop containing potentially high risk information contact the Office of General Counsel (Mary Anne Mendes 617-495-1280 or mary_anne_mendes@harvard.edu). For loss of a laptop with no high risk confidential information contact the University Helpdesk (617-495-8411). If the theft occurred on campus notify Harvard University Police: Phone: 617-495-1212 or 617-495-1215. If the theft occurred off-campus, file a police report in the city where the theft occurred.
10.	Web Based Surveys and Other Data Collection Tools Data collection tools that request confidential information must ensure that responses cannot be accessed by unauthorized persons and that confidential information is not improperly disclosed or shared. CA units must ensure that if a vendor is involved in conducting surveys or analyzing results that include confidential information, the appropriate contract rider must be in place.	