IT Professional Code of Conduct to Protect Electronic Information

In the course of supporting the business of the University, IT staff performing regular duties may have access to data in applications, emails and file systems or on desktops, servers and networks and other systems that must be protected by the University. In performing their duties IT staff will comply with applicable University policies including the Harvard Information Security Policy and Harvard Electronic Communications Policy.

As a Harvard IT organization,

- IT staff will receive communications and training on the Code of Conduct
- IT staff will be required to annually review and affirm the Code of Conduct
- IT leadership will provide guidance on this Code of Conduct as challenges are observed or encountered.
- IT leadership will review and revise the Code of Conduct as needed in response to any incidents or as technology changes

As IT professionals,

- We have access to user's electronic information[1], some of which may be personal and confidential
- We require access to user's electronic information in order to develop, test, implement and support the University's applications, systems and networks and to ensure they run properly; to protect against threats such as attacks, malware, and viruses; to protect the integrity and security of information; to help support business continuity; and to help deal with threats to campus safety and the safety of individuals.
- It is part of our job to help protect all user's electronic information from unauthorized access

As IT professionals,

- We only obtain the information we need to perform our job or which we have been directed to obtain by proper University or legal authorities

[1] For definition of "user's electronic information" see:
http://hwpi.harvard.edu/files/provost/files/policy_on_access_to_electronic_information.pdf

- We only use the information gathered for the purpose for which it was obtained, properly protect the information while in our possession, and dispose of it properly once it is no longer needed for business purposes
- We will not peruse or examine user's electronic information for any purpose other than to address a specific issue
- We understand any failure to meet the Code of Conduct is considered a violation of trust and is grounds for disciplinary action up to and including dismissal
- We will sign a yearly acknowledgment that we have received, read, and understood this Code of Conduct

Below are some examples of the Code of Conduct in practice. These are meant to be representative and helpful, but not comprehensive. If a need arises for exceptions to the principles and examples in this Code of Conduct document, approval must be obtained from the University CIO, University CSO or school CIO.

Field Technicians	• Technicians must never request or ask a user for their password or PIN and must not observe a user entering their password or PIN • Technicians must not open emails or files while troubleshooting an issue unless the user gives specific permission and must examine only the content of emails or files as required to troubleshoot a particular problem • Remote access to a desktop for support purposes can only occur with the approval of the end-user via a specific desktop prompt
Quality Engineers, Developers, Project Managers and Business Analysts	• When developing, testing analyzing, maintaining or troubleshooting issues in University applications, records should be only be interrogated if they are related to the problem being investigated. • When showing examples of pages, files, business flow or report output in documentation, appropriate measures should be taken to disguise the information to protect the identity of the individual(s) associated with the data • For purpose of presentation, development, testing, analyzing, maintaining, or troubleshooting, appropriate measures should be taken to disguise the information to protect the identity of the individual(s) associated with the data
Network engineers	• Data traversing the network must not be monitored except for maintenance, specific diagnostics and system protection purposes (e.g. virus protection scanning) • Access to log information must only be used for business purposes and as required to support the integrity of systems

Helpdesk staff	• Never ask users for passwords or PINs • Only enable email forwarding to another designation when requested by the mailbox owner
System Administrators & DBAs	• Data contained in log files and databases should not be disclosed beyond the need of the IT group to develop, maintain, troubleshoot or perform diagnostics unless under direction from proper University or legal authorities • Information about a specific user's access to networks, systems, databases, or any other computer-based resources must not be disclosed to anyone beyond the owner unless under direction from the proper University or legal authorities or for the purposes of development, testing, maintenance, protection and support of an IT system • The casual viewing of any data contained in logs or databases that fall outside of an employee's job responsibilities is strictly prohibited
Production Control and Computer Operations	• All physical access to University IT Data Centers must follow established access management protocols; all requests for access from unauthorized individuals must be referred to a supervisor or manager • All requests for access to systems must follow established access management protocols; all requests for systems access that fall outside of the specific ones covered by the access management protocol must be referred to a supervisor or manager • All requests for privileged access to production systems must follow the established procedures for granting such access, including the timely and accurate logging of the request and the timely reverting of privileges upon completion of the work that prompted the request for privileged access

Security Engineers	• Harvard's information security professionals adhere to a stringent code of ethics through their certification by the International System Security Certification board, which requires that they:
	1. Protect society, the commonwealth, and the infrastructure
	2. Act honorably, honestly, justly, responsibly, and legally
	3. Provide diligent and competent service to principals
	
	• When launching an **investigation** in response to an alert about possible malicious activity (from an automated tool, a user, or a third party), security engineers must act in a responsible and ethical manner, specifically:
	  • Investigate only within the scope that has been identified by the alert and for the identified reason
	  • Track the malicious activity to an originating machine and contact the owner and their IT support, sharing the information and assisting in a resolution process

	• Should an individual decline to participate in the resolution, security engineers must:
	  • Launch an escalation process to obtain management approval prior to further action
	  • Follow the defined escalation path which includes notice to local management, CISO, HR, and OGC
	
	• When conducting **forensics** on an acquired computer, security engineers must:
	  • Limit their investigative activities narrowly, working on only relevant information
	  • Only look at individual personal information if it is required for the investigation.
	  • Keep physical and digital investigation materials (e.g. copy of a hard drive) securely locked
	  • Maintain a chain of custody for evidence, requiring responsibility and signoff for each step of the process