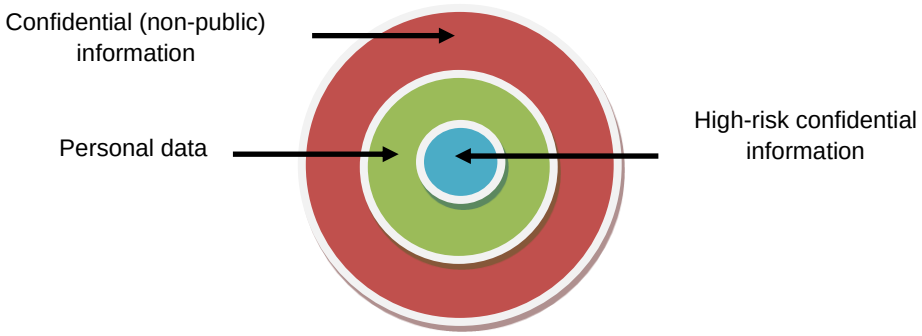
Seattle University Data Privacy Policy

Last updated: July 1, 2011

Definitions

The data privacy policy is based on a tiered definition of confidential information; these definitions are intended to facilitate compliance with privacy laws and are consistent with widely used terminology.



Confidential information ("CI") is the most comprehensive category and covers all **non-public information** about Seattle University and its stakeholders, including employees, students, and donors. The university assumes that all employees have access to some form of confidential information. Some examples of confidential information are budgets, prospective student information, contracts with third parties, and business plans. If something is not public information, it is considered confidential by default.

Personal data ("PD") is a subset of confidential information that is information about people. Examples include educational records, health and medical information, credit card numbers, and employment records.

A subset of personal data is classified as high-risk, either because the exposure of this information can cause harm or because the information is specifically protected under law. **High-risk confidential Information** ("HRI") includes an individual's name in conjunction with the individual's (1) Social Security, credit or debit card, individual financial account, driver's license, state ID, or passport number, (2) human subject information or personally identifiable medical information, or (3) biometric information. In general one may think of high-risk confidential information as personal data associated with a name; extra care must be taken to protect high-risk confidential information in both electronic and paper form.

The data privacy policy applies to these categories in different ways. Policy statements are labeled CI, PD, or HRI to make it easier to distinguish between them. Anything that applies to confidential information also applies to the subsets of personal data and high-risk confidential, and likewise, anything that applies to personal data applies to high-risk confidential information.

Policy

Basic Data Privacy Policy

CI: Seattle University protects confidential information.

PD: Seattle University does not collect, transmit or store personal data unless there is a business need to do so. Government-issued ID numbers (such as social security numbers) are only used when there is a clear business requirement that has been approved by the chief information officer (CIO).

Sharing Personal Data with Third Parties

PD: Seattle University does not share personal data with third parties with except in the following four situations: (1) when individuals have provided prior consent, (2) when third parties act as agents of the university and adhere to data privacy standards that meet or exceed the university's standards, (3) when participating in higher education data exchange consortia or research studies where providing such data is necessary and the parties receiving the data adhere to data privacy standards that meet or exceed the university's standards, and (4) when compelled to do so under the law. Disclosure in the fourth situation requires approval of the Office of University Counsel and a valid legal request, such as a subpoena.

General Access to Confidential Information

CI: Confidential information is restricted to people with a business need for that information. Business needs are often established by virtue of an individual's role, for instance, an academic advisor requires access to student educational records while a nurse requires access to patient records.

HRI: Departments who wish to work with high-risk confidential information (or contract with a vendor to do so) must obtain prior approval from the CIO. Prior approval may be assumed if other individuals in the same role already have access.

Access to Electronic Confidential Information

CI: Confidential information stored electronically frequently requires that an individual log into a system or application (for instance, Datatel or a shared network folder). Such systems and applications have "owners," i.e., people who manage the application and authorize or revoke access. Owners must be able to identify individual users of those systems and ensure that only those users with legitimate business needs are granted access. In addition, access should be configured such that users only can access what they require based on their current status/role at the university.

CI: In technology systems and applications, administrators have an additional layer of access that permits them to modify the system itself on top of the data it contains. ("Administrator" in this sense is not synonymous with "a senior staff member.") Administrative access rights to servers with confidential information must be limited to system administrators with a specific business reason for access and such access must be logged; any access rights must change if their university or status changes.

CI: Seattle University confidential (non-public) information may not be saved on any computer directly accessible from the Internet or from the open portions of Seattle University's internal network.

Access to Non-Electronic Confidential Information

CI: Confidential information is also stored in non-electronic formats, most frequently on paper. When this information comprises a system of records (e.g., admissions files), this system must have an "owner" who can ensure that access is restricted to those with a legitimate business need. For instance, the owner may control key distribution to a locked file cabinet.

CI: It is easier to control and monitor access to electronic systems than paper, therefore, individuals are discouraged from printing confidential information when it is not necessary to do so.

Storage of High-Risk Confidential Information

CI: When not in use, non-electronic records containing confidential information must be kept in physically secure locations, for instance, in a locked office or locked file cabinet. Given wide variation in office configurations and types of confidential information, each department must establish its own protocol. These protocols must comply with applicable laws (e.g., HIPPA or FERPA) and be approved by the CIO.

HRI: High-risk confidential information may not be stored on a mobile device (laptop, portable USB drive, mobile phone, etc.) except by permission of the CIO. When permission is granted, the high-risk confidential information must be encrypted. This applies to members of the Seattle University community as well as university suppliers, vendors and contractors.

Destruction of Confidential Information

CI: All departments must develop record retention and destruction policies. When confidential information is no longer needed, it must be properly disposed of.

PD: Physical records containing personal data and high-risk confidential information should be shredded. Electronic records containing personal data or high-risk confidential information should be deleted, although this information may continue to exist in backup form for a period of time for business continuity purposes. Backup data is a separate classification of information that requires its own retention and destruction policy and is managed by the CIO.

Transmission

HRI: High-risk confidential information may not be emailed unless it is password-protected or encrypted. Microsoft Outlook passwords are not sufficient; however, Microsoft Office or Excel passwords are sufficient. Passwords must be transmitted separately.

Off-Site Considerations
PD: The university discourages employees from removing personal data and high-risk confidential information from campus. When it is required, employees are expected to protect that data like they would their own identity, credit cards, or check book.

Credit Cards
HRI: Use of a credit card or payment card may create high-risk confidential information; those records must be protected in accordance with this policy.

Recording Information about the Activities of Individuals
CI: Any department that maintains logs or automatically generated records of actions of individuals must adopt written policies, approved by the CIO, on the purpose of, and retention, access, and destruction policies for, such logs and records.

Surveys
PD: Seattle University does not collect personal data in surveys unless it is essential to the purpose of the study and the benefits of the study are sufficient to merit such collection. Surveys that do collect personal data must receive informed consent from survey recipients to voluntarily provide such information. The resulting data must be managed in such a way that it meets the data privacy standards of the university.

Contracts with Vendors
CI: Seattle University vendors dealing with Seattle University confidential information, whether or not they obtain the data directly from Seattle University, must have a written contract covering their services including the proper contract riders requiring the protection of Seattle University information. Departments should be aware that contracts may also require that the university protect the confidential information of vendors.

HRI: Departments that wish to contract with a vendor to collect or work with high-risk confidential information must obtain prior approval from the CIO.

Reporting Security Breaches
CI: If it becomes known or suspected that Seattle University confidential information may have been acquired or used by an unauthorized person or for an unauthorized purpose, the matter should be immediately reported to the Office of University Counsel. Should University Counsel not be available, the CIO or Public Safety (open 24 hours a day) can be contacted instead. Members of the university are encouraged to contact University Counsel if unclear about whether the situation warrants such a report.

Compliance
Upon employment and annually thereafter, all employees, including student employees, must demonstrate that they understand this policy and certify that they comply with it. In addition to the potential penalties outlined in the information policy framework, employees who fail to do so will have their user login revoked.