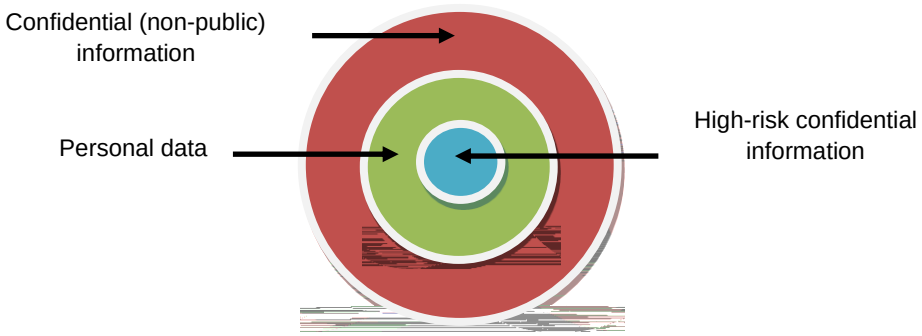
Seattle University Data Privacy Policy

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.

Seattle

CI: Seattle University confidential (non

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.