

RSA SecurID/Entrust Token Eligibility Policy

The following populations are eligible to receive a 2-factor authentication device (RSA SecurID/Entrust Token) from UW Technology:

- All customers must have an UW NetID
- Employees with a UW NetID, an Employee Identification Number (EID) and employee status=current in Higher Education Personnel and Payroll System (HEPPS)
- Students with UW NetID, an EID, a beginning and ending date of employment in HEPPS.
- Affiliate Employees with a UWnetID, and an EID.
- Any potential customer that has an agreement for SecurID service with UW Technology. For example, a Memorandum of Understand (MoU) or approval from UW Technology Executive Management (Director or above)

All 2-Factor customers must have a business case for requesting a 2-factor authentication device

- The access is required based on the UW Information System Security Policy for Confidential, and Restricted information. For each data category below there is a requirement of a two-layer minimum extra security measure on all Authentications of Confidential and Restricted Data that is accessed. See the Minimum Data Security Standards in the UW Information System Security Policy

<http://www.washington.edu/computing/security/pass/minimum.data.security.standards.pdf>

- **CONFIDENTIAL:** Data that is very sensitive in nature and typically subject to federal or state regulations. Unauthorized disclosure of this data could seriously and adversely impact the university or the interests of individuals and organizations associated with the university.
- **RESTRICTED:** Data that is generally circulated and subject to disclosure laws, yet sensitive enough to warrant careful management and protection to ensure its integrity, appropriate access, and availability.