PROTECTION OF SENSITIVE DATA

Protection of Sensitive Data

Stanford University maintains sensitive non-public data protected by laws and agreements, including Social Security numbers, financial information, health information, and student records. It is incumbent on every member of the Stanford community with access to such data to be familiar with and abide by Stanford's data classifications requirements provided at the Data Classification, Access, Transmittal and Storage (http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html) web site. Members of the Stanford community should also familiarize themselves with applicable laws and University policies on privacy as provided by the University, including Administrative Guide Memos 6.3.1 Information Security (https://adminguide.stanford.edu/chapter-6/subchapter-3/policy-6-3-1/), 6.4.1 Identification and Authentication Systems (https://adminguide.stanford.edu/chapter-6/subchapter-4/policy-6-4-1/), 6.6.1 Information Security Incident Response (https://adminguide.stanford.edu/chapter-6/subchapter-6/policy-6-6-1/), and 3.4.2 Card and Payment Account Acceptance and Processing (https://adminguide.stanford.edu/chapter-3/subchapter-4/policy-3-4-2/). For information on best practices for securing mobile computing devices, see the Guidelines for Securing Mobile Computing Devices (http://www.stanford.edu/group/security/securecomputing/mobile_devices.html) web site.