



# Chapter Eleven

## Security

### Sections in this Chapter

<a href="#">Physical Security</a> .....	1
<a href="#">Systems Security</a> .....	2
<a href="#">Departmental or Area Security</a> .....	2
<a href="#">Custody and Return of Property by Departing Employees</a> .....	2
<a href="#">References and Resources</a> .....	3

### Physical Security

Each member of the Stanford community has a general obligation to safeguard and make appropriate use of university and sponsor-owned property and equipment either assigned for individual use or as part of a common area. Each department must ensure that there are reasonable security measures implemented in their areas to prevent theft, damage or misuse of equipment. The Department Property Administrator (DPA) must play an integral role relative to these issues. Safeguarding of property includes, but is not limited to:

- Exercising reasonable care and security measures to prevent theft, misuse, or damage and maintain assets in good condition
- Provide adequate protection for equipment during movement, storage or while being used
- Ensure that equipment is properly stored and secured when not in use
- Do not commingle equipment in a manner that would pose a risk, i.e. equipment/flammable supplies
- Segregate government-owned property where feasible
- Where specialized security is necessary, ensure access is controlled and limited
- Ensure staff, faculty and students and other personnel accessing the area are aware of your security requirements
- Challenge unknown or suspicious persons in your area
- Report lost, stolen, damaged or impaired property to appropriate individuals, including, but not limited to, a direct supervisor or common area manager, **and notify the appropriate Department Property Administrator** of capital equipment/property moved to a different location

[Check the DPA Listing](#) to locate your Department Property Administrator.

## Systems Security

**Online systems access:** Stanford uses an authorization [WebAuth] to grant authorized employees access to on-line applications. Specific levels of access within applications are defined by roles assigned with the Authority Manager. Roles within the Sunflower Assets application used for property management are granted by the Property Management Office. Login IDs and passwords for any Stanford system are to be used only by the individual to which they are assigned. Refer to the [Administrative Guide Memo 63, “Information Security”](#) for additional Stanford Policy. Upon termination of employment with Stanford, access to online systems is discontinued.

When you are finished using secure Stanford websites (such as Oracle Financials, Stanford Mailing List Services, pages with employee confidential information, etc.), be sure to quit the browser or logoff. If you don't, people subsequently using your computer will be able to use the browser program to go to those websites, and the websites will treat that person as you, giving that person access to Stanford's and your web assets. You are responsible for preventing this type of “identity theft”, and the best way to do it is to quit the browser program when you are finished with it, or lock your computer if you need to leave your computer but aren't through with the browser. Please contact [HelpSU](#) if you need assistance with access or information on Stanford-secure websites.

## Departmental or Area Security

Access to departmental areas is generally available to Stanford employees and visitors. Each department is responsible for determining and implementing adequate access restrictions within their respective areas as needed to ensure the safeguarding of assets, data, or personnel.

## Custody and Return of Property by departing Employees

Each DPA should periodically review the “Custodian” field in Sunflower Assets (SFA), for assets under their responsibility, to verify all custodians are current Stanford employees. It is recommended that this occur at least annually. Each department is responsible for establishing a standard departure process for terminating employees. A [checklist of points to cover during a termination](#) review is available to assist on the HR website. Among the check-out points, meeting with the DPA and transferring custody for assigned assets should be included. Per [Administrative Guide Memo 22.8](#), *“...employees are required to return to the department any University-owned property, including any keys and identification cards, in their possession. Departments are responsible for obtaining these items.”*

If an employee departs the University prior to accounting for all their assigned property, the DPA should contact their Human Resources (HR) representative and inform the PMO. When the employee returns the equipment, the department manager or HR representative should notify the DPA so the SFA records can be updated. The annual update of off campus equipment forms is a good review. This review should also be performed, and applicable forms and records updated when employees transfer between Stanford departments. Equipment belonging to one department should be returned prior to any new equipment from another department being distributed. Again, work with your personnel manager and DPAs in other departments to ensure records are kept up to date.

## References and Resources

- [Administrative Guide Memo 63, “Information Security”](#)
- [Administrative Guide Memo 22.8](#)