

[Edit Policy](#)UNIVERSITY
of VIRGINIA

SEC-037: Access Privileges and Return of University Property

Date: 02/05/2016 Status: Final Policy Type: University
Contact Office: [Compliance \(UVA HR\), UVA Human Resources](#)
Oversight Executive: Vice President and Chief Human Resources Officer
Applies To: Academic Division and the College at Wise.
Table of Contents:
[Policy Statement](#)

- [1. New Employee Hires](#)
- [2. Employee Terminations](#)
- [3. Employee Transfers](#)
- [4. Contractors and Consultants](#)
- [5. University-Affiliated Organizations and Other Non-University Affiliates](#)
- [6. Timing of Access Changes](#)
- [7. Annual Audit of SIS/IS Responsibilities](#)
- [8. Common Access Privileges](#)

[Procedures](#)

Reason for Policy:

The University aims to protect the safety, security, privacy, and property of the institution by controlling the access that is given to individuals for its facilities and networks and facilitating the return of its property upon transfer or termination.

Definition of Terms in Statement:

- **Joint Engagement:**
An arrangement under which an employee of the University provides services to one or more University-Related Foundations or, conversely, an employee of a University-Related Foundation provides services to the University.
- **Manager:**
The individual employed by the University of Virginia to whom another University employee, Foundation Employee, or other non-affiliated person (e.g., visiting scholar, contractor, consultant, etc.) directly reports.
- **University-Associated Organization (UAO):**

An independent and separately incorporated legal entity, officially recognized by the University, subject to an executed UAO- Memorandum of Understanding (MOU), and meeting all the following criteria:

- Organized and exists under Virginia law and in good standing with the State Corporation Commission;
- Qualifies as a tax-exempt organization;
- Exists and operates for the benefit of the University or one or more of its units by providing one or more of the following support functions: fundraising, asset management, programs and services; and
- Not an agency, organization, corporation, or unit of the University or the Commonwealth of Virginia.

Policy Statement:

Managers and other University officials have a responsibility to: (1) authorize appropriate access privileges to employees, contractors, and others working under their direction or sponsorship and to modify or revoke those privileges when individuals transfer to another job within the University, terminate from the University, or otherwise no longer need these privileges; and (2) facilitate the return of department and/or University property (e.g., computers, lap-top computers, cell phones, etc.) upon transfer or termination.

1.

New Employee Hires:

When an employee is hired into a department, it is the responsibility of the employee's manager to authorize only appropriate access privileges for the employee. Examples of such privileges are purchasing cards, parking permits, telephone Forced Authorization Code (FAC) numbers, computer accounts, photo ID badges, building and room keys, etc. See below, [Common Access Privileges](#), for a more complete list.

2.

Employee Terminations:

When an employee terminates service with the University, it is the employee manager's responsibility to ensure that all access privileges are revoked and all keys, badges, and other physical items are collected from the employee in accordance with relevant policies. Managers must follow the procedures in the [Offboarding Toolkit](#) for salaried staff and wage employees or the [Faculty Departure Checklist](#).

3.

Employee Transfers:

When an employee transfers from one job to another, it is the responsibility of both the employee's previous and new managers to modify the employee's access privileges as appropriate for the employee's new job situation and collect any property belonging to the department/University.

4.

Contractors and Consultants:

It is the responsibility of the manager to whom a hired contractor or consultant reports to authorize only appropriate access privileges for that individual. Further, it is that manager's responsibility to ensure that all access privileges are revoked and all keys, badges, and other physical items are collected from the contractor or consultant when that individual's engagement with the manager ends.

5.

University-Affiliated Organizations and Other Non-University Affiliates:

University-Affiliated Organization (UAO) employees, visiting faculty, research collaborators,

government officials and other non-University affiliates may be granted access privileges to certain University resources in accordance with relevant policies. It is the responsibility of the University official who enters into a joint engagement with a UAO employee or who sponsors a non-University affiliate to authorize only appropriate access privileges for that individual. Further, it is that official’s responsibility to ensure that all access privileges are revoked and all keys, badges, and other physical items are collected from the non-University individual when that individual’s affiliation with the University ends.

6.

Timing of Access Changes:

Access revocations should generally be effective and physical items should be collected on the day these are no longer required by the individual, and no later than the day after that individual transfers to another job within the University, terminates from the University, or otherwise no longer needs these privileges. Managers and other University officials are responsible for notifying privilege-granting departments of necessary changes sufficiently in advance of the effective dates to allow the departments to process these changes in a timely manner. It is important to note that by policy a select few privileges may extend beyond the employee’s or non-University affiliate’s connection with the University. Privilege-granting departments will apply those policies when processing change requests.

7.

Annual Audit of SIS/IS Responsibilities:

Each year University Human Resources and Information Technology Services will review the UVA Integrated Systems (Student, HR, Finance) responsibilities that should remain active and those that should be deactivated. University policy requires that the supervisor of individuals to whom faculty/staff report should revoke access privileges when their employees, UAO employees, or non-University affiliates no longer need these privileges.

8.

Common Access Privileges:

Common access privileges are listed in the following table along with specific departments to whom requests for addition, modification, or revocation of access privileges should be made. The list is not all-inclusive.

| Access Privilege | Department to Notify | Relevant Website (If Applicable) |
|--|--|---|
| Login Authority for Specific Computer Applications, e.g. Oracle Financials, PeopleSoft Human Resources | Varies depending upon application | http://www.virginia.edu/integratedsystem |
| Accounts on Centrally-maintained Computers | Information Technology Services (Agency 207); Health System Technology Services (Agency 209) | http://www.its.virginia.edu/accounts http://www.virginia.edu/informationpolicy/accounts.html https://www.hsts.virginia.edu/forms/lan-account-request |
| Accounts on | Employee’s | |

| | | |
|--|---|--|
| Departmental-maintained Computers | Department | |
| Small Purchase Card | Purchasing | http://www.procurement.virginia.edu/pa/gepcard |
| Travel Credit Card | Accounting Services | http://uvapolicy.virginia.edu/policy/FIN-017 |
| Long Distance Calling Card & Long Distance Forced Authorization Code (FAC) | Information Technology Services - Communication Services | http://its.virginia.edu/commserv/telephone/longdistance.html |
| Identification Cards | University ID Office (Agency 207); Health System ID Office (Agency 209) | http://www.virginia.edu/idooffice/ http://www.medicalcenter.virginia.edu/intranet/safetysecurity |
| Parking permits, including service vehicle permits | Parking & Transportation | http://www.virginia.edu/parking/ |
| Building & Room Keys/Badges | Employee's Department | |
| Desk Keys | Employee's Department | |

Procedures:

Salaried Staff and Wage Employees: [Offboarding Toolkit](#)

Faculty: [Faculty Departure Checklist](#)

[IT Checklist for Leaving UVA](#)

Related Information:

[SEC-038, Management of the University Keyed System \(Key & Lock Policy\)](#)

[Medical Center Policy 0176, Access Control to Medical Center Facilities](#)

Major Category: Safety, Security and Environmental Quality

Next Scheduled Review: 02/05/2019

Approved by, Date: Policy Review Committee, 02/05/2016

Revision History: Updated definition 5/15/19. Supersedes (previous policy): Responsibility of Managers and Other UVa Officials for Access Privileges

Source URL: <https://uvapolicy.virginia.edu/policy/SEC-037>

-- ARCHIVED --