Privilege Management
Policy and Procedure for
Decentralized Administrators

Purpose

This document sets forth policy and procedures for Decentralized Administrators in the Privilege Management (PM) web application.

Introduction and Background

Privilege Management is a proprietary web application used by University and Medical Center. The application combines People, Privileges and Resources (cost centers, home departments, etc) to create Privilege Assignments which are utilized by a variety of applications and processes.

Vanderbilt has decentralized much of the security administration process. Decentralized Administrators (DAs) can administer numerous user privileges across a wide variety of applications. DAs are assigned to specific business units and organizations throughout the institution. For areas without a Decentralized Administrator, privilege management will be provided by centralized, application-specific administrators (AAs).

Policy

Decentralized Administrators (DA) will be established, with approved requests from their functional areas, by the Decentralized Managing Administrators (DMA) for either the University or Medical Center areas. During this process, the DA’s purview will be established based upon where their DA privilege is granted.

Decentralized Administrators are able add, modify or delete their own privileges. However, for any privilege acted upon which is deemed “high risk,” the action will be subject to workflow approval by their Privilege Approver(s). See Appendix A.

DAs may consider security requests (a request for privilege assignments) received via formalized paper form or via email as valid request methods. At no time is a DA allowed to consider valid any verbal request for privileges, since these are not auditable.
Decentralized Administrators will retain all security requests for a minimum period of three (3) years, regardless if the requests are in paper or electronic format (scans, emails, etc). After three years from the date of the request, DAs may dispose of their security requests.

All properly approved privilege requests received by DAs must be performed in a timely manner. It is the responsibility of the Decentralized Administrator to ensure that privilege requests contain the appropriate level of approval, regardless of the format in which they are received (paper or electronic).

Functional areas are responsible for notifying their Decentralized Administrator when an employee’s role assignments are no longer appropriate based on his/her job functions, such as when the employee changes job codes, transfers to another home department, is placed on medical Leave of Absence (LOA), or is terminated.

To prevent unauthorized transactions and inappropriate data access, it is the responsibility of the Decentralized Administrator to review both the Transfers and Terminations reports for their respective areas. This review must be performed at least monthly using each week’s reports within the Privilege Management application, but it is highly recommended that this review be performed each Monday.

Decentralized Administrators are responsible for conducting an annual review of all privilege assignments within their purview, or area of responsibility. Privilege assignments for employees who transferred to another home department, were terminated from Vanderbilt or for any user who no longer has valid reasons for their assignments shall have their privileges suspended or deleted, as appropriate, during this time.

If the Decentralized Administrator finds active privilege assignments for an employee who is out on medical or other leave for an extended period of time, the administrator should immediately suspend their privilege assignments until the employee returns to work. If an employee has privileges outside of the administrators’ purview which should be deleted or suspended, it is the DA’s responsibility to notify the administrator or business officer within that area.

Decentralized Administrators are responsible for maintaining records of each annual review for a period of three years. Annual review history may be maintained in either paper or electronic format, as long as the time period encompassed meets the three year standard.
Procedure

1. Process Security Requests
2. Address Transferred, Terminated and Leave of Absence Employees
3. Perform Annual Review of Privileges Review

1. Process Security Requests

When requests for security are received, Decentralized Administrators will perform the following steps:

A. Verify that the request was properly approved and confirm that the request is within their purview as a Decentralized Administrator.

I. If not properly approved, the request should be returned to the initiator for appropriate approvals. Since DAs can exist in a variety of organizational structures, this implies that DAs should ensure those requesting privileges have the actual authority make such a request. DAs can receive privilege requests informally (via email), so an email from a departmental authority figure authorizing a request may suffice.

II. If the Decentralized Administrator does not have authority in Privilege Management to make all necessary changes listed on a request, the request should be forwarded to the appropriate Decentralized Administrator for processing.

III. If no single Decentralized Administrator has the authority to enter all the privilege assignments requested, a copy of the request should be forwarded by the requestor to the appropriate centralized Application Administrator(s) for processing the remaining role assignments. A note should be included indicating where the original request will be maintained.

B. If questions arise regarding the requested privilege assignment(s), the Decentralized Administrator will contact the appropriate departmental personnel and clarify the business needs.

Forms to request privileges are located on the Privilege Management application homepage, http://vanderbilt.edu/fis/Apps/pm.htm, under Security Request Forms.
2. Address Transferred, Terminated and Leave of Absence Employees

Following are the procedures for monitoring employees who have transferred, terminated or who have been placed on Leave of Absence (LOA).

Employees who have transferred or terminated are listed on reports available within the Privilege Management applications Admin tab. These reports are generated each Sunday night and are available for review each Monday. This review must be performed at least monthly using the weekly reports, but it is highly recommended that DAs perform their reviews each Monday. See Appendix B for examples of each report.

A. Transferred Employees
   Decentralized Administrators will review the Transfers report to identify employees who:

   I. Transferred from a home department **within** their area of responsibility (purview) to a home department **outside** their area of responsibility. In this instance, the administrator should first confirm that the user’s roles should be removed, then proceed accordingly. Please note that the employee may need to retain their roles for a period of time for transition purposes. In this case, it is recommended that DAs modify the **target end date** for the privileges or **suspend** the privileges altogether.

   II. Job Code Change. In this instance, the Decentralized Administrator should confirm with the department head that the user’s current role assignments are still appropriate considering the change in job code. If the role assignments are no longer applicable, they should be revised to reflect the employee’s new responsibilities.

B. Terminated Employees
   Decentralized Administrators will review the Terminations report to identify employees who are classified as “terminated,” but did not have their role assignments automatically deleted.

   On the weekly Terminations report, Decentralized Administrators should pay particular attention to the “Auto Delete” column. This field shows whether a person’s role assignments were automatically deleted. If there is a “Y” in this column, the person’s role assignments were automatically deleted. If there is an “N” in this column, the person’s role assignments were not removed automatically, so Decentralized Administrators will need to determine if they should remove any privileges manually.
Decentralized Administrators are responsible for users listed on the weekly Terminations report who are assigned to a home department or have role assignments within the Administrator’s area of responsibility. For these users, the DA may need to confirm with the user’s department head to be certain that all role assignments should be deleted. Although it is rare, in certain instances it may be justified to provide role assignments to a person classified as “terminated.” In this situation, the person’s roles should be suspended until they can be deleted.

Leave of Absence reports are not provided within the Privilege Management application. There are, however, procedures a DA should follow to accommodate Leaves of Absence.

C. Leave of Absence (LOA) Employees
In addition to reviewing the two reports listed above, the DA will work with department heads to identify employees on LOA. Administrators should address LOA employee role assignments in accordance with the following policy:

I. Administrators should perform a “Person Search” in Privilege Management using the employee’s VUnet ID or name.
II. All privileges within the DA’s purview should be set to a “Suspended” status.
III. If privileges exist for the person on LOA outside of the DA’s purview, then the DA should contact the appropriate DA to suspend any remaining privileges.
IV. Once an employee returns from a medical leave of absence, the DA can reinstate all suspended roles within his/her purview.

3. Perform Annual Review of Privileges

Decentralized Administrators will conduct annual reviews of all role assignments in their area of responsibility to ensure they remain valid. Privileges for employees who transferred, terminated, are on medical LOA or who no longer need a particular role(s) shall be deleted or suspended as appropriate in Privilege Management.

DAs shall execute the DA Procedures for Annual Audit, located on the Privilege Management application homepage, on the FIS website at the following URL:
http://vanderbilt.edu/fis/Apps/pm.htm
Related Documents

Appendix A: Illustration of PM Workflow

Appendix B: Example of Privilege Management Transfers and Terminations Report

**DA Procedures for Annual Audit:** Located on PM application homepage [http://vanderbilt.edu/fis/Apps/pm.htm](http://vanderbilt.edu/fis/Apps/pm.htm)

---

**Trustee and Effective Dates**

Trustee:

Thomas M. Head  
Program Manager, FIS  
University Finance, Vanderbilt  
[fis-applications@vanderbilt.edu](mailto:fis-applications@vanderbilt.edu)

**Effective:** August 1st, 2011  
**Last Revised:** June 23rd, 2011
Appendix A
Workflow in Privilege Management

As depicted in the Workflow diagram above, Decentralized Managing Administrators (DMAs) establish both DAs and Privilege Reviewer & Approvers.

Once established, DAs are the privilege granting authority. Regardless if a privilege requires workflow approval, it all starts with the DA initiating the request.

If the DA grants a privilege that is not considered high-risk, it goes into effect immediately.

If the DA grants a privilege that is high-risk, it goes into the worklist for Privilege Reviewers or Privilege Approvers for final determination.
Appendix B
Privilege Management Transfer & Termination Reports

Example of weekly Privilege Management Transfer Report:

<table>
<thead>
<tr>
<th>Employee Name</th>
<th>(ID/Role)</th>
<th>ValNet ID</th>
<th>Job Code</th>
<th>Previous Dept</th>
<th>Previous Dept Name</th>
<th>Current Dept</th>
<th>Current Dept Name</th>
<th>Effective Date</th>
<th>Date of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dougan, Amanda F</td>
<td>0011202 / 0</td>
<td>DOUGLAF</td>
<td>Yes</td>
<td>177000</td>
<td>Housing Administration</td>
<td>12-01-2003</td>
<td>12-10-2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fisher, Peter G</td>
<td>0030063 / 0</td>
<td>FELITIPF</td>
<td>Yes</td>
<td>159480</td>
<td>Teaching Center</td>
<td>01-04-2004</td>
<td>12-10-2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gardiner, Deborah A</td>
<td>0005661 / 0</td>
<td>GARMINDA</td>
<td>201124</td>
<td>7th Floor Pediatrics</td>
<td>01-04-2004</td>
<td>01-02-2004</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hall, Lance H</td>
<td>0037665 / 0</td>
<td>HALELH</td>
<td>Yes</td>
<td>104230</td>
<td>Continuing Med Educ</td>
<td>01-01-2004</td>
<td>12-30-2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jones, Vicki R</td>
<td>0015313 / 0</td>
<td>JONESVR</td>
<td>201131</td>
<td>6 South</td>
<td>04-01-2004</td>
<td>12-10-2003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kees, Dennis D</td>
<td>0017666 / 0</td>
<td>KEEDADD</td>
<td>Yes</td>
<td>120740</td>
<td>English</td>
<td>01-01-2004</td>
<td>12-31-2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Martin, Richard L</td>
<td>0001364 / 0</td>
<td>MARTINRL</td>
<td>Yes</td>
<td>150310</td>
<td>English Language Con</td>
<td>11-16-2003</td>
<td>12-06-2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>McCoy, Beverly R</td>
<td>0007088 / 0</td>
<td>MCCAULBR</td>
<td>Yes</td>
<td>104230</td>
<td>Center for Structure</td>
<td>104379</td>
<td>Hematology/Oncology</td>
<td>12-08-2003</td>
<td>12-31-2003</td>
</tr>
<tr>
<td>Schmidt, Paul A.</td>
<td>0032332 / 0</td>
<td>SCHMITHF</td>
<td>Yes</td>
<td>108810</td>
<td>Network Computing Se</td>
<td>120152</td>
<td>EEO</td>
<td>01-01-2004</td>
<td>12-31-2003</td>
</tr>
<tr>
<td>Simpson, Shawn K</td>
<td>0020972 / 0</td>
<td>SIMPSONSK</td>
<td>Yes</td>
<td>106300</td>
<td>Medical Administration</td>
<td>104450</td>
<td>Ophthalmology</td>
<td>12-20-2003</td>
<td>12-20-2003</td>
</tr>
<tr>
<td>Thompson, Victoria L</td>
<td>0006075 / 0</td>
<td>THOMPSVL</td>
<td>201084</td>
<td>115 Surgery</td>
<td>209107</td>
<td>7th Floor Pod A</td>
<td>01-01-2004</td>
<td>01-02-2004</td>
<td></td>
</tr>
</tbody>
</table>

MM current employees were processed.
12 employees have transferred.

*** End of Report ***
## Appendix B (cont)

Privilege Management Transfer & Termination Reports

Example of weekly Privilege Management Termination Report:

<table>
<thead>
<tr>
<th>Employees Name</th>
<th>ID</th>
<th>VnNet ID</th>
<th>No.</th>
<th>Home Dept Id</th>
<th>Home Dept Name</th>
<th>Auto Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reilly, K S</td>
<td>0017578</td>
<td>REILLYS</td>
<td>4209990084</td>
<td>120520</td>
<td>Economics</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4209990138</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>42447000011</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roth, Bradley J</td>
<td>0010308</td>
<td>ROTHBJ</td>
<td>42063000301</td>
<td>120630</td>
<td>Physics And Ast</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>42063030802</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4206303642</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4206306642</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sciadini, Lorraine C</td>
<td>0004511</td>
<td>SCIADILC</td>
<td>1207300000</td>
<td>120700</td>
<td>Spanish And Pol</td>
<td>Y</td>
</tr>
<tr>
<td>Watson, Mary R</td>
<td>0017577</td>
<td>WATSONMR</td>
<td>1260940000</td>
<td>126260</td>
<td>Leadership, Pol</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1261600000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4269990100</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

27572 people were processed.
30 person(s) were removed.
48712 assignments were processed.
100 assignment(s) were removed.

*** End of Report ***