## Project Scope

There are ten components to the scope of the Security Maintenance Project (italic/shaded were completed in Phase 1):

<table>
<thead>
<tr>
<th>Scope Component</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Maintenance of Security Roles Assigned to a Position (Departmental Roles)</td>
<td>• View current security roles assigned to a position</td>
</tr>
<tr>
<td></td>
<td>• Initiate Security Role change transactions</td>
</tr>
<tr>
<td></td>
<td>• Workflow approval of security role change transactions</td>
</tr>
<tr>
<td></td>
<td>• Automatic update of roles in SAP upon final approval</td>
</tr>
<tr>
<td></td>
<td>• Eligibility of roles determined for each position</td>
</tr>
<tr>
<td>2 Maintenance of Security for Non-Employees &amp; for Temporary Assignments</td>
<td>• Initiate creation of SAP user ID for non-employees requiring SAP access</td>
</tr>
<tr>
<td></td>
<td>• Assign security roles to non-employee user ID’s along with end date for role</td>
</tr>
<tr>
<td></td>
<td>• Create temporary (time delimited) security roles for employee users (typically for when user changes positions but requires old roles on a temporary basis during transition)</td>
</tr>
<tr>
<td></td>
<td>• Support creation of “dummy” positions to support workflow for non-employees</td>
</tr>
<tr>
<td>3 Maintenance of Security Roles Assigned to a Position (Central Roles)</td>
<td>• View current security roles assigned to a position</td>
</tr>
<tr>
<td></td>
<td>• Initiate Security Role change transactions</td>
</tr>
<tr>
<td></td>
<td>• Workflow approval of security role changes</td>
</tr>
<tr>
<td></td>
<td>• Automatic update of roles in SAP upon final approval</td>
</tr>
<tr>
<td></td>
<td>• Eligibility of roles determined for each position</td>
</tr>
<tr>
<td>4 Maintenance of Workflow Approvals Assigned to a Position + Fund Code Based Approvals for a User</td>
<td>• View Workflow Approvals assigned to a position</td>
</tr>
<tr>
<td></td>
<td>• View Fund Code based approvals (Travel, B@D) which are assigned to the holder of the position for individual fund codes</td>
</tr>
<tr>
<td></td>
<td>• Initiate Workflow Approval change transactions</td>
</tr>
<tr>
<td></td>
<td>• Workflow approval of Workflow Approval change transactions</td>
</tr>
<tr>
<td></td>
<td>• Automatic update of Workflow Approvals in SAP upon final approval</td>
</tr>
<tr>
<td>5 Maintenance of Organizational Access Assigned to a Position</td>
<td>• View Organizational Access assigned to a position (used for Payroll access and BPS)</td>
</tr>
<tr>
<td></td>
<td>• Initiate Organizational Access change transactions</td>
</tr>
<tr>
<td></td>
<td>• Workflow approval of Organizational Access change transactions</td>
</tr>
<tr>
<td>Scope Component</td>
<td>Details</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>• Automatic update of Organizational Access in SAP upon final approval</td>
</tr>
</tbody>
</table>
| 6 Travel Initiator Assignments | • View current initiator assignments assigned to a user ID  
• Initiate Travel Initiator assignment change transactions  
• Workflow approval of Travel initiator assignment changes  
• Automatic update of travel initiator assignments in SAP upon final approval |
| 7 Phase 1 - Display Enhancements | • Buy@Duke thresholds  
• ECRT Primary & Secondary Coordinator organization unit assignments  
• Travel Alternate approvers and additional funding approvers  
• SRM department administrators organization unit assignments  
• A/P check request Management Center and Central Administration approvals and thresholds  
• Special designations  
  o Sponsored programs Department Administrator  
  o Travel Corporate Card Representative (TRaC rep)  
• Business Manager |
| 8 Organizational Reporting of Security Roles, Workflow Assignments & Org Access | • Create report(s) that provide ability to see which positions/users have which security roles, workflow assignments or org access with an Org Unit (BFR)  
  o Anyone who has the ability to run this report(s) will have the ability to run it for any Organizational Unit at Duke |
| 9 Fix Problems with Existing Identify Management Process | • Resolve problems with current Identity Mgt process such as terminated employees who return |

**Project Governance**

*Steering Committee* – The role of Steering Committee will be monitor progress of the project, provide key input into the project design and resolve issues that arise during the project. The Steering Committee will meet monthly. Steering Committee members are (new members for Phase II are bold):

- Todd Orr – ASM
- Chris Meyer – OIT
- Sue Roepke – ASM
- Rachel Satterfield – Controller
- Scott Seaman - OIT
- Ned Neeley - ASM
- Lisa Frazier – Accounting Systems & Procedures
- Susan Bonifield – Engineering School

*Advisory Committee* – The role of the Advisory Committee will be to provide an end-user departmental perspective during the design and development of the new security maintenance solution. The Advisory Committee will meet monthly. Advisory Committee members will be (new members for Phase II are bold):

- Todd Orr
- Chris Meyer
- Sue Roepke
- Rachel Satterfield
- Scott Seaman
- Ned Neeley
- Lisa Frazier
- Susan Bonifield
In addition to these standing committees, during the project we will conduct design reviews with:

- Operational Departments with Functional Ownership – Procurement, Corporate Payroll, A/P, ET&R, Budget Office, etc.

**Key Assumptions**

1) Requests for changes to Security Roles, Workflow Approvals, Organizational Access, and Travel Initiator Assignments will be submitted through the Duke@Work SAP Portal. Approvals for these access changes will be done via standard SAP approval processes (Universal Worklist).

2) Request for changes can only be initiated by the Security Administrator through the tool. They can request any access (not just eligible roles).

3) Initiators (Security Administrators) can also be Approvers
   a) A department approver can initiate and approve a request at save. A separate approval set will not be required.
   b) In small departments, the Security Administrator and Business Manager is often the same person.
   c) An approver cannot approve changes to their own security.

4) Security change requests can contain security role changes, organization access changes, workflow approval changes and travel initiator assignments in a single request.
   a) Only one request per position can be in process at a time
   b) Approvals within one request will be grouped into like approval routings
      i) This will allow separation of eligible changes which will require minimum approvals to be processed and updated quickly
      ii) Special access within the request with be grouped by common approval routings and processed as a separate workflow
      iii) Record will remain locked until all workflows for the request have been completed
   c) While the request is in process, the user should have the ability to see the requested changes and the workflow status
5) Need ability to create a request for a position by referencing another position
   a) Position the request is being created for cannot have any existing access assigned
   b) Allow the selection of the access to populate the request with information from the referenced position
   c) Ability to change the request (add/delete) after the initial population prior to saving and submitting to workflow

6) Security Roles, Workflow Approvals and Organizational Access will continue to be maintained at the position for all employees. Non-employees’ user IDs will be holders of “non-employee positions to facilitate access requests and approvals. Non-employee access will be assigned to the user ID and date delimited.

7) Travel initiators assignments will continue to be maintained by organizational unit or individual PERNR assignment to the user ID.

8) Concept of Eligibility and Ownership will be used for security roles, workflow approvals, organizational access or travel initiator assignment requests.

   a) Security Roles
      i) Role eligibility will be assigned on the Organizational Hierarchy
      ii) Each role will have a functional owner that will be an approver for all requests where the position is not eligible for the role. (Company code 0010 position requests Company code 0020 access – the owner of the company code 0020 role would be an approver of the request)

   b) Organizational Access (PD profiles)
      i) Default eligibility for a position is the position’s own organizational unit
      ii) Security Administrator for a department will be eligible to request org access for all positions within their department (making that position eligible to receive the access)
      iii) Each organizational unit will have an owner that will be an approver for all requests where the position is not eligible for the organizational unit

   c) Workflow Approvals
      i) Ownership is two-fold
         (1) Workflow approval flavor will have an owner
             (a) Departmental flavors’ owners will be defined as the department
             (b) Central office flavors’ owners will be specifically identified
         (2) Organizational unit that the approval is for will be same owner as the Organizational Access
      ii) Approval(s) would be combination of both

   d) Travel Initiator Assignments
      i) Eligibility and ownership will be the same as Organizational access
ii) Assignment by PERNR will use eligibility and ownership of the organizational unit the position the PERNR is a holder

e) Departmental approver (Business Manager) would be the same for security roles, organizational access, workflow approvals and travel initiator assignments

i) To minimize approval routing

ii) Provide enhanced oversight on the overall access being granted

9) Changes to the functionality of individual security roles and the design of the Organizational Access for HR/Payroll will not be included in the scope of the project.

10) Development Office security initiation and approval will migrate to standard University-wide processes as part of Phase II