

**AD Policy Working Group**  
**August 16th, 2013**  
**3110 Engineering Building II**  
**3pm-4:30pm**

Present: Donna Barrett, Billy Beaudoin, Dan Green, Julie Tilley, Dan Evans, Daniel Henninger, Tom Farwig, Joshua Gira

Guests: Debbie Carraway, Alan Gerber

---

**Business handled outside of meetings:**

**Fixing ADWS and PowerShell Permissions**

Changes to the membership of "NCSU-Read Group Memberships" generally go through the policy committee because its permissions circumvent the FERPA-related security settings. This includes reading the People and Managed Groups OUs.

In order to get AD Web Services and the Powershell Module to work correctly, a user account running code that requires the AD PS module needs to be in the domain-level BUILTIN\Users group. The default membership includes "Authenticated Users" and was removed a long time ago. Breaking the AD module is the only thing we know of that this point that it breaks.

So, we're planning on:

1. Adding the "NCSU-Departmental OU Admins" group to the "NCSU-Read Group Memberships" group, which effectively doesn't change any permissions, simply gathers all the accounts with those permissions under one group.
2. Adding the "NCSU-Read Group Memberships" group to the BUILTIN\Users group so that service accounts and OU admins can access the data over ADWS that they can already get over LDAP.

Additionally, ITECS and the Libraries want 2 more service accounts added to "NCSU-Read Group Memberships":

- coedean.jira.svc - Service account used for the Jira project management software we are building a POC for. It needs to be able to read AD groups for login permissions, role-based access control and so forth.
- LIB.journey.service - Service account for some of their apps to get at group info for granting/denying access to various library resources.

Policy Committee approved 8/13/13.

=====

**Agenda:** Meeting was cancelled due to low agenda items and preparation for the start of classes next week.