Identity Management
@
Brandeis University

#NERCOMPIdM
bit.ly/nercomp_IdentityMgmt
Who am I?

Ian Rifkin
irifkin@brandeis.edu
Director of Data and Systems Integration
Brandeis University

- Web and Middleware Development
- Identity Management
- Data Warehouse / Integration Hub
About Brandeis

Founded in 1948

Waltham, MA (9 miles west of Boston)

Undergraduate enrollment: 3,635

Graduate enrollment: 2,087

Staff FTE: 1,150

Faculty FTE: 569
What is Brandeis IdM?

(A) Web pages where people can change their passwords and other account information.

(B) "Middleware" code and databases for keeping track of users' roles and statuses for account access, using data from the SIS and HRIS systems to get official information about people.

(C) Literally a never-ending project

(D) All of the above...and more!
What technologies are involved with IdM?
Technologies Involved

- Databases
- Custom Code
- Custom UIs
- OpenLDAP
- Active Directory
- Shibboleth

And a PeopleSoft aspect I will explain...
Vendors and the cloud

We don’t currently use a IdM/IAM vendor product

How many of you use a vendor IdM or IAM product? Thinking about it?

How many of you have a SaaS ERP?

Other SaaS services?
What are some benefits of SaaS?
How is Identity Management (IdM/IAM) used?

User-facing identity.brandeis.edu is where end users go to

- Create accounts (students, employees, and sponsored account process)
- Change passwords
- Reset password
- Set email aliases
- Edit email delivery destination
- Enroll/Manage your two-factor authentication devices
- Enable/Disable additional Google Consumer Apps
- Google Groups Self-Service
- And more
What does Identity Management mean to you?
Why is IdM important?

Ability to implement policy decisions in a timely manner

Understand how/why access controls work (or don’t work)

Able to support community access needs

Many systems rely on Identity Management to function even if they are not directly part of the codebase

IDM is not just a “backroom” technical issue—it’s everybody’s business
In-house developed systems
All code is not created equally

Original state:

- Messier code: mixing of MVC, user exceptions in code
- Messier release processes: live production edits
- Messier support: Just reset your password a few times as a first step
- Tier 2 support request? Time to write SQL updates!
- Messier UI: sponsored account process meaningless
- And with less features than current state
Improvements and risks

Current state:

- Massive improvements increasing functionality and supportability
- Well organized code
- Clear release processes
- Improved support
- Usually easy to make changes based on business needs (more so than SaaS vendors would be able to do)

But it is a lot of code (>500k lines)
The power and risk of custom: retaining staff

Custom solutions can be maintainable, affordable and full-featured but...

It’s only successful with staff that understand it.

I’ve been fortunate to have IDM staff that not only are great at what they do, but have been on the team for years.

What happens when one leaves? What happens when all leave?
As I explain the current state consider the question: Should the custom code continue? Why or why not?
Types of Accounts and Source Systems

Staff (PeopleSoft HRIS)

Faculty (PeopleSoft HRIS and PeopleSoft SIS)

Students (PeopleSoft SIS)

Alumni (Alumni Office CRM)

Sponsored Accounts (Custom/IDM)
Roles of a data warehouse
IdM in a Data Warehouse

The data from the systems of record to a “data warehouse” database.

A custom process handles automatic merging of records, creates an internal IDM ID per person, determines role/status, etc.

There are also custom interfaces to manually merge records, set custom role/status data (e.g. Trustees, non-employee researchers, etc.)

The custom identity.brandeis.edu environment (Over 500k lines of custom code) caches the result from the IDM Data Warehouse process.
IdM as a hub of data

Identity Management is an important hub of bio-demo and account information.

Utilizes the data from the systems of record (human resources, student information, alumni, and sponsored) to assign roles and statuses to accounts.

This role status information is used by a configurable interface to create entitlement information which provides a robust framework for authorization management.
One version of truth

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>PRIMARYNAME</th>
<th>SOURCESYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>irifkin</td>
<td>Rifkin, Ian P</td>
</tr>
<tr>
<td>2</td>
<td>irifkin</td>
<td>Rifkin, Ian P</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>PRIMARYNAME</th>
<th>SOURCESYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>irifkin</td>
<td>Rifkin, Ian P</td>
</tr>
</tbody>
</table>
The mystery of your name

One IdM interface to let you know how your name appears in each system of record and how to update it (or set a preferred name)

https://identity.brandeis.edu/identity-manage/name

Note: The Mystery of Google -- If a person creates a Google+ account with their Brandeis Google Apps account they have the ability to overwrite their name across some Google systems.
Role/Status

Roles signify a type of relationship with the university (e.g. Staff, FacultyHR, Student, Applicant, etc.)

Status can be one ACTV, INAC, EXPR.

The difference between INAC and EXPR is time.
## Explanation of roles/status

<table>
<thead>
<tr>
<th>HR Roles</th>
<th>FacultyHR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Staff</td>
</tr>
<tr>
<td></td>
<td>TempStaff</td>
</tr>
<tr>
<td></td>
<td>PostDoc</td>
</tr>
<tr>
<td>SAGE Roles</td>
<td>FacultySAGE</td>
</tr>
<tr>
<td></td>
<td>Applicant</td>
</tr>
<tr>
<td></td>
<td>Student</td>
</tr>
<tr>
<td></td>
<td>Student-GPS</td>
</tr>
<tr>
<td>IDM Roles</td>
<td>Sponsored</td>
</tr>
<tr>
<td>Status (for Roles)</td>
<td>ACTV (Active)</td>
</tr>
<tr>
<td></td>
<td>INAC (Inactive)</td>
</tr>
<tr>
<td></td>
<td>EXPR (Expired)</td>
</tr>
</tbody>
</table>
Entitlements

Access controls based on role/status

Determines if user appears in LDAP/People Directory

Controls access to services like Google, online Library resources, printing
<p>| Role/Status                        | ActiveCommunityMember | ActiveDirectory | LDAP | NETFaculty | NETsponsored | NETStudent | StaffApplicatons | canTaveShell | canSponsorAccounts | e4proxy | fileShareLTS | googleApps | moodleAccount | phonebook | serviceDesk | studentPrint | vpn | gApps | Consumer | GmailVisibility | multifactor | NETAlumni | noPad | sh |
|-----------------------------------|-----------------------|-----------------|------|------------|--------------|------------|------------------|--------------|---------------------|---------|--------------|------------|----------------|-----------|------------|-------------|-----|-------|-----------|-----------------|------------|-----------|-------|---|----|
| Affiliate-EmeritusACTV           | ✓                     | ✓               | ✓    | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| Affiliate-EmeritusEXPR           |                       |                 |      | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| Affiliate-EmeritusINACT          |                       |                 |      | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| AlumniACTV                       | ✓                     | ✓               | ✓    | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| ApplicantACTV                    |                       |                 |      | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| ApplicantEXPR                    |                       |                 |      | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| ApplicantINACT                   |                       |                 |      | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| Brandeis-FellowACTV              | ✓                     | ✓               | ✓    | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| Brandeis-FellowEXPR              |                       |                 |      | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| Brandeis-Osher-InstituteACTV     | ✓                     | ✓               | ✓    | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| Brandeis-Osher-InstituteEXPR     |                       |                 |      | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| Employee-Service-ExtensionACTV   | ✓                     | ✓               | ✓    | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| Employee-Service-ExtensionEXPR   |                       |                 |      | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |
| Employee-TWP-AccessACTV          | ✓                     | ✓               | ✓    | ✓          | ✓            | ✓          |                  | ✓            |                     | ✓       | ✓            | ✓          | ✓             | ✓          | ✓          |              | ✓   | ✓     |           | ✓              | ✓           | ✓         |       |   |    |</p>
<table>
<thead>
<tr>
<th>Role/Status</th>
<th>ActiveCommunityMember</th>
<th>ActiveDirectory</th>
<th>LDAP</th>
<th>NETFaculty</th>
<th>NETSponsored</th>
<th>NETStudent</th>
<th>NETnull</th>
<th>NETudoRemote</th>
<th>canHaveShell</th>
<th>coSign</th>
<th>ezproxy</th>
<th>facstaffPrint</th>
<th>fileSharesLTS</th>
<th>googleapps</th>
<th>moodleAccount</th>
<th>phonebook</th>
<th>phonebookDesk</th>
<th>studentPrinter</th>
<th>vPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retired/Library/StaffACTV</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>StaffACTV</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>StaffEXPR</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>StaffINAC</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>TemporaryStaffACTV</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>TemporaryStaffEXPR</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>TemporaryStaffINAC</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Calculating entitlements

Handling cases where people may have many affiliations with the university (staff, student, alumni, faculty, etc.) and assigning permissions appropriately.

Fairly intensive process, can’t run for everyone all the time

Regular incremental process for individuals

Less frequent batch runs against everyone just in case

**Recalculate Role/Status**

Recalculate

**Note** - only recalculate if you think something is broken.
<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
<th>UID</th>
<th>Role / Status</th>
<th>Enabled Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rifkin</td>
<td>Ian</td>
<td>irifkin</td>
<td>AlumniACTV, FacultyHRACTV, FacultySageACTV, StaffACTV, StudentEXPRESSPR, Student-GPSEXPR, TeachingACTV, TemporaryStaffEXPRESSPR, VendorEXPRESSPR</td>
<td>ActiveCommunityMember, ActiveDirectory, canHaveShell, canSponsorAccounts, coSign, ezproxy, facstaffPrint, fileSharesLTS, gAppsConsumer, googleapps, LDAP, moodleAccount, multiFactor, NETeduroamRemote, NETFaculty, NETStaff, phonebook, phonebookEmployee, serviceDesk, shellAccount, StaffApplications, vpn</td>
</tr>
</tbody>
</table>
# Entitlement Exceptions

**Add New Exceptions**

If the exception already exists, the state and expiration date will be updated.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>ActiveCommunityMember</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ActiveDirectory</td>
</tr>
<tr>
<td></td>
<td>canHaveShell</td>
</tr>
<tr>
<td></td>
<td>canGraceOtherAccounts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service State</th>
<th></th>
</tr>
</thead>
</table>

| Expiration Date    | 2019-02-23             |

<table>
<thead>
<tr>
<th>Note / Ticket (optional)</th>
<th>Add Exception</th>
</tr>
</thead>
</table>
### User Details

**Name:** Waldorf, Stadler  
**UnetID:** 100269997  
**Sponsored:** Yes  
**Role/Status:** Sponsored/ACTV

### Exception Details

*Items in **bold/italic** are exceptions.*

<table>
<thead>
<tr>
<th>State</th>
<th>Service</th>
<th>Note</th>
<th>Update Date</th>
<th>Expiration Date</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>🗑</td>
<td>canSponsorAccounts</td>
<td>Recalculation of all permissions</td>
<td>2012-10-28 01:30:13</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>🗑</td>
<td>ezproxy</td>
<td>service exception changed: deleted ezproxy/2</td>
<td>2017-12-12 06:57:52</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>🗑</td>
<td>StaffApplications</td>
<td>service exception changed: deleted StaffApplications/2</td>
<td>2017-10-19 14:53:49</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>✔</td>
<td>ActiveCommunityMember</td>
<td>role status change: updated Sponsored/ACTV</td>
<td>2015-10-08 13:14:18</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>✔</td>
<td>ActiveDirectory</td>
<td>Recalculation of all permissions</td>
<td>2016-03-05 18:40:08</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>✔</td>
<td>canHaveShell</td>
<td>role status change: updated Sponsored/ACTV</td>
<td>2015-10-08 13:14:18</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>✔</td>
<td>coSign</td>
<td>Recalculation of all permissions</td>
<td>2014-03-22 21:52:24</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>✔</td>
<td>fileSharesLTS</td>
<td>Recalculation of all permissions</td>
<td>2014-03-22 21:52:26</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>✔</td>
<td>gAppsConsumer</td>
<td>User opted in</td>
<td>2017-03-22 14:34:57</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>✔</td>
<td>googleapps</td>
<td>service exception changed: deleted googleapps/1</td>
<td>2015-02-03 13:23:42</td>
<td></td>
<td>?</td>
</tr>
</tbody>
</table>
How do entitlements work

Identity is responsible for distributing this information to many other systems.

Data feeds, SSO SAML responses, etc.

Examples:

- Access to online library resources depending on role
- Staff printing vs. student printing

But only useful if service provider will do authorization with data we provide
Interfaces and support
# IDM User Interfaces

## New User Accounts

- Create an official staff/faculty/student/alumni account
- Request a sponsored account

## Computer & Device Registration

- Register a device on the network for Internet access, or move/re-name an existing device

## Existing Users

- Paycheck, W-2 and Grade Overview
- Identity self-service (Manage your mail options, password, password reset options)
- Change your password
- Reset your password (using email or cellphone) if you forgot it
- Retrieve your forgotten UNet ID
### Your Brandeis Account

Your password was last changed on 2017-03-21 10:22:01 by helpdesk staff.
Your password currently expires on 2019-03-21.

- **Change your password**
- **Set/Update your password reset data**
- **Set your mail options** mail aliases, forwarding, directory
- **Enroll/Manage your two-factor authentication devices**. This information only applies two-factor authentication. For more information, see [here](#)
- **Enable/Disable additional Google Consumer Apps** (Blogger, YouTube, Picasa)
- **Google Groups Self-Service** create, add members, unsubscribe
- **Question about how your name appears?**
- **Enable/Disable shell access**

### Alumni

### B Connect Services

### Sponsored Brandeis Accounts
Brandeis IDM Support

Tier 1 support is managed by the Help Desk.

Tier 2 IDM support includes

- merging identities/accounts
- processing exceptions related to access
- liaising with HRIS to handle their needs for account extensions, creations, and deactivations as well as out of office replies.

Tier 2 IdM support receives 1 to 20 tickets a week.
Help Desk Tools

The Help Desk have custom interfaces on identity.brandeis.edu to help support users.

Account dashboard: Display user account information e.g. is account locked

Account diagnostic tool: Test user login, returns result in a support ticket

Verify user and password reset tools

Ability to resend sponsored account creation link with token

Create and manage Google “Shared Mail Accounts”
Help Desk Tools

Account Dashboard (and information verification for password reset)
Verify User and Reset Password (using security questions)
Resend Sponsored Account Creation Token
Password Reset
View Questions and Answers
Create or Delete Google Groups
Create and Manage Shared Mail Accounts
Manage Help Desk Users

The account diagnostic tool (which examines the account and sends an email to the UNET RT queue) can be found at https://apps.brandeis.edu/AccountDiagnostic/index. This should only be run by the user.
# Account Dashboard

## System / Account Status

<table>
<thead>
<tr>
<th>System</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>EXIST S</td>
</tr>
<tr>
<td>Google</td>
<td>EXIST S</td>
</tr>
<tr>
<td>LDAP</td>
<td>SENSIT I V</td>
</tr>
</tbody>
</table>

### Last Google Login
2018-02-23 15:14:59 EST

### Visible in GMail
Yes

This controls whether or not a user’s name will auto-complete in the To field when composing an email in GMail. This user will show up.

### People Directory
View irifkin’s entry

<table>
<thead>
<tr>
<th>Name</th>
<th>Ian P Rifkin (all)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
<td>irifkin</td>
</tr>
<tr>
<td>Forwarding Address</td>
<td><a href="mailto:irifkin@gapps.brandeis.edu">irifkin@gapps.brandeis.edu</a></td>
</tr>
</tbody>
</table>

### Mail Aliases
irifkin
ianirifkin

### Student ID
W0166132

### Employee ID
W0166132

### PaperCut Status
User has faculty/staff printing privileges.

### Shell Status
Allowed — Opted in.

### Password Status
**Last change:** 2017-03-21 10:22:01  
**Method:** Help Desk Tool  
**Expires:** 2019-03-21

### Role / Status
AlumniACTV
FacultyHRACTV
FacultySageACTV
StaffACTV
StudentEXPR
Student-GPSEXPR
TeachingACTV
TemporaryStaffEXPR
VendorEXPR

Role / Status should not be communicated to the end user.
Account Diagnostic Tool

Only run this tool if you have been asked to do so by LTS personnel.

Please enter your username and password below and then submit. Please be patient as this may take a while.

Username
Password
Confirm
Ticket #

Send Diagnostic
Tools for special groups

Offices Directory editing for department administrators

Trustee password reset tool for President's Office

Family contact data collection/editing/viewing

Entitlement search and exceptions (employee printing; library access)
Administrative Tools

Manually lock/unlock accounts; View/edit mail responder

View/edit GMail account delegates; Administratively manage user aliases and forwarding options

View audit log

Send password reset link email

Manage entitlement rules and user-level exceptions
<table>
<thead>
<tr>
<th>Department</th>
<th>Mail Accepting General ID</th>
<th>Technology Svcs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Current</td>
</tr>
<tr>
<td></td>
<td></td>
<td>irifkin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ianrifkin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New *</td>
</tr>
<tr>
<td></td>
<td></td>
<td>irifkin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ianrifkin</td>
</tr>
</tbody>
</table>

* To clear all MAGIDs, submit a single empty line.

**Forward Address**
irifkin@gapps.brandeis.edu

Make Changes
<table>
<thead>
<tr>
<th>Date</th>
<th>Actor</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-07-06</td>
<td>system</td>
<td>Processed renewal for swaldorf</td>
</tr>
<tr>
<td>15:24:11</td>
<td></td>
<td>Sponsor uid updated from jen9580 to jen9580</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sponsor uenid updated from 100270250 to 100270250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Title updated from Other to Other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department id updated from N1003 to N1003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department name updated from Library &amp; Technology Services to Library &amp; Technology Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expiration date updated from 2017-10-07 00:00:00 to 2018-10-07</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status updated from ACTIVE to ACTIVE</td>
</tr>
<tr>
<td>2016-07-06</td>
<td>Request</td>
<td>test?</td>
</tr>
<tr>
<td>15:23:49</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-07-06</td>
<td>system</td>
<td>Processed renewal for swaldorf</td>
</tr>
<tr>
<td>15:22:16</td>
<td></td>
<td>Sponsor uid updated from g Bainio to jen9580</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sponsor uenid updated from 100086849 to 100086849</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Title updated from Other to Other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department id updated from N1003 to N1003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department name updated from Library &amp; Technology Services to Library &amp; Technology Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expiration date updated from 2016-10-07 00:00:00 to 2017-10-07</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status updated from ACTIVE to ACTIVE</td>
</tr>
<tr>
<td>2015-10-08</td>
<td>system</td>
<td>Processed renewal for swaldorf</td>
</tr>
<tr>
<td>10:52:23</td>
<td></td>
<td>Sponsor uid updated from g Bainio to g Bainio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sponsor uenid updated from 100086849 to 100086849</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Title updated from Other to Other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department id updated from N1003 to N1003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department name updated from Library &amp; Technology Services to Library &amp; Technology Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expiration date updated from 2013-04-05 00:00:00 to 2016-10-07</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status updated from INACTIVE to ACTIVE</td>
</tr>
<tr>
<td>2013-04-05</td>
<td>system</td>
<td>No renewal for account</td>
</tr>
<tr>
<td>09:05:01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-03-15</td>
<td>system</td>
<td>Processed renewal for swaldorf</td>
</tr>
<tr>
<td>12:42:57</td>
<td></td>
<td>Sponsor uid updated from g Bainio to g Bainio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sponsor uenid updated from 100086849 to 100086849</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Title updated from Other to Other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department id updated from N1003 to N1003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department name updated from Library &amp; Technology Services to Library &amp; Technology Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expiration date updated from 2012-04-05 00:00:00 to 2013-04-05</td>
</tr>
</tbody>
</table>
Search for user
Send a password reset link email
List of sensitive accounts (be patient - slow)
Adobe CSV file of employees

<table>
<thead>
<tr>
<th>Org Status</th>
<th>Locking</th>
<th>Exceptions</th>
<th>Delegates</th>
<th>Responder</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff RabbInstructor</td>
<td>View</td>
<td>View</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
</tbody>
</table>
Passwords and SSO

Are stored in

- LDAP
- Active Directory (AD)
- Google (for IMAP and CalDAV)

Historical: CoSign (with AD, LDAP), custom SAML, LDAP auth

Current: Shibboleth as SSO middleware (CoSign, LDAP, Duo)

Future: Shibboleth with authentication (Deprecate CoSign)
A couple of interesting Shibboleth items...
Shibboleth for Gating
SSO for PeopleSoft

SIS and HRIS are part of PeopleSoft environment

Apache HTTP proxy server (with Shibboleth SP) in front of WebLogic

Cookies (PS, WebLogic, Shib SP, Shib IdP, Duo -- yikes!)

PSoft has an expiration page that edits cookies if you hit it
But if SSO is logged out user may not reach expiry page

Session hook to the rescue (delete PS_TOKEN as part of authentication process)
PeopleSoft

But now we’re moving to Workday!

Oh and that Data Warehouse piece? That’s part of PeopleSoft too!
Workday - Short Term Plans

It is imperative to have a functional IdM environment as we move forwards with WorkDay.

Not urgent to deprecate the PeopleSoft IDM processes in the Data Warehouse (but I don’t want to be the last PeopleSoft instance running either).

Phase 1: integrate WorkDay user data with the existing IdM environment as a new source of Identity data.

   This includes new integration work, but it does not require changing the underlying code and processes.
Workday - Longer Term Plans

Replace the PeopleSoft code/processes from IdM...but with what?

Rewrite only what’s needed

Or

Opportunity to review the entire IdM environment?
IdM Environment Review

Coding language

Webserver software

Database Software

Etc.

Should we consider vendor solutions??
IdM/IAM Vendors

More vendors in the IdM/IAM field then there were years ago when Brandeis IdM was created.

Would a vendor add features? Reduce staff workload? Other?

Initial research revealed a capable vendor that does much of what we do

- But it’s not cheap
- And would change user experience

What are the benefits? More research is needed!
Is SaaS alone a benefit?

SaaS feels safer but is it?

Puts the risk and trust in a vendor. Just pay a bill and hope for the best.

Example risk: if vendor changes or goes out of business — may be tougher to recover.

What’s the business continuity plan?
Decisions in a bubble
IDM Governance

Difficulty in engaging non-technical staff

Complexities difficult for non-IDM staff

But decisions should not be made in a bubble

Use existing governance/stakeholders if available

Need to take small pieces and explain clearly

Work towards understanding approaches at other institutions
Keeping the conversation going

How can we help each other?

Ian Rifkin
irifkin@brandeis.edu
Director of Data and Systems Integration
Brandeis University