Improving Data Security Practices for Symphony

Spencer Anspach
Library Systems Analyst/Programmer
& Head, Database Management

Adam Crandell
Head, Library Applications

INDIANA UNIVERSITY

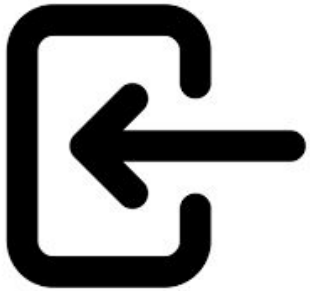
Enforcing IU Data Security Policies

- Data security of increased institutional importance
- IU has four data sensitivity levels: Public, University Internal, Restricted, and Critical
- Symphony contains all but Critical data
- For continued access, employees must meet certain requirements
  - Have their own login(s)
  - Have a sufficiently complex password (PIN)
  - Be employed by a library or library affiliated unit
  - Sign an Acceptable Use Agreement
  - Complete three tutorials: Data Protection, FERPA, and HR

By the Numbers

Potential Staff: 903

Staff with Accounts: 535



Staff Accounts: 1020

Libraries: 43

Campuses: 7

Auditing

- Training Compliance
- Activity
- Employment

HOW TO TRACK?

User Date Fields for Tracking

User date created

System assigned/not editable. This may be useful for a number of purposes, so we didn't want to change it.

Privilege granted

We will use for the date of last certification.

Privilege expires

Not currently used to lock out expired users; we will use to track certification expiration (Full-time staff: 24 mos. / Part-time staff: 13 mos.)

Last activity

Used by system if record is ever used for checkout; possibly also reserves, routing. Also, not editable.

Birth date

Age/b.d. is not needed for login records and is editable, so we will use to track last login.

Tracking Recertification

Use Renew Privilege wizard

- Sets Privilege Granted to current date
- Sets Privilege Expires (per User Profile setting)

Can be used for predicting soon-to-expire certifications and inactive accounts

Symphony doesn’t currently lock users out based on Privilege Expires date, but we’d welcome this (hint!)

Know Who's Logging On

History logs

Yesterday

```
cat `gpn hist`/`transdate -d-1 | grep -P -o "^\d\d\d\d\d\d"`.hist | grep -P
"^E`transdate -d-1`" | seltrans -oFW | sort -u | seluser -iB | edituser
-s`transdate -d-1`
```

(Yesterday, if today is the first of the month)

```
zcat `gpn hist`/`transdate -d-1 | grep -P -o "^\d\d\d\d\d\d"`.hist.Z | grep -P
"^E`transdate -d-1`" | seltrans -oFW | sort -u | seluser -iB | edituser
-s`transdate -d-1`
```

Today

```
cat `gpn hist`/`transdate -d+0`.hist | seltrans -oFW | sort -u | seluser -iB |
edituser -s`transdate -d+0`
```

Know Who's Logging On (cont.)

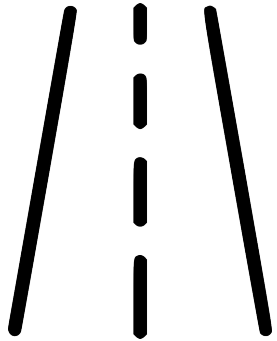
Logins

```
ls -altr `gpn locks`/Users/* | cut -d/ -f7 | seluser -iJ | edituser
-s`transdate -d+0`
```

We do this manually. Ideally it would be a cron job to run multiple times per day.

This is only necessary because actual WorkFlows logins aren't in the log; if they are ever logged, this will be superfluous. (There is an enhancement request: Enhance the WorkFlows logon process https://support.sirsidynix.com/enh/75819 Go vote!)

Future Work



- Depends on future enhancements
  - Logins recorded in history logs
  - Logins respect expiration date to lockout expired staff
- Cron job to capture active users
- Use of web services to have real-time reporting and interact / merge with University reporting sources
- Ways to track change in job responsibilities and if they need more / less permissions

Thanks!

Spencer Anspach

sanspach@iu.edu

Adam Crandell

acrande@iu.edu