Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
January 30, 2020

Program Description

The first or foundational phase of the Loyola Digital Experience (LDE) called LDE Foundation – Collaboration and Security will take the University to the next level for technology and will lay the foundation for the remaining LDE phases. ITS will be introducing new technology and applications at the University to strengthen information security and enhance collaboration.

Below is a summary of the ITS projects that are part of the LDE Foundation – Collaboration and Security program and their status:

Project	Status
Azure Multi-Factor Authentication (MFA) for Office 365	In Progress
Azure (MFA) & Application Conditional Access	In Progress
Azure Information Protection (AIP) & Data Loss Prevention (DLP)	In Progress
Intune (Mobile Device Management)	In Progress
Azure Password Self-Service	In Progress
Azure Privileged Identity Management	Not Started
Exchange Online Protection & Advanced Threat Protection	Not Started
O365 Application Portal (Single Sign-On)	Not Started
LastPass (Password Management)	Complete
Exchange Online Migration	Complete

Summary Status

Quick Summary of Activities:

- LastPass (Password Management) – Testing complete. Go Live complete December 2019.
- Mobility – Mobility policy on hold with cabinet review. Configuration set-up underway.
- Azure Multi-Factor Authentication – Pilot feedback provided by ITS and Library. Updates to communication are underway, branding updates, and January pilots scheduled.
- Information Protection (AIP) & Data Loss Prevention (DLP) – **DLP** focus group business user test cases signed off. Additional test cases, can be implemented after, per UISO. **AIP** Logging updates are underway to ensure the logging process works as expected.
- Added PSS Project #'s for all remaining LDE Projects, with end dates in 2020.

- Monthly ITS newsletter that includes LDE program announcements and updates sent out for January.

Key Issues & Risks:

- Mobile device policy needs to be approved by Cabinet for the MDM and MFA projects.
- Increase awareness campaign for MFA & DLP/AIP via content writer consultant to be hired.
- AIP logging delays due to possible client changes and Microsoft back-end issue.
- MFA timeline under strain due to resource challenges.
- Update communications for LDE program and channels being utilized for consumption.
- Resource challenges in key groups, with all the planning, development, testing and implementations occurring within a short timeframe.
- Impact to resources for future projects, based on delays to current projects.
- Potential to move towards a portal.office.com approach for authentication, may create need to revisit how these projects are implemented.

Detailed Status

<table>
<tr><th colspan="5">PSS 2563 – Azure Multi-Factor Authentication for Office 365</th></tr>
<tr><th rowspan="2">Project Sponsors</th><th rowspan="2">Project Manager</th><th rowspan="2">Target Completion</th><th rowspan="2">Phase</th><th colspan="2">Project Health</th></tr>
<tr><th>Last Period</th><th>This Period</th></tr>
<tr><td>Sibenaller / Vonder Heide</td><td>Integration Partners / Heather Chester</td><td>Fall 2020</td><td>Executing</td><td>Lime</td><td>Lime</td></tr>
<tr><td colspan="6">Scope:
Implement Azure Multi-Factor Authentication (MFA) and Conditional Access to strengthen information security by requiring a second form of authentication for applications.

Recent Activity:
• Pilot feedback gathered from ITS and Library with MFA for Office 365.
• Updating documentation to reflect suggestions from pilot groups. Focus is on MFA for various applications, not just the application enabling MFA at that time.
• Scheduled pilot sessions for January and February for MFA O365.
• University-wide roll out in February thru April 2020.
• Separated MFA Office 365 from the additional MFA “other application” roll outs, due to awareness campaigns, and the breadth and depth of applications being considered, requirements, and configuration and testing of new authentication process. This will appear as another project in the next status update.</td></tr>
</table>

- Communication plan identified over 20 channels for sharing information for faculty, staff, and students (in person events, emails, flyers, and socialization)
- Resolved Enrolled vs. Enforced issue when users set-up MFA O365.

Issues/Risks:

- Communication and training updates needed to streamline information.
- Branding campaign being developed.
- Size and complexity of the project, causing delays with many other projects occurring at once.

Next Steps:

- 1.) Confirm deployment approach for communication plans for MFA O365. 2.) Finalize pilot groups for MFA O365. 3.) Confirm roll-out university-wide plan for MFA O365.

PSS 2963 – Azure Multi-Factor Authentication & Application Conditional Access					
Project Sponsors	Project Manager	Target Completion	Phase	**Project Health**	
				Last Period	**This Period**
Sibenaller / Vonder Heide	Integration Partners / Heather Chester	Fall 2020	Executing	**Lime**	**Lime**

Scope:
Implement Azure Multi-Factor Authentication (MFA) and Conditional Access to strengthen information security by requiring a second form of authentication for applications.

Recent Activity:

- Separated MFA O365 with MFA for other applications to due to the complexity and requirements for authentication for each application. Currently there are 10 applications in the scope to be planned for authentication changes to MFA and ADFS.
- Slate Ugrad TEST environment instance move to Azure ADFS from LDAP successful. GPEM instance will be tested in January in TEST environment. Both instances will be validated with MFA Jan/Feb 2020.
- Lawson is the next to be scheduled for Go live this Summer/Fall.
- Sakai / Longsight discussions have started and requirements are being gathered for their authentication needs with ADFS.
- Other applications are under review consideration.
- Enrolled vs. Enforced for when users set-up MFA O365, has been resolved.

Issues/Risks:

- Communication needed to streamline with LDE communications and user-community overall changes being impacted.
- Size and complexity of the project, causing delays with many other projects occurring at once.

Next Steps:

- 1.) Confirm authentication on schedule for MFA O365 as it's a dependency for all other go lives. 2.) Confirm application work underway for Lawson, Sakai, and Slate.

PSS 2036 – Azure Information Protection & Data Loss Prevention					
Project Sponsors	Project Manager	Target Completion	Phase	**Project Health**	
				Last Period	**This Period**
Sibenaller / Vonder Heide	Integration Partners / Heather Chester	Summer/Fall 2020	Executing	**Green**	**Lime**

Scope:
Implement Azure Information Protection & Data Loss Prevention (DLP) to control and help secure email, documents, and sensitive data that are shared outside the organization. Use classifications or embedded labels and permissions to enhance data protection.

Recent Activity:

- Meeting held to review final test cases, review requirements, and confirm next steps.
- DLP Business Focus Group test cases signed off by the focus groups.
- UISO approved moving forward with implementation.
- Marketing, Communication, and Branding Strategy underway (hi-level). Waiting on consultant to be hired to develop awareness tools and website content.
- Test client to be installed on focus group machines for testing of labels (3 Data Classification levels when saving a file).
- Security team held several meetings with implementation partner, Integration Partners, to refine the AIP "rules" and logging results to achieve the best desired outputs.

Issues/Risks:

- Confirm multiple groups to enable PII rules. Understand how to socialize outside of HR and across the university.
- Confirm with business users timeframes for implementation and next phases.
- New resources on project, will impact project timeline a little, with transition.

Next Steps:

- 1.) Finalize requirements. 2.) Create communication, branding, and marketing approach. 3.) Gather feedback on Label testing. 4.) Confirm timeline and next steps. 5.) Hire content writer consultant to develop awareness campaign deliverables.

Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
January 30, 2020

PSS 2818 – LastPass (Password Management)					
Project Sponsor	Project Manager	Target Completion	Phase	Project Health	
				Last Period	This Period
Sibenaller / Vonder Heide	Warren Francis	Fall 2019	Executing	Green	Green

Scope:
Implementation of LastPass, a cloud-based password manager tool. LastPass will assist users to manage and protect their personal and business passwords, which will enhance overall information security at the University.

Recent Activity:

- Susan gave approval of LastPass communication language. We updated the website to contain the same language prior to go-live on December 4th.
- Anthony is finalized the LastPass website including FAQ's. We will update the FAQ's over time as we see what type of questions come in.
- The team finished testing the application in preparation for 12/4 go-live.

Issues/Risks:

- None

Next Steps:

- 1.) University Marketing will send out communication to all faculty, staff, and students to let them know that LastPass is now available.

PSS 2397 – Intune (Mobile Device Management)					
Project Sponsors	Project Manager	Target Completion	Phase	Project Health	
				Last Period	This Period
Sibenaller / Vonder Heide	Heather Chester	Summer 2020	Executing	Green	Green

Scope:
Implement mobile device management at Loyola to protect university data on mobile devices. Project to start R&D Summer 2019, due to LDE Targeted implementation for Spring 2020.

Recent Activity:

- No updates since 10/5/2019 due to resource constraints.
- UISO provide pilot test cases for BETA in January for Desktop team to set-up, configure the environment, and test policies.
- Working with Microsoft Fast Track and SWC, included in our Microsoft agreement, for support to set-up policies and create a successful 1st pilot.

Issues/Risks:

- Confirm Mobile Device policy is presented and approved to cabinet.

Next Steps:

- 1.) Enable pilot test cases. 2.) Set-up and configure system based on policies. 3.) Obtain Mobile Device policy approval from cabinet. 4.) Begin beta test.