



Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
November 30, 2019

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

Summary Status

Quick Summary of Activities:

- LastPass (Password Management) – Testing complete. Go Live scheduled for 12/4.
- Mobility – Presenting mobile policy to cabinet. Pilot testing to begin in December.
- Azure Multi-Factor Authentication – Pilot feedback provided by ITS and Library. Updates to communication are underway, branding updates, and additional pilots scheduled for January.
- 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.



**Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
November 30, 2019**

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

Key Issues & Risks:

- Mobile device policy needs to be approved by Cabinet for the MDM and MFA projects.
- Increase branding and awareness for MFA and DLP/AIP.
- Update communications for LDE program and channels being utilized for consumption.
- AIP logging delays due to possible client changes.
- 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

PSS 2563 – Azure Multi-Factor Authentication & 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
<p>Scope: Implement Azure Multi-Factor Authentication (MFA) and Conditional Access to strengthen information security by requiring a second form of authentication for applications.</p> <p>Recent Activity:</p> <ul style="list-style-type: none"> • 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. • Determine end of opt-in period for early 2020 for MFA O365. • 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. This will appear as another project in the next status update. 					



**Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
November 30, 2019**

- 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.
- Enrolled vs. Enforced for when users set-up MFA O365, has been resolved.

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 communication plans for MFA O365. 2.) Confirm pilot groups for MFA O365. 3.) Confirm Slate GPEM Azure ADFS go live dates.

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
<p>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.</p> <p>Recent Activity:</p> <ul style="list-style-type: none"> • Meeting held to review final test cases, review requirements, and confirm next steps. • DLP Business Focus Group test cases signed off by a few groups. • UIISO approved moving forward with implementation. • Marketing, Communication, and Branding Strategy underway. • Microsoft Tenant and logging successfully implemented. Training held with LUC Server Team. • Security team held several meetings with implementation partner, Integration Partners, to refine the AIP “rules” and logging results to achieve the best desired outputs. <p>Issues/Risks:</p> <ul style="list-style-type: none"> • Confirm multiple groups to enable PII rules. • Confirm with business users timeframes for implementation and next phases. 					



**Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
November 30, 2019**

- New resources on project, will impact project timeline a little, with transition.
- Next Steps:**
- 1.) Finalize groups for Go Live. 2.) Create communication, branding, and marketing approach.

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
<p>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.</p> <p>Recent Activity:</p> <ul style="list-style-type: none"> • 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. <p>Issues/Risks:</p> <ul style="list-style-type: none"> • None <p>Next Steps:</p> <ul style="list-style-type: none"> • 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



***Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
November 30, 2019***

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.
- UIISO will provide pilot test cases for BETA in December to set-up 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.