Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
February 22, 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
Exchange Online Migration	In Progress
Azure Multi-Factor Authentication & Conditional Access	In Progress
Azure Information Protection & Data Loss Prevention	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

Summary Status

Quick Summary of Activities:

- Planning of the LDE program awareness and communication in progress. Test internal website pages created and preparing content on strategy and program. General awareness email has been drafted.
- More detailed program timeline and individual project implementation rollout plans currently in progress.
- Results from the Exchange Online proof of concept testing are being reviewed & analyzed.
- Azure Multi-Factor Authentication (MFA) & Conditional Access, Information Protection & Data Loss Prevention (DLP) and LastPass projects are underway.

- Integration Partners, the vendor assisting with the MFA and DLP implementations, is currently working with ITS resources during the discovery phase of the project and will present their findings and recommendations on 2/27.

Key Issues & Risks:

- The impact of the implementation of program changes on users needs to be taken into consideration during planning. The rollout of applications needs to be carefully coordinated and managed.
- ITS resources are working on multiple LDE projects or other concurrent ITS projects. Need to manage the time of resources between competing priorities to ensure project expectations are met.
- The start of the Intune (Mobile Device Management) project is currently scheduled for Summer 2019. However, the timing needs be revisited since the implementation of MFA, investigation into the new Illinois law regarding reimbursement of personal cell phone usage and the timing of the University mobile device policy needs to be coordinated.

Detailed Status

**Target Completion timeframes are pending ITESC, Cabinet and Dean's Council approvals of the program*

PSS 2784 – Exchange Online Proof of Concept					
Project Sponsors	Project Manager	Target Completion*	Phase	**Project Health**	
				Last Period	**This Period**
Sibenaller / Vonder Heide	Heather Chester	Summer 2019	Executing	**N/A**	**Green**

Scope:
The Proof of Concept (POC) was approved by the ITESC to migrate the Infrastructure Support Services (ISS) Team to Exchange Online.

Recent Activity:

- Attended program planning meetings.
- Migrated 31 users in ISS.
- Created testing template for end users to test on various devices, On Prem, Remote, Native apps, or various devices.
- Held testing feedback focus group to gather feedback on testing concerns, questions, etc.
- Website under development to drive users to information about common migration questions and additional Microsoft Features and Functionality.

Issues/Risks:

- None at this time.

Next Steps:

1) Investigate testing feedback, 2) Obtain program level communication plan, 3) Obtain approval from ITESC on 2/27 to move forward with enterprise wide migration

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 / Mary Bunker	Spring 2019	Analysis	**N/A**	**Green**

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:

- Statement of Work and Non-Disclosure Agreement (NDA) fully executed by Loyola and Integration Partners.
- Project kicked off with Integration Partners on 1/17/19.
- Weekly meetings taking place with Integration Partners to review project status and any outstanding issues.
- VPN and domain access established for Integration Partners consultant.
- Integration Partners currently in the discovery phase of project and determining Loyola's readiness and any gaps.
- Integration Partners compiling findings and recommendations for review with Loyola on 2/27/19.
- Loyola communication and rollout planning currently in progress.

Issues/Risks:

- None at this time.

Next Steps:

1) Review Integration Partners' findings and recommendations on 2/27, 2) Prepare for Proof of Concept for March, 3) Review initial communication and rollout plan with management

Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
February 22, 2019

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 / Mary Bunker	Summer 2019	Analysis	**N/A**	**Green**

Scope:
Implement Azure Information Protection & Data Loss Prevention (DLP) to Control and help secure email, documents, and sensitive data that is shared using classifications or embedded labels and permissions, enhance data protection at all times.

Recent Activity:

- Integration Partners is currently in the Discovery phase for this project which is running concurrently with the MFA project
- Discussed with Integration Partners considerations for Proof of Concept (POC) to take place in the mid-March timeframe such as engaging a user group to discuss classifications (naming, labels) and automation. Per Integration Partners, there are canned items available for HIPAA and PCI.

Issues/Risks:

- None at this time.

Next Steps:

1) Review Integration Partners' findings and recommendations on 2/27, 2) Determine if users will be involved in choosing labels and if there will be automated labels and classifications as well, 3) Need to get HIPPA group together and potentially expand to HR and Finance for Proof of Concept

Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program
Executive Status Report
February 22, 2019

PSS 2818 – LastPass (Password Management)					
Project Sponsor	Project Manager	Target Completion*	Phase	Project Health	
				Last Period	This Period
Sibenaller / Vonder Heide	Mary Bunker	Spring 2019	Analysis	**N/A**	**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:

- Two meetings held with the vendor to discuss rollout, deployment homepage, and configuration settings for the product.
- Implementation for the full university dependent on Microsoft Multi-Factor Authentication (MFA) product implementation because of an issue with existing users and federated logon as well as mandating MFA for the master password for LastPass.
- UISO team discussed policies to propose when LastPass is configured for public consumption.

Issues/Risks:

- Dependency on MFA project.

Next Steps:
1) UISO to meet with senior leadership regarding the information security policies to be created or updated for LastPass project, 2) Waiting for MFA project to progress further

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	Planning	**N/A**	**Green**

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:

- Understanding MGC role for new laws in effect.

Issues/Risks:

- MGC assistance with new law implementation. Understand impact from leadership, and how it would affect the project implementation.

Next Steps:

1) Understand law impacts and how to engage MGC, 2) Reconfirm kickoff date, 3) Kickoff project, 4) Obtain ISAC Security Policy approval.