***Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program***
***Executive Status Report***
***March 31, 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 | In Progress |
| Exchange Online Protection & Advanced Threat Protection | In Progress |
| O365 Application Portal (Single Sign-On) | Not Started |
| LastPass (Password Management) | Complete |
| Exchange Online Migration | Complete |

## Summary Status

**Quick Summary of Activities:**

- All LDE project activities deferred for 2-3 weeks due to COVID campus mobilization of off-campus operations.
- Azure Multi-Factor Authentication O365 – Pilot feedback provided in January and February and began scheduled roll-outs for Faculty and Staff in February and March. All deployment requested by Provost for Faculty to stop mid-March due to COVID impacts. All awareness and marketing campaigns operationalized in February and March to faculty, staff, and students.

# *Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program*
## *Executive Status Report*
## *March 31, 2020*

- Azure Multi-Factor Authentication Other applications – Slate ready for deployment. Lawson requirements and configuration under development. Sakai requirements gathering in process with vendor. Identifying which applications can be planned next for requirement gathering and when to revisit.
- Mobility – Mobility policy on hold with cabinet review. Configuration set-up underway by Desktop team. Policy requirements provided by security team for configuration of MDM.
- Information Protection (AIP) & Data Loss Prevention (DLP) – **DLP** focus group business user testing underway with labels. 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.

**Key Issues & Risks:**

- Mobile device policy needs to be approved by Cabinet for the MDM and MFA projects. Otherwise anyone can use the mobile device for authentication and still not have the device password protected as it's not required at this time in any policy.
- MFA other applications: Need to work on 2 or 3 applications at a time for authentication requirements gathering, changes, testing, and deployment (not only to reduce impact to the user community but the resources needed to gather requirements, set-up testing, and identify any additional change/costs needed for a successful implementation).
- Hired content writer for awareness campaign for MFA & DLP/AIP; however, the resource did not continue. Looking for an additional resource to contribute to the awareness tasks.
- AIP logging delays due to 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

| PSS 2563 – Azure Multi-Factor Authentication for Office 365 | | | | | |
|---|---|---|---|---|---|
| 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:**

- Deployments in February and March underway with success. Not a lot of questions or concerns from remaining pilot feedback or new groups enrolling in MFA.
- Finalized website updates, including a new page for Suggested Technology.
- Changed scope to include Conditional Access, which will limit users who have older authentication (legacy) or older devices (over 3 years old) may have some limitations for using MFA.
- University-wide roll out in February thru April 2020 for Faculty, Staff thru Summer, and Students by end of September.
- Communication plan deploying 20 channels to share information for faculty, staff, and students (in person events, emails, flyers, and socialization).
- Communicated to all groups scheduled for enrollment of deferring enrollment for a few weeks
- Coordinated with LDE leadership and CIO on delaying deployments.
- Content writer consultant hired. Assisted with additional awareness tasks and deliverables mid-February thru mid-March. Resource did not continue after mid-March and working to hire another resource in April.

**Issues/Risks**:

- Volume of Communication and training updates needing completed at one.
- Gathering and creating group lists for deployments is an imperfect science.
- Size and complexity of the project, causing delays with many other projects occurring at once.

**Next Steps:**

- 1.) Replan timeline for leadership approval roll-out university-wide plan for MFA O365. 2.) Adjust communication plans (no longer print awareness is applicable around campus).

| **PSS 2963 – Azure Multi-Factor Authentication for Other Applications** | | | | |
|---|---|---|---|---|
| Project | Project Manager | Target | Phase | **Project Health** |

***Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program***
***Executive Status Report***
***March 31, 2020***

| Sponsors | | Completion | | Last Period | This Period |
|---|---|---|---|---|---|
| Sibenaller / Vonder Heide | Integration Partners / Heather Chester | December 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:**

- Slate Ugrad TEST environment ready for deployment. Ned to confirm when all MFA O365 users are enrolled for GPEM and UGrad. Deployment moved to June due to enrollment deadlines shifting to June 1.
- Lawson requirements gathering, configuration updates needed for authentication to work properly (changes are required to current back-end configuration). Go live still scheduled for Summer/Fall 2020.
- Sakai / Longsight discussions underway and can authentication with ADFS and MFA. Test environment needs to be set-up. Tim Walker and Jeff Apa assisting with coordination.
- Other applications are under review consideration.

**Issues/Risks**:

- Confirm coordination of communication changes to user community, based on MFA O365 enrollment of all applicable groups.
- Communication needed to streamline with LDE communications and user-community overall changes being impacted.
- Size and complexity of the project, causing delays with other projects occurring at once. Authentication requirements for each application are unknown, require configuration changes (sometimes very complex and adding additional costs).

**Next Steps:**

- 1.) Confirm authentication requirements and deliverables are moving forward for MFA with Lawson, Sakai, and Slate. 2.) Confirm schedule for MFA O365 as it's a dependency for all other go lives.

| **PSS 2036 – Azure Information Protection & Data Loss Prevention** | | | | |
|---|---|---|---|---|
| Project | Project Manager | Target | Phase | **Project Health** |

***Loyola Digital Experience (LDE) Foundation: Collaboration & Security Program***
***Executive Status Report***
***March 31, 2020***

| Sponsors | | Completion | | Last Period | This Period |
|---|---|---|---|---|---|
| Sibenaller / Vonder Heide | Integration Partners / Heather Chester | 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:**

- Delays for user testing due to Microsoft back-end issue. UISO team working to resolve issue and escalate within Microsoft. Microsoft issue resolved as of 3/6.
- No meetings in February due to back-end Microsoft issue and illness on the UISO team at the end of January / early February.
- Communication plan underway (hi-level). Waiting on consultant to be hired to develop awareness tools and website content in April / May.
- Testing of functionality for labels will be captured in April.

**Issues/Risks**:

- Confirm and finalize requirements.
- Socialize these policies across the university. Determine approach with LDE sponsors.
- 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***
***March 31, 2020***

| PSS 2397 – Intune (Mobile Device Management) | | | | | |
|---|---|---|---|---|---|
| Project Sponsors | Project Manager | Target Completion | Phase | **Project Health** | |
| | | | | **Last Period** | **This Period** |
| Sibenaller / Vonder Heide | Heather Chester | Fall 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:**

- Policy configuration underway by Desktop team with application.
- Secured test devices for testing.
- Schedule internal best test for team in April or May.
- Gather ITS test users for next beta test.
- Work with SWC and FastTrack for awareness campaign.

**Issues/Risks**:

- Confirm Mobile Device policy is presented and approved to cabinet.
- Ensure we have enough test devices for testing.
- Confirm deployment and user experience impact with bigger LDE implementation schedule/plan.

**Next Steps:**

- 1.) Enable pilot test cases. 2.) Finalize configuration of system based on policies. 3.) Obtain Mobile Device policy approval from cabinet. 4.) Begin beta test.