OVERVIEW
Encrypting data on desktops and laptops is a required foundational protection required and is the first line of defense from data tampering and theft. This solution will replace and update functionality of existing encryption options for participating units, eliminating the need for units to self-fund this requirement.

RATIONALE
The university required an improved encryption solution to allow for more secure key management, as well as comprehensive enterprise visibility and management of encryption policies. A team of cross-unit representatives has selected Dell Data Protection Encryption (DDPE) as the preferred solution, to be managed by Enterprise Security as a university-wide service.

This project will provide encryption for all institutional data at rest on desktops and laptops. Additionally, it provides an encryption solution to the university that will allow management of both proprietary and OS-centric solutions (BitLocker/FileVault). Enterprise reporting capabilities will facilitate compliance with the Information Security Standard. This project contributes to strategies to reduce risk of data tampering and theft.

RESULTS

- **Milestone:** Deployment of 60% of the University total FTE count. Participating units include:
  - Athletics
  - CFAES (ATI & DARDC)
  - College of Optometry
  - Mansfield
  - OOS
  - OSUWMC
  - College of Medicine
- **Milestone:** Management of BitLocker/FileVault Keys in deployed units
- **Milestone:** Creation of a unit-led encryption steering committee for ongoing service quality

End results
Each project deliverable will complete according to the FY15 agreed activities. Completion of the entire project will be June 30, 2015.

RESOURCES

People and their roles

Executive Leader: Helen Patton
Tech Lead: Patrick Mayer
Resource Manager: Ryan Treptow
Steering Committee: To Be Determined

Enterprise Security – accountable for ensuring the completion of this project. Partnership with the following groups is also required:
- Participating Units – for local unit deployment and communications
- OCIO Communications – for unit engagement
- OCIO Service Management – for creation of Service in the OCID catalog
- OCIO Infrastructure – for servers/database build/deploy

Other resources

Virtual Operating systems, storage and licensing support will be required ongoing.

Dependent on OCIO Active Directory program for rollout to OCIO supported units

RISKS

- Resource conflicts due to operational/project priorities
  - Mitigation: Bi-weekly resource alignment touch points
  - Engineering single point expertise
  - Mitigation: Work with Security team to cross-train and/or identify alternative support resources

RUN

Project Manager: Amber Buening
Documentation: https://infsec.osu.edu

Reporting Plan/Roadmap:
- Monthly status report to Executive Leader (to be shared with Project Sponsors)
- Reporting to the Steering Committee (frequency to be determined)

Rollout Plan:
Beginning with OCIO, will rollout encryption functionality, training and communication support to participating units. Units will determine deployment timelines based on individual scheduling concerns.

FY16 unit deployments will be explored outside the scope of the project.

REVIEW

Project wrap-up and review: (DATE TBD)
There will be an implementation review process with each unit deployment, as well as an overall project review

Results review: (DATE TBD)