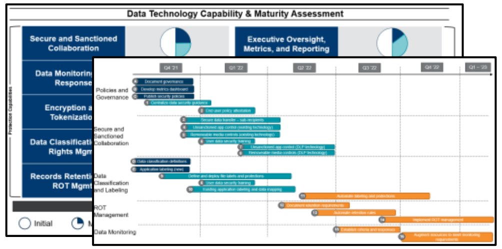
Design and Implement – Case Study

Background: 1,200 user state agency engaged Kudelski Security to develop their data classification taxonomy and security strategy. After the initial assessment, the agency engaged Kudelski to implement eight (8) projects from their roadmap and make optimal use of their Microsoft 365 E5 investment.

8 weeks

6 months

Phase I – Assess (FY21)


Data Technology Capability & Maturity Assessment
Secure and Sanctioned Collaboration
Executive Oversight, Metrics, and Reporting
Data Monitoring Response
Encryption a Tokenizatio
Data Classificati Rights Mgm
Records Retenti ROT Mgmt
Protection Capabilities
Initial
Q4 '21
Q1 '22
Q2 '22
Q3 '22
Q4 '22
Q1 – '23
Policies and Governance
Document governance
Develop metrics dashboard
Publish security policies
Centralize data security guidance
End user policy attestation
Secure and Sanctioned Collaboration
Secure data transfer – sub-recipients
Unsanctioned app control (existing technology)
Removable media controls (existing technology)
User data security training
Unsanctioned app control (DLP technology)
Removable media controls (DLP technology)
Data Classification and Labeling
Data classification definitions
Application labeling (new)
Define and deploy file labels and protections
Existing application labeling and data mapping
Automate labeling and protections
ROT Management
Document retention requirements
Automate retention rules
Implement ROT management
Data Monitoring
Establish criteria and responses
Augment resources to meet monitoring requirements

- FY21 data security assessment
- Identified **gaps** between **current** and proposed **target states**
- Recommended **17 projects** to address gaps
- Projects divided between **Phase II** and **Phase III**

Phase II - Implement

Kudelski Security partnered to deliver projects across **3 workstreams**:

1. **Education and Guidance**
   Equipping users with the knowledge to protect data
2. **User-Facing Protections**
   Empowering users to protect data and implementing guardrails
3. **Critical Repository Protections**
   Identifying confidential repositories to apply appropriate protection

Phase II - Outcomes

- ✓ **Trained** users on data security **standards** and **best practices**
- ✓ Equipped users to **classify** data and **report incidents**
- ✓ Implemented **scalable guardrails** to prevent data leaks
- ✓ Discovery across **asset types**
- ✓ Used **Microsoft 365** for **5 of 8 projects**
- ✓ Matured **6 NIST categories**

KUDELSKI SECURITY

Executive Summary

Three workstreams, eight projects to holistically improve data security

Education and Guidance

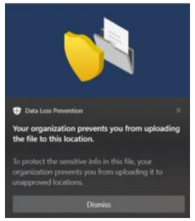
1
CLASSIFY
2
SHARE SECURELY
3
REPORT

1. Training: delivered data security and privacy education to users

2. Reporting: created standard data security incident reporting process

User-Facing Controls

3. File/Email Labeling: established and deployed sensitivity labels for files and email



Data Loss Prevention

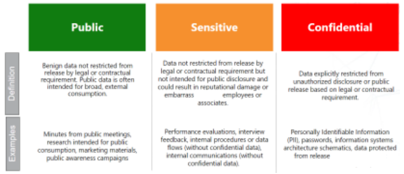
Your organization prevents you from uploading the file to this location.

To protect the sensitive info in this file, your organization prevents you from uploading it to unapproved locations.

4. DLP: deployed removeable media and web DLP controls to protect against data loss

5. Secure Transfer: template for secure external data transfer; implemented for one department

Critical Repository Protections



	Public	Sensitive	Confidential
Definition	Benign data not restricted from release by legal or contractual requirement. Public data is often intended for broad, external consumption.	Data not restricted from release by legal or contractual requirement but not intended for public disclosure and could result in reputational damage or embarrass employees or associates.	Data explicitly restricted from unauthorized disclosure or public release based on legal or contractual requirement.
Examples	Minutes from public meetings, research intended for public consumption, marketing materials, public awareness campaigns	Performance evaluations, interview feedback, internal procedures or data flows (without confidential data), internal communications (without confidential data).	Personally Identifiable Information (PII), passwords, information systems architecture schematics, data protected from release

6. Container Labeling: enhanced SharePoint labels to include sensitivity; discovered confidential sites

7. Structured Discovery: piloted structured repository data discovery and labeling software

8. Application Labeling: enhanced software inventory intake to include fields for confidentiality and criticality

KUDELSKI SECURITY