MAP Pilot

Machine Actionable Plans

RECOMMENDATIONS FOR MAKING MADMPS WORK FOR YOU

A GUIDE FOR IT AND INFORMATION SECURITY DEPARTMENTS

webmgr@arl.org
bit.ly/mappilot

A product of the IMLS-funded MAP Pilot

A collaboration between the Association of Research Libraries (ARL) and the California Digital Library (CDL.)

Institutions like yours are grappling with issues around information security and data security. For many there is a lack of consensus about the best approach and systems to use to remain compliant with sharing and security policies. There are huge variations of need between disciplines, and a lack of awareness among many researchers about the needs for private vs. public data sharing and when each is appropriate.

You may lack sufficient and consistent visibility into researcher needs, compliance, and planning. Data Management Plans (DMPs) are frequently incorporated into grant proposals, but it is often difficult for other departments to access useful information. Even if accessible, they are often not updated, leaving librarians and IT scrambling to provide resources or change a researcher's plans when plans are not updated, or they report something incorrectly in their plans. While some DMPs may be published through the DMP Tool or similar services, accessible DMPs are not necessarily the same version that was submitted with a grant proposal.

Here's the good news. The DMP Tool team, together with ARL, recently worked with a number of institutions to facilitate campus integrations that can enhance data security by helping identify risks; and transform communications,boosting efficiency at your institution. Pilot institutions have connected maDMPs through APIs to local systems and in some cases created new notification systems to better streamline DMP consultation and the allocation of resources; improve communication between departments; prepopulate DMP fields for ease of use; and even create an AI-responsive review tool for maDMPs. There are a lot of avenues for you to explore in alignment with your institution's strategic priorities.

MAP Pilot

Machine Actionable Plans

Benefits of maDMPs

01. Data security posture enhancement

By providing a holistic view of data and its usage, maDMPs can empower IT & security teams to proactively identify and mitigate data security risks. They can also help institutions improve their overall data security posture, making them more resilient to cyberattacks and data breaches.

02. Centralized data management

DMPs provide a single source of truth for research data, allowing security teams to easily monitor and control data access and usage across different systems and applications. This centralized approach simplifies data discovery, making it easier to identify sensitive data and implement appropriate security measures. When machine-actionable, data from DMPs can feed into systems for automated monitoring.

03. Resource allocation

maDMPs can integrate into systems built for resource allocation, so your department can be notified of resource (including equipment, storage, and personnel assistance) needs automatically, helping teams plan and allocate resources reliably.

04. Notifications for efficient consultation

maDMPs can also integrate into systems to be notified of consultation needs, formatted in ways that makes consultation efficient and seamless. One institution has even developed a prototype for an AI tool that supplies automated feedback on DMPs, which could when further developed and integrated with institution systems, create efficiencies for IT & Information Security teams.

05. Enhanced security controls

maDMPs can help enforce data retention policies and ensure that data is securely deleted when it is no longer needed. maDMPs can offer far more rigorous control of security than closed static DMPs controlled by individual researchers.

06. Improved data governance

maDMPs facilitate the implementation of data governance policies and procedures, ensuring that data is used and stored responsibly and ethically. They can help track data lineage, identify data quality issues, and ensure that data is accurate and consistent.

07. Streamlined compliance effort

maDMPs can help institutions comply with data privacy regulations, such as GDPR and CCPA, by providing tools for data mapping, consent management, and data subject access requests. They can also help organizations track and manage data breaches, ensuring that they are handled in a timely and effective manner.

MAP Pilot

Machine Actionable Plans

Recommendations

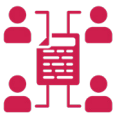
Establish governance and alignment

Join your library in securing the support and sponsorship of senior leadership, demonstrating alignment with institutional strategic priorities, and using case studies and recommendation guides from pilots from other institutions to outline what is achievable. Engage related departments early in the process through demonstrating strategic alignment, and outlining stakeholder benefits with examples to those groups. In both cases, connect maDMP integration potential to institutional goals for research excellence.

Join a cross-functional working group with library, IT, research administration, and faculty representatives to establish policy alignment and implementation priorities; and take part in workflow mapping, conducting a gap analysis of current DMP processes across departments, and identifying points where automation could reduce administrative burden.

Champion a data stewardship and compliance strategy

Implement or champion an institutional research data stewardship and compliance strategy to align research units and supporting departments, instituting a framework that accounts for variability between disciplines. In addition to supporting initiatives like institutional implementation and adoption of maDMPs, it will also help your institution align its policies to strategic priorities and core principles.



Evaluate capabilities

Evaluate API capabilities and data structures ahead of integration planning with your cross-functional team to identify opportunities and anticipate challenges with automation and integration ahead of designing a pilot. Some of our pilot institutions found that not identifying limitations earlier enough in the pilot process limited their progress.

Questions?

Find out more about maDMPs by visiting bit.ly/mappilot and viewing the resources created from the maDMPs Pilot. You can also ask your library about your institution's research data policies and planned or existing integrations

MAP Pilot
Machine Actionable Plans