Securing Institutional Data in a Mobile World
01 | What is a mobile device?
02 | Protecting institutional data
03 | The challenge
04 | What can we do?
01 | What is a mobile device?
What is a “mobile device”?

a phone?
a tablet?
a laptop?
anything that can be physically moved?
A “mobile device”:

• is a *portable computing device* such as a smartphone or tablet;
• is typically operated by being *held in the user’s hand*;
• and, is running a *mobile operating system*. 
There are over 1,000,000 mobile devices in use at UW–Madison

- Institutionally owned
- Personally owned
- Users with two or more devices
Each of these over \[
\begin{array}{ccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}
\]

mobile devices are part of our attack surface
02 | Protecting institutional data
What is “institutional data”?

- data that is damaging if lost?
- data protected by law or policy?
- data that is worth money and time?
- data that doesn’t appear valuable?
“Institutional data”:

- is *any* data that is owned or generated by UW–Madison;
- *is* often protected by law and policy;
- *is* worth money and time;
- and *is almost always* valuable to someone…
- …whether because of the data itself, or the system(s) on which it is stored or accessed.
## UW–Madison Data Classification

### Restricted
Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause a **significant level of risk** to the University, affiliates or research projects. Data should be classified as Restricted if:

- **protection of the data is required by law or regulation,** or
- **UW Madison is required to self-report to the government** and/or provide notice to the individual if the data is inappropriately accessed.

### Sensitive
Data should be classified as Sensitive when the unauthorized disclosure, alteration, loss or destruction of that data could cause a **moderate level of risk** to the University, affiliates or research projects. Data should be classified as Sensitive if the loss of confidentiality, integrity or availability of the data could have a serious adverse effect on university operations, assets or individuals.

### Internal
Data should be classified as Internal when the unauthorized disclosure, alteration, loss or destruction of that data could result in **some risk** to the University, affiliates or research projects. By default, **all Institutional Data that is not explicitly classified as Restricted, Sensitive or Public data should be treated as Internal data.**

### Public
Data should be classified as Public prior to display on web-sites or once published without access restrictions; and when the unauthorized disclosure, alteration, loss or destruction of that data would result in **little or no risk** to the University and its affiliates.
### UW–Madison Data Classification

<table>
<thead>
<tr>
<th>Restricted</th>
<th>Sensitive</th>
<th>Internal</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause a <strong>significant level of risk</strong> to the University, affiliates or research projects. Data should be classified as Restricted if:</td>
<td>Data should be classified as Sensitive when the unauthorized disclosure, alteration, loss or destruction of that data could cause a <strong>moderate level of risk</strong> to the University, affiliates or research projects. Data should be classified as Sensitive if the loss of confidentiality, integrity or availability of the data could have a serious adverse effect on university operations, assets or individuals.</td>
<td>Data should be classified as Internal when the unauthorized disclosure, alteration, loss or destruction of that data could result in <strong>some risk</strong> to the University, affiliates or research projects. By default, all Institutional Data that is not explicitly classified as Restricted, Sensitive or Public data should be treated as Internal data.</td>
<td>Data should be classified as Public prior to display on web-sites or once published without access restrictions; and when the unauthorized disclosure, alteration, loss or destruction of that data would result in <strong>little or no risk</strong> to the University and its affiliates.</td>
</tr>
</tbody>
</table>

- protection of the data is required by law or regulation, or
- UW Madison is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed.
Securing Institutional Data in a Mobile World / Protecting institutional data

**UW–Madison Data Classification**

**Restricted**
Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause a significant level of risk to the University, affiliates or research projects.

Data should be classified as Restricted if:
- protection of the data is required by law or regulation,
- UW Madison is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed.

**Sensitive**
Data should be classified as Sensitive when the unauthorized disclosure, alteration, loss or destruction of that data could cause a moderate level of risk to the University, affiliates or research projects.

Data should be classified as Sensitive if the loss of confidentiality, integrity or availability of the data could have a serious adverse effect on university operations, assets or individuals.

**Internal**
Data should be classified as Internal when the unauthorized disclosure, alteration, loss or destruction of that data could result in some risk to the University, affiliates or research projects.

By default, all Institutional Data that is not explicitly classified as Restricted, Sensitive or Public data should be treated as Internal data.

**Public**
Data should be classified as Public prior to display on websites or once published without access restrictions; and when the unauthorized disclosure, alteration, loss or destruction of that data would result in little or no risk to the University and its affiliates.

“exceptionally grave damage”

“serious damage”

“damage”

“little to no damage”
# UW–Madison Data Classification

## Restricted

Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause a significant level of risk to the University, affiliates or research projects. Data should be classified as Restricted if:

- Protection of the data is required by law or regulation, or
- UW Madison is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed.

## Sensitive

Data should be classified as Sensitive when the unauthorized disclosure, alteration, loss or destruction of that data could cause a moderate level of risk to the University, affiliates or research projects. Data should be classified as Sensitive if the loss of confidentiality, integrity or availability of the data could have a serious adverse effect on university operations, assets or individuals.

## Internal

Data should be classified as Internal when the unauthorized disclosure, alteration, loss or destruction of that data could result in some risk to the University, affiliates or research projects. By default, all Institutional Data that is not explicitly classified as Restricted, Sensitive or Public data should be treated as Internal data.

## Public

Data should be classified as Public prior to display on websites or once published without access restrictions; and when the unauthorized disclosure, alteration, loss or destruction of that data would result in little or no risk to the University and its affiliates.

This is all institutional data.
Securing Institutional Data in a Mobile World / Protecting institutional data

UW–Madison Data Classification

**Restricted**
Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause a **significant level of risk** to the University, affiliates or research projects. Data should be classified as Restricted if:

- **protection of the data is required by law or regulation,** or
- **UW Madison is required to self-report to the government** and/or provide notice to the individual if the data is inappropriately accessed.

**Sensitive**
Data should be classified as Sensitive when the unauthorized disclosure, alteration, loss or destruction of that data could cause a **moderate level of risk** to the University, affiliates or research projects. Data should be classified as Sensitive if the loss of confidentiality, integrity or availability of the data could have a serious adverse effect on university operations, assets or individuals.

**Internal**
Data should be classified as Internal when the unauthorized disclosure, alteration, loss or destruction of that data could result in **some risk** to the University, affiliates or research projects. By default, all **Institutional Data that is not explicitly classified as Restricted, Sensitive or Public data should be treated as Internal data.**

**Public**
Data should be classified as Public prior to display on websites or once published without access restrictions; and when the unauthorized disclosure, alteration, loss or destruction of that data would result in **little or no risk** to the University and its affiliates.

This is our protected Institutional data.
UW–Madison’s annual budget is $3,000,000,000,000 of which $1,200,000,000,000 is research.
Who would want this data?
Who would want this data?

Anyone for whom it has value.
Unlike data breaches we may know about, we may never know about the loss of research data.
Protected institutional research data: the crown jewels of UW–Madison as a premier research university.
03 | The challenge
The challenge:

Protect institutional data accessed via mobile devices
What is Mobile Device Management (MDM)?
What is Mobile Device Management (MDM)?
What is Mobile Device Management (MDM)?

- A way to manage, administer, and secure mobile devices
  - University-owned devices
  - Non-university-owned devices
    - Bring Your Own Device (BYOD)
- A vehicle to secure (access to) institutional data on mobile devices, while keeping personal data segregated
- A tool to implement enforce university IT policies for the protection of protected institutional data
What is Mobile Device Management (MDM) not?

- A way to spy on users’ personal or private data
- A vehicle to violate the law or UW policy
- A tool to arbitrarily remotely wipe devices
What is Mobile Device Management (MDM)?
What is possible with MDM?

- Centralized administration
- Centrally-managed deployment
- Security policy implementation and enforcement
- Inventory management and tracking
- Containerization for certain functions
- Apple Device Enrollment Program (DEP)
- Configuration management (apps, VPN, enterprise services)
- Anonymized metrics collection
- Internal/In-house app catalogs
- Remote wipe — administrative measures
What is not possible? Monitoring of:

- Text messages (SMS, MMS)
- Phone calls (carrier or VoIP)
- Photos, videos, and media
- Personal email and messaging accounts
- Web bookmarks, cookies, browsing history
- Voicemail or other voice messages
- FaceTime, iMessage, Signal, Telegram, WhatsApp, etc.
- GPS or other location data*
- Metadata or historical data related to any of the above

* Unless it is a business requirement, with user permission
When can administrative measures be taken?

- **User request**
- *For a university-owned device*, must be authorized by the Dean or Director of the employing unit, or that unit’s HR department.
- *For a non-university-owned device*, must be authorized by the Dean or Director of the employing unit, in consultation with the UW–Madison Chief of Police or the Provost.
- If ownership of the device is uncertain, *it must be treated as a non-university-owned device.*
If an individual is determined to intentionally misappropriate institutional data, they can do so.

What we are protecting against:

• Unintentional loss of data and devices
• Misconfigured devices
• Lax security
• External threats
• Insider threat (mitigation)
User privacy is paramount — Privacy First

- Multitenant privacy settings for data collection and display
- Role-based access
- Custom privacy notices
- Self-service portal
- AirWatch Privacy App and Privacy Officer
- Data encryption of PII at database level
- Description of what is and is not collected
- Users have full control over the privacy of their personal and private information
The Internet of Things (IoT)

“Internet of Things is shorthand for Internet of Things That Should Not be Connected to the Internet.” — Scott Manley
The Internet of Things (IoT)

- Is expected to exceed 20 billion devices by 2020
- Are often running custom operating systems…
- …which are also often unpatchable or unmanageable
- Questionable security landscape
- Are often be small, mobile, wearable, disposable
- May access (or have access to) institutional data
- Represent both an attack vector and attack surface

- But, many of these devices *can* be managed
04 | What can we do?
Every connected device is part of our attack surface
What is possible with MDM?

- Centralized administration
- Centrally-managed deployment
- Security policy implementation and enforcement
- Inventory management and tracking
- Containerization for certain functions
- Apple Device Enrollment Program (DEP)
- Configuration management (apps, VPN, enterprise services)
- Anonymized metrics collection
- Internal/In-house app catalogs
- Remote wipe — administrative measures
What is possible with MDM?

• Centralized administration
• Centrally-managed deployment
• Security policy implementation and enforcement
• Inventory management and tracking
• Containerization for certain functions
• Apple Device Enrollment Program (DEP)
• Configuration management (apps, VPN, enterprise services)
• Anonymized metrics collection
• Internal/In-house app catalogs
• Remote wipe — administrative measures

Every one of these items was discussed as a need at the 2016 BYOD and Cloud IT Policy Forum
What is possible with MDM?

- Centralized administration
- Centrally-managed deployment
- Security policy implementation and enforcement
- Inventory management and tracking
- Containerization for certain functions
- Apple Device Enrollment Program (DEP)
- Configuration management (apps, VPN, enterprise services)
- Anonymized metrics collection
- Internal/In-house app catalogs
- Remote wipe — administrative measures

Over 60 IT professionals at UW–Madison responded to a 2016 survey indicating a need for MDM.
A UW–Madison central MDM solution
A UW–Madison central MDM solution

- Provides reliable, uniform, managed security to mobile devices as required for UW–Madison users.
- Enables compliance with regulatory requirements or security best practices for mobile devices.
- Supports remote wipe for devices with protected institutional data that are lost or stolen.
- **Architected as an “opt-in” platform as directed by Deans and Directors of university components.**
- Hosted on premise at UW–Madison in the Campus Computing Infrastructure (CCI) environment.
- Does not require any additional software, hardware, or other infrastructure at customer location.
- Is suitable for managing devices that access or process Internal, Sensitive, or Restricted Data.
- Supports institutionally-owned or personally-owned (“Bring Your Own Device”, or BYOD) devices that access protected data classes or are under a management regime.
- **Allows binding to departmental or organizational directory services.**
- Does not manage, access, or manipulate private personal data on personally-owned devices.
- Targeted at devices or systems running Apple iOS or Google Android.
- Supports (but does not require) Apple Device Enrollment Program (DEP) for applicable iOS devices.
- No customer license cost during the pilot.
- Final license cost is being negotiated with the vendor.
- If successful, is intended to seamlessly transition to a UW–Madison production service.
A UW–Madison central MDM solution protects our institutional data.

- Provides reliable, uniform, and comprehensive managed security for UW–Madison users.
- Enables compliance with regulatory requirements or security best practices for mobile devices.
- Supports remote wipe for devices with protected institutional data that are lost or stolen.
- Architected as an “opt-in” platform as directed by Deans and Directors of university components.
- Hosted on premise at UW–Madison in the Campus Computing Infrastructure (CCI) environment.
- Does not require any additional software, hardware, or other infrastructure at customer location.
- Is suitable for managing devices that access or process Internal, Sensitive, or Restricted Data.
- Supports institutionally-owned or personally-owned (“Bring Your Own Device”, or BYOD) devices that access protected data classes or are under a management regime.
- Allows binding to departmental or organizational directory services.
- Does not manage, access, or manipulate private personal data on personally-owned devices.
- Targeted at devices or systems running Apple iOS or Google Android.
- Supports (but does not require) Apple Device Enrollment Program (DEP) for applicable iOS devices.
- No customer license cost during the pilot.
- Final license cost is being negotiated with the vendor.
- If successful, is intended to seamlessly transition to a UW–Madison production service.
• Visit mobile.wisc.edu/mdm
• Join mdm@lists.wisc.edu
• Participate in the MDM discussion
• Deploy MDM in your department or unit
• Raise the issue with Deans and Directors
• Discuss in IT policy and governance forums
• Advocate for central services you believe in
Questions or comments?
mobile.wisc.edu/MDM