DataDiscovery

UW-Madison Policy for Restricted Data Security Management

The current version of the policy is published at: https://kb.wisc.edu/itpolicy/cio-restricted-data-management-policy

The Restricted Data Security Management Policy supports the discovery and protection of UW-Madison Restricted Data on devices and services used for UW-Madison business.

The history of the policy is documented below.

Quick Links

- Current version, including alternative formats
- Archived versions, include comparisons between versions (Wiki login required)
- Policy drafts (if any, Wiki login required)

Recently Updated

IT Policy Process RACI Chart
May 17, 2019 • updated by GARY W DECLUTE • view change

Com Meeting 2019-05-20
May 16, 2019 • updated by GARY W DECLUTE • view change

Documents

Current	Related	Background
• Current version, including alternative formats • Archived versions, include comparisons between versions (Wiki login required) • Draft versions (if any, Wiki login required)	• Sensitive Information Definition (includes Restricted Data definition) • Data Discovery Project	• Security Baseline

History

Milestones, Items of particular interest

Date	Activity
11/03/16	***Version 2017-11-03 published.*** Extended the initial period to Dec 31, 2018, during which only SSN is covered by the policy. In the leading and trailing comments on the policy and procedures documents, indicated that the deadline for reports has been extended to Dec 31, 2018. No reports are due in 2017. All other provisions of the policy still apply. Some additional maintenance updates, (links, references, etc.)
11/17/16	***Version 2016-11-17 published.*** Extended the initial period to Dec 31, 2017, during which only SSN is covered by the policy. In the leading and trailing comments on the policy and procedures documents, indicated that the deadline for reports has been extended to Dec 31, 2017. No reports are due in 2016. Changed the title of the policy and procedures from "Restricted Data Management..." to "Restricted Data Security Management..." to make it clear that the policy only addresses security of restricted data.The URL was not changed. Some additional maintenance updates, (links, references, redundant or unnecessary text, etc.)

08/17/16	***2016-01-08 version, maintenance revision A published.*** In both the policy and procedures, replaced each instance of "Identify Finder" with "Sensitive Data Manager (formerly Identity Finder)". Product was renamed by the vendor. No substantive changes.
01/08/16	***Version 2016-01-08 published.*** Extended the initial period to Dec 31, 2016, during which only SSN is covered by the policy. Migrated to the IT Policy KB. Fixed links. Reformatted some sections for readability. Small changes in language for clarity. The only substantive change was to extend the initial period.
08/2015	Migrated to IT.WISC.EDU website. No substantive changes.
04/14/15	***Version 2015-04-14 published.*** Major revision to change the standard of protection for restricted data, plus minor revisions to include KB and other references. For a detailed comparison with the 2015-03-11 version see DataDiscovery Policy Archive (Wiki login required). Significant policy and procedure changes include but are not limited to: • Change the standard to be used for protecting restricted data. (NOTE: This is the change that make it a major revision.) • Add references to KB articles that include procedures, training, reporting instructions and FAQ. • Add other references.
04/08/15	KB articles are finished. They include procedures, training, reporting form, FAQ, etc.
03/11/15	***Version 2015-03-11 published.*** Major revision. There were signficant changes to the policy. Procedures were almost entirely re-written. For a detailed comparison with the 2014-07-31 version see DataDiscovery Policy Archive (Wiki login required). Significant policy changes include but are not limited to: • Clarify intent of the policy. • Clarify how restricted data is defined, and how that applies to SSN's. • Clarify why the policy will initially only apply to SSN's. • Clarity who the policy applies to. • Clarify what devices and services the policy applies to. • Clarify what must be reported by reference to the reporting procedures – i.e. report whatever the reporting procedures require. Reporting requirements may vary from year-to-year. • Clarify who managers are accountable to. • Add guidance for how to handle pesonally-owned devices and privately contracted services that contain restricted data. • Introduce the concept of "significant use" as a criteria for determining priority for discovery, protection and reporting. The procedures define significant use. (Note: threshold for significant use may need to change as risk level changes.) • Clarify how "satisfactory assurances" are defined. • Clarify the authority of data stewards to make final decisions regarding the management of restricted data. (NOTE: this may become redundant when data governance policy is established.) • Clarify the goals of enforcing the policy (if necessary) by denying access to computing resources. • Specify the standard to be used for protection of restricted data. Signficant procedure changes are too numerious to list. Essentially a complete re-write.
02/20/15	Received final feedback from Legal Services and others. Changes were for clarify and consistency. Revised draft to incoporporate changes.
01/29/15	Revised draft incorporating initial feedback from Legal Services and others. More feedback from Legal Services is pending. There were many changes to improve clarity and consistency. These did not substantially change the meaning. There were three substantive changes: • The original language assumed that actual locations would be listed, (e.g. Laptop #657, etc.) Instead, only aggregate numbers will be reported, without identifying specific locations, (except perhaps in comments or other supplementary information.) There were multiple good reasons for this change. The language of the policy and procedures needed to be adjusted in order to avoid the implication that actual locations must be listed, without precluding it in the future or in special circumstances when following up with units. • "Possible" locations of UW-Madison SSN's must be reported as locations that contain UW-Madison SSN's. The current reporting tool only distinguishes between SSN's present or not present at a location. Reporting possible locations as actual locations does not require that possible locations be otherwise treated the same as actual locations. It will depend upon the circumstances. • Added a section that requires reporting of the location of UW-Madison SSN's that are known, likely or suspected to be present in encrypted data. This question was raised by multiple people. Enryption does not provide complete protection, so we still want to know whether or not SSN's are present when it is practical to make that determination. While there are scenarios where it is not practical to scan or otherwise check encrypted data, the presence of SSN's can sometimes be deduced by other means.

01/06/15	Finsihed draft incorporating feedback from UW-MIST, MTAG and others. Forwarded to CISO, and CIO office for further review. There were several small but substantive changes that removed ambiguities, covered addition cases, or provided necessary additional information to enable or encourage compliance.
01/01/15	***Policy takes effect (the 2014-07-31 version.)*** Development of reporting procedures and other implementation has been slower than projected. Because the deadline for reporting is December 31, 2015, it is not harmful to allow the policy to take effect as originally planned. If the implementation is completed in early 2015, there will still be sufficient time to comply with the policy.
12/23/14	Due date for comments on the policy and procedures by MTAG.
12/16/14	MTAG meeting. Asked MTAG members to comment on the 2014-11-24 policy and procedures by completing two surveys by Dec 23.
12/12/14	Due date for comment comments on the policy and procedures by UW-MIST.
12/04/14	2014-12-04 UW MIST Meeting Agenda. Briefly presented one page summary of the procedures. Ask UW-MIST members to comment on the 2014-11-24 policy and procedures by completing two surveys by Dec 12.
11/24/14	Revised draft. This version was used for review by UW-MIST, MTAG and others. Target date for publishing policy, reporting procedures, baseline plus standard, etc. is now 1 Feb 2015. Project team to coordinate all the pieces for that date. The policy did not fundamentally change from the version published in July. There were, however, a number of adjustement that were more than cosmetic. The implementation procedures were radically revised from the July version. There was very little information about implementation details available in July.
11/21/14	Revised draft.
11/13/14	Revised draft.
11/10/14	Revised draft.
11/06/14	2014-11-06 UW MIST Meeting Agenda. Discussed data discovery priorities, (extracted from 2014-11-03 version). Revised the draft per that discussion. Discussed the difference between the current IT Departmental Secrity Baseline and the first draft of the IT Departmental Security Baseline Plus.
11/03/14	First draft revision of policy and procedures. Target date for publishing is 1 Jan 2015.
10/23/14	Discussed reporting priorities at data discovery project meeting. Look OK.
10/16/14	Meeting to discuss design of reporting procedures. Drafted and forwarded priorities for reporting based upon that meeting.
08/06/14	IT Policy Forum 2014-08. Discussion of data discovery.
08/06/14	Restricted Data Discovery and Management project meeting.
07/31/14	***Version 2014-07-31 published on CIO policy page.*** Notes: • The policy does not take effect until January 1, 2015, to allow time to develop the reporting procedures and other implementation details. • The procedures in this version are primarily a placeholder.
07/30/14	Restricted Data Discovery and Management project meeting.
07/28/14	***CIO approves version 2014-07-31 for publication.***
07/23/14	Restricted Data Discovery and Management project meeting.
07/22/14	DoIT begins a comprehensive scan for SSN on DoIT computers.

07/21 /14	Revision of plan for publishing the policy. Goal is still July 31.
07/16 /14	Restricted Data Discovery and Management project meeting.
07/10 /14	CISO approves revisions. Submitted v2014-07-10b to CIO for review. (Only change was to reduce the amount of markup, leaving just the substantive revisions marked.)
07/10 /14	Revised policy draft, v2014-07-10a submitted to CISO for review. Summary of changes: • Effective date of policy will be Jan 1, 2015. • Policy will only apply to SSN's from Jan 1, 2015 to Dec 31 2015. This period may be extended. • Clarified roles, accountability and responsibility for compliance. • Clarified alternative procedures for reporting restricted data on personally owned devices. • Clarified that scope of policy applies to both UW-Madison-owned and non-UW-Madison owned devices when they are used for university busines. • Clarified applicability to both graduate and undergraduate student employees. Other students are exempt. • Provided informal background definition of "UW-Madison Data". • Added extensive text to background regarding university respect for the privacy of the individual, and respect by individuals for university obligations to protect the data. • Clarified enforcement for contrators and associates. • *Very extensive* modification of the implementation procedures. A majority of comments received were implementation issues, plus the intial draft procedures were rough and largely incomplete.
07/09 /14	Restricted Data Discovery and Management project meeting.
07/08 /14	Restricted Data Discovery and Management communications team meeting.
07/07 /14	Summarized recommended changes to draft policy based on feedback during the comment period. Discussion of revisions.
07/03 /14	***Comment period ends. Summarized comments received during the policy comment period.***
07/02 /14	Restricted Data Discovery and Management project meeting.
06/26 /14	Development of plan for publishing the Restricted Data Management policy by July 31.
06/25 /14	Restricted Data Discovery and Management project meeting.
06/23 /14	***Kick off meeting of the Restricted Data Discovery and Management project.***
06/19 /14	Comment period on policy draft v2014-06-04 begins.
06/17 /14	Policy draft v2014-06-04 discussed at MTAG.
06/10 /14	Planning for the Restricted Data Discovery and Management project.
06/05 /14	Policy draft v2014-06-04 discussed at UW-MIST.
05/12 /14	Revised the implementation to introduce a two-phased approach that only requires the discovery and reporting of SSN's during Phase I.
05/07 /14	Policy Planning Team meets to discuss security policy in general, and the draft policy in particular, including suggestions for vetting, etc. Result is the 2014-05-07a draft.
05/07 /14	UW-Madison IT Security Office meets to discuss the draft, including suggestions for vetting, etc. Result the 2014-05-07 draft.
05/05 /14	Development of the Data Discovery Service is accelerated. This is related to the pilot implementation of the poilcy and procedures and subsequent revision from lessons learned.
05/03 /14	Draft of rough timeline for policy development.
05/02 /14	***First draft cleared to begin vetting process.***

05/01/14	***First draft of policy. In a nutshell:*** • All UW-Madsion units, including their contractors and associates, must report annually on the presence of restricted data on all computer services, devices and media used for university instruction, research and administration, and • includes reduction of the presence of Restricted Data, because the best way to reduce the risk is to reduce the amount present, and a convenient time to work on this is in conjunction with an annual reporting process. Implementation procedures specify: • use of Identity Finder with scan results reported centrally is sufficient to meet the reporting requirement, (with the exception of Restricted Data that Identify Finder is generally unable to locate,) along with additional cases and means of reporting. • the importance of piloting the implementation and adjusting the policy and procedures based on lessons learned, and • the need for a period of adjustment to allow campus to implement supporting services and allow units to implement internal reporting procedures using those services.
04/2014	Meetings with leadership, including a report on baseline security project. Gap: use of Identity Finder to locate restricted data is not mandatory. Consensus among leadership that locating Restricted Data should be mandatory. Decision is made to address this gap immediately.

Contact