Steve Smith

From: Bob TURNER
Sent: Thursday, June 29, 2017 10:01 AM
To: David Stack
Cc: Robert Cramer; UW-Madison Provost; LAURENT HELLER; Secretary of the Faculty; MICHAEL LEHMAN; John Krogman; uw-mist@lists.wisc.edu
Subject: RE: UW System Information Security Policies - Invitation to Review and Comment by June 30, 2017

David,

The UW System Information Security policies and procedures were reviewed by the UW-Madison Information Security Team which is a cross section of the institutions information security community and a fair representation of the academic, research and administrative communities. I am inserting substantive comments and recommended corrections to the linked documents as directed in Rob Cramer's e-mail and should be complete by close of business Friday, June 30th. The table below summarizes significant comments and recommended corrections:

Policy/Procedure #	Policy/Procedure Title	Comments/Recommended Changes
Revised Policy and Procedure		
1030/1030A	Authentication	No comments or corrections submitted. Based on action at this past Tuesday's UW Information Assurance Council meeting, this policy will be reviewed and updated by UW-IAC Policy Review Team no later than July 30th. Changes will be based on NIST 800-63-3 – Digital Identity Guidance released in Mid-June
1031A	Data Classification	Under 4. Procedures, item iii – this statement seems out of place as a data steward's action in a data classification procedure. Perhaps the statement should be an action for a system owner or sponsor.
New Policy and Procedure		
1035	Data Protection	• In 6. Policy Statement in addition to the FERPA notice showing how data can contain elements from multiple classifications, the concepts for limited data set Personal Health Information should also be detailed.
1035A	Data Protections Procedure	• In several places the word "university" is used where the term "institution" is more appropriate and in keeping with the naming convention in the other policies and procedures. • Examples should be provided for the more complex issues that are addressed in simple statements. Examples include including context for the encryption and authentication of information while being copied, printed or in transmission; and the "Must securely destroy…" statement in the Media Sanitization and Disposal line in the table starting on Page 2 (actual statement is on Page 4) • In the table starting on Page 2 of the draft, recommend deleting the Low Risk (Public Data) column and insert a statement in the narrative stating "low risk data requires no special protections or restrictions" • Same table – the requirement for multi-factor authentication for High Risk should indicate a phase-in period will be given to prevent many projects from being out of compliance the day the procedure is signed. Recommend add after the word "required" the phrase "as institutionally supported solutions become available." Adding a statement of the intended date/month/quarter the controls must be in place.

		• Same Table – in the Data Storage line for High Risk information the data encryption line appears to be a less restrictive statement that the one in the Access Control line.

I appreciate the opportunity the UW IAC gave me to lead the Policy Review Team. The team's collective wisdom and recommended actions on policy and procedure place us in much better shape to push forward with common approaches to materially reducing risk associated with these critical cybersecurity issues.

Bob Turner
Chief Information Security Officer
Office of the CIO and Vice Provost for Information Technology
University of Wisconsin-Madison
1210 W Dayton Street, Room 2112
608-263-2477 – Office
608-572-6671 – Mobile
bob.turner@wisc.edu
https://it.wisc.edu/about/office-of-the-cio/cybersecurity/

OFFICE OF CYBERSECURITY
CIO AND VICE PROVOST FOR INFORMATION TECHNOLOGY
UNIVERSITY OF WISCONSIN-MADISON

From: David Stack [mailto:dstack@uwsa.edu]
Sent: Thursday, June 08, 2017 6:20 PM
To: UW Information Assurance Council <uwiac@uwsa.edu>; UW Technical Information Security Committee <uwtisc@uwsa.edu>
Subject: FW: UW System Information Security Policies - Invitation to Review and Comment by June 30, 2017

Please note this email message from Rob Cramer asking for broad stakeholder input on all of the proposed information security policy revisions by June 30th.

— David

David Stack
Interim Associate VP & CIO
University of Wisconsin System
dstack@uwsa.edu

From: Rob Cramer <rcramer@uwsa.edu>
Date: Wednesday, June 7, 2017 at 2:51 PM
To: Rob Cramer <rcramer@uwsa.edu>
Subject: UW System Information Security Policies - Invitation to Review and Comment by June 30, 2017

Good afternoon,

The eight UW System Administrative Policies and Procedures on information security are scheduled for regular review. Revisions to these policies and procedures have been proposed for your review. In addition, a new policy and procedure (1035 & 1035.A) focusing on *Data* Protections are being proposed for adoption. Please see attached a summary of the proposed policy revisions and actions.

Links to access each draft policy and procedure are below. Please share with others at you institution as appropriate. This note is being sent to:

- Provosts
- Chief Business Officers
- Senior Student Affairs Officers
- Chief Information Officers
- Faculty Representatives
- Academic Staff Representatives
- University Staff Representatives
- Student Representatives

A UW Login is required to view each draft policy and procedure and provide comments. At the top of each revised policy/procedure are track changes indicating revisions to the current version of each document. Please provide comments through the relevant links to each policy/procedure by **June 30, 2017**.

Revised:
UW System Administrative Policy 1030, *Information Security: Authentication*
UW System Administrative Procedure 1030.A, *Information Security: Authentication*
UW System Administrative Policy 1031, *Information Security: Data Classification*
UW System Administrative Procedure 1031.A, *Information Security: Data Classification*
UW System Administrative Policy 1032, *Information Security: Awareness*
UW System Administrative Policy 1033, *Information Security: Incident Response*

Note: UW System Administrative Procedure 1032.A & UW System Administrative Policy 1034, *Acceptable Use*, are proposed for rescission.

New:
UW System Administrative Policy 1035, *Information Security: Data Protections*
UW System Administrative Procedure 1035.A, *Information Security: Data Protections*

I appreciate your time and attention to this important matter.

Sincerely,

Robert

Robert Cramer
Vice President for Administration