UWM POLICY ON THE PROTECTION OF CONFIDENTIAL RESEARCH DATA

No: _____

History: Original _____ ____, 2009

Authority: UWM's Information Security Policy (S-59) (and references therein)

Initiators: Provost and Vice Chancellor for Academic Affairs; Vice Chancellor for Research & Economic Development

Responsible Parties: Information Security Architect and Associate Dean for Research, Graduate School

---

I. PURPOSE

The University of Wisconsin-Milwaukee is committed to establishing administrative, technical and physical safeguards for information systems and processes. This commitment requires ongoing risk assessments and data protection efforts. One activity requiring ongoing data protection efforts is research. The validity of research outcomes is dependent on the integrity of research data.

Researchers at the University of Wisconsin-Milwaukee obtain data from various sources for research purposes. Certain research data may be categorized as "confidential" according to standards adopted by UWM and referenced below in section III. This includes confidential data obtained to assess whether the potential exists to develop a research project. This policy outlines how UWM will protect confidential research data.

UWM encourages the use of similar procedures for the voluntary protection of sensitive data and may require their use in some cases.

II. POLICY

It is the policy of the University of Wisconsin-Milwaukee that confidential research data be adequately safeguarded and protected at all times. This policy is accomplished through the use of data security plans and related documents which must be approved and implemented in all cases before confidential data is received or generated. Amended plans must be approved before data is used or shared beyond the scope of the original plan. In some cases, the data security plans may be incorporated into IRB reviews or contract approval processes but these do not remove the obligation to put an approved plan in place.

III. DEFINITIONS

Research includes all activities specifically undertaken to produce research outcomes, regardless of whether theses activities are commissioned by an agency external to UWM.

Confidential data is data which, if accessed by unauthorized entities, (1) could cause personal or institutional financial loss, (2) would constitute a violation of statute, act or law, (3) would constitute a violation of confidentiality agreed to as a condition of storing or transmitting data. Examples of such data include social security numbers, credit card numbers, and data covered by FERPA or HIPAA. This data may be obtained from an external source (with appropriate agreements in place), internal institutional source, or generated by a research activity, either funded or unfunded. (The "UWM Information Security Standards" provide a more thorough definition and discussion of confidential data, and is available through the University Information Technology Services website.)

IV. PROCEDURES

All researchers using confidential data in the course of research must have a data security plan which has been approved and implemented prior to receipt or creation of confidential data. The plan should meet the protection standards described in the ""UWM Information Security Standards."

In addition, researchers who obtain data from external sources that require a University agreement must also complete an approved Data Protection Agreement Signature Request Form (see section B). Researchers who plan to use UWM data must complete an approved Request Form for UWM Information for Research Purposes (see section C).

A. Data Security Plans

Researchers should follow the below steps to create and seek approval for a data security plan:

1. The researcher works with the school/college information technology staff to complete the Data Security Questionnaire (Appendix A).

2. The researcher submits the Data Security Questionnaire to the Information Security Architect for review. The Information Security Architect will work with the researcher to create a Data Security Plan.

3. The researcher submits the plan to the school/college Unit Business Representative (UBR) or associate dean, and the Information Security Architect for review and approval.

4. The researcher submits the plan to the Dean for approval once it has been approved by the school/college UBR or associate dean, and the Information Security Architect,

The researcher is responsible for ensuring (a) the Data Security Plan is accurate and (b) that confidential data is used consistent with terms of the Plan.

The school/college and Information Security Architect are responsible for (a) ensuring that the Data Security Plan reasonably protects confidential data to be used in the described research and (b) monitoring the researcher's compliance with the Plan.

The school/college and the Information Security Architect must retain copies of the Data Security Plan for a period of eight (8) years following completion of the research.

The researcher must retain a copy the finalized Data Security Plan until all confidential data is returned or destroyed. If the researcher leaves the University, confidential data cannot be removed without an agreement between the researcher and the Information Security Architect.

B. Data License Agreements with Outside Entities

Researchers at UWM sometimes obtain data from external sources for research purposes, which includes identifying whether the potential exists to develop a research project. Some sources require a University signature on an agreement to protect the data. *In these cases, a researcher cannot sign such an agreement.* The signature must be from the Office of Sponsored Programs (OSP) regardless of funding for the research and regardless of whether or not the research is funded.

The following process should be observed to ensure that the data is properly protected before RSA signs the required agreement:

1. The researcher completes a Data Protection Agreement Signature Request Form (Appendix B), attaching both a completed Data Security Plan (Appendix A) and a copy of the data protection agreement proposed by the external source. The researcher should work with school/college information technology staff in completing these documents. By completing this request, the researcher documents the special protections that will be employed to keep the data secure. These protections must be in accord with the protections required by the data source.

2. The researcher submits the plan to the school/college Unit Business Representative (UBR) or associate dean, and the Information Security Architect for review and approval..

3. The UBR/associate dean and the Information Security Architect will review the request and work with the researcher to obtain additional information or to clarify the request if needed, and to ensure that the right protections are employed.

4. When the UBR/associate dean and Information Security Architect are satisfied that the researcher's plan meets the requirements of the external source and adequately safeguards the data, the UBR will forward the agreement to OSP with a cover note indicating approval by both the school/college and Information Security Architect and advising OSP that it is acceptable to sign the agreement.

5. The researcher will attach a copy of the Data Protection Agreement Signature Request Form, Data Security Plan, and the agreement with the external source to the WISPER record of the agreement.

Other reviewing bodies, such as UWM's Institutional Review Board, may request confirmation from the researcher that the review process has been satisfactorily completed.

The school/college and the Information Security Architect must retain copies of the Data Security Plan, Data Protection Agreement Signature Request Form, and the agreement with the external source for a period of eight (8) years following completion of the research.

The researcher must retain a copy of the finalized data security plans until all confidential data is returned or destroyed. If the researcher leaves the University, confidential data may not be removed from the university or taken with the researcher without a signed written agreement between the researcher and the university to ensure that all obligations under the agreement with the data source are met.

C. Use of UWM Data for Research

Any researcher who wishes to access non-confidential UWM information for the purposes of research should contact UWM's Public Records Custodian. Such records will be made available on the same terms as to any member of the public.

If a researcher seeks to access UWM information or data that would not be releasable to member of the public, the researcher should follow the process outlined below:

1. The researcher completes a Request Form for UWM Information for Research Purposes (Appendix C) and Data Security Plan (Appendix A) and submits both forms to the Dean or Division Head for the unit holding the information and to the Dean of the researcher's home School or College. The researcher should work with school/college information technology staff in completing these documents.

2. The Dean or Division Head for the unit holding the information reviews the request and consults with the Dean of the researcher's home School or College (regarding how the research supports the university's mission), the Office of Legal Affairs (regarding any legal issues associated with

granting the request), and the Information Security Architect (regarding the adequacy of the Data Security Plan). If the Dean or Division Head is satisfied that release of the information supports the mission and objectives of the university, and that all legal and security concerns have been properly addressed, the Office of Legal Affairs prepares a UWM Data Security Agreement.

3. The Dean or Division Head for the unit holding the information meets with the researcher to discuss the UWM Data Security Agreement and obtain signature by the researcher. The Dean or Division Head then forwards the agreement to the Provost for approval and signature.

4. After the UWM Data Security Agreement is fully executed, the unit holding the data may release it to the researcher. At all times, the unit holding the data is responsible for overseeing the researcher's compliance with the UWM Data Security Agreement. Any breaches of the agreement must be reported to the Provost as soon as they are discovered.

The school/college and the Information Security Architect must retain copies of the Data Security Plan, the Request Form for UWM Information for Research Purposes, and the UWM Data Security Agreement for a period of eight (8) years following completion of the research.

The researcher must retain a copy the finalized Data Security Plan until all confidential data is returned or destroyed. If the researcher leaves the University, confidential data cannot be removed without an agreement between the researcher and the Information Security Architect.

V. Compliance Date for Existing Confidential Data

Researchers who hold confidential data at the time this policy becomes effective have twelve months to secure an approved Data Security Plan.

VI. Sanctions

Failure to comply with this policy may result in loss of privileges to access confidential research data, university disciplinary action, loss of state liability protection, and/or civil or criminal prosecution. The appropriate due process and policies will be followed depending upon whether faculty, academic staff, classified staff or students are alleged to be involved.

VII. Contact Information

Questions regarding the interpretation of this policy should be directed to:

Information Security Architect

[insert contact info]

APPENDIX A:
DATA SECURITY QUESTIONNAIRE

All researchers using confidential data in the course of research, including assessing whether the potential exists to develop a research project, must have a data security plan which has been approved and implemented prior to receipt or creation of confidential data.

Confidential data is data which, if accessed by unauthorized entities, (1) could cause personal or institutional financial loss, (2) would constitute a violation of statute, act or law, or (3) would constitute a violation of confidentiality agreed to as a condition of storing or transmitting data. Confidential Data is defined in the Data Classification document located on the UITS website. Examples of such data include social security numbers, credit card numbers, data covered by FERPA or HIPAA. Researchers are encouraged to consult the "UWM Information Security Standards" available through the University Information Technology Services website for a more thorough definition and discussion of confidential data.

Researchers should confer with their Institutional Review Board if the request involves human subjects.

1	Date	
2	Name of PI	
3	Department/College	
4	What is the confidential data that you are working with in your research (e.g. social security numbers, patient health information, student information, financial information, etc.)?	Describe:
5	What will the data be used for (briefly describe project and data usage need)?	Describe:

6	Who will need to access the research data? (e.g. number of employees, undergraduate students, graduate students, non-UWM persons, etc.)	Describe:
7	Where will the data be accessed from: (e.g. specific UWM location(s); from researcher's home)?	Describe:
8	Will the data be forwarded outside of UWM either electronically or on paper?	Y/N. If Y, describe:

9	What will happen to the data when the project is completed?	Data:
10	Where will the data be stored? Choose all that apply: ❖ On a file Server housed at UWM a) operated & maintained by UWM people b) operated by UWM people, maintained by vendor or consultant c) operated & maintained by external vendor or consultant ❖ On a file service housed, operated and maintained by external vendor ❖ On a desktop computer ❖ On a laptop computer ❖ Other (describe).	Answer:
11	If a file server is housed at UWM: ❖ Where is server housed? ❖ Who operates and maintains the server and software?	Location_____ Server/Software Maintainer:

12	If the file services are provided by external vendor: ❖ Does proposed vendor contract include confidential information rider(s)? ❖ Attach a description of vendor security processes and configuration	Y/N Security program attached? Y/N
13	Are there any special processes or steps proposed to ensure that the data is protected? .	Describe:
14	Please provide any additional supporting information.	Y/N

APPENDIX B:
DATA PROTECTION AGREEMENT SIGNATURE REQUEST FORM

Use this form to request confirmation from the School/College UBR and Information Security Architect that research data obtained from an external source will be protected in accord with the protections required by the data agreement. This form is to be used regardless of whether external funding is sought and whether the data is de-identified or not.

Researchers should confer with their Institutional Review Board if the request involves human subjects.

Researchers must not sign the agreement with the external data source. The University signature must be provided by Office of Sponsored Programs (OSP) after this request is approved by the UBR, Information Security Architect, and Dean.

1	Date	
2	Name of requester	
3	Department	
4	Name of external source providing data	
5	What is external source (e.g. federal government agency, state government agency, foreign government, private company, non-profit organization, etc)?	Provide details:
6	What is the data? What parts of the data are confidential?	Describe:

7	How will the data be used for research at UWM?	Describe:
8	Attach copy of external data source request.	
9	Attach copy of Data Security Plan	

I hereby certify that the attached Data Security Plan meets the requirements of the license agreement for that data.

I hereby certify that the School/College and researcher understand the requirements of the license agreement for the data and are responsible for compliance with the agreement and the attached Data Security Plan.

I certify that a copy of this request, the Data Security Plan, and the agreement will be maintained both by the researcher and the School/College business office for a period of eight (8) years following completion of the research.

_____ _____
Signature of Researcher Date

_____ _____
Signature of UBR or Associate Dean Date

_____ _____
Signature of Information Security Architect Date

_____ _____
Signature of Dean Date

[This request form and attachments should be submitted to Research Services Administration, Attention: _____.]

APPENDIX C:
REQUEST FORM FOR UWM DATA FOR RESEARCH PURPOSES

Use this form to request the use of UWM data for research purposes.

Researchers should confer with their Institutional Review Board if the request involves human subjects.

This request form should be submitted to the Dean or Division Head of the UWM unit holding the data.

1	Date	
2	Name of requester	
3	Department	
4	Name of unit holding requested data	
5	What is the data? What parts of the data are confidential?	Describe:
6	How will the data be used for research at UWM?	Describe:

7	How does this research support UWM's mission (e.g. will it improve the quality of teaching or economic development in the region)?	
8	Over what period of time will the data be used?	
9	What will happen to the data following completion of the project?	
9	Attach copy of Data Security Plan	