GLB Act Compliance Goes Beyond FERPA

RESOURCES

EDUCAUSE Midwest Regional Conference 2005
Chicago, IL

Suzanne Carter, University Legal Counsel
cartersl@legal.uwm.edu

David Stack, Deputy CIO
david@uwm.edu

University of WI–Milwaukee

Slides from the conference presentation
Sample privacy notice
Confidentiality agreement for IT staff
Draft of security program

Copyright The Board of Regents of the University of Wisconsin System 2005
This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.
GLBA: Why care?

- The Gramm-Leach Bliley Act of 1999 is intended to ensure that proper protections are in place before an individual’s personal financial information is disclosed to a third party.

GLBA: Why care?

- FERPA “protects the privacy of student education records” not financial information.
- There are areas of exposure that FERPA safeguards don’t address.
- E.g., services not provided solely to students.

GLBA: Why care?

- GLBA was not intended to apply to higher ed, but the FTC has determined that universities are “financial institutions” because we disburse financial aid.

GLBA: Why care?

- Pro-active, good faith efforts may be a valuable asset in court.
**Definitions**

- **Consumer**
  - Individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual’s legal representative. Example: applying for a loan.

- **Customer**
  - A consumer who has a *continuing relationship* with a financial institution.
  - E.g: agreeing to obtain tax or credit counseling services.

**Definitions**

- **Personally Identifiable Financial Information – PIFI:**
  - “… any information that a financial institution obtains about a consumer in conjunction with providing a financial product or service.
  - This includes information provided during any financial transaction.”
  - (FFIEC)

**Components of GLB**

- I. Privacy notices (reporting)
- II. Safeguarding of information

**I. Privacy Notices**

- **Identify the programs that capture PIFI:**
  - And are not already covered by FERPA, e.g.,
    - University provided mortgages
    - Campus financial clinics
    - Short-term loan services
  - No need to focus on financial aid or scholarships

- **FTC Requirements:**
  - Financial Institutions must not disclose PIFI to a nonaffiliated third party any nonpublic personal information unless it provides or has provided to the consumer a *clear and conspicuous* statement including the following…
I. Privacy Notices

• FTC requires that notices include:
  – Description of the PIFI collected
  – The Institution’s policies with regard to disclosing PIFI
  – Categories or types of persons or entities to whom PIFI may be disclosed;
  – Contact information in case consumers have questions

• FTC Requirements:
  – Consumer must be given opportunity, before PIFI is first disclosed to direct that the information will not be disclosed.
  – Consumer must be given an explanation of how he or she may exercise this nondisclosure option.

• FTC Requirements:
  – Notices are required for customers regardless of whether the institution shares the information with nonaffiliated third parties.

• FTC Requirements:
  – Notices are required for consumers only if the institution shares information with nonaffiliated third parties outside of “specific exceptions.”

• FTC Requirements:
  – “Specific exceptions” where privacy notices to consumers are not required:
    • disclosures necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes.

• FTC Requirements:
  – In addition, institutions should review policies to protect PIFI, e.g.,
    • Employee Training
    • Confidentiality Agreements or Statements
    • Risk Assessments
    • Methods for Tracking Disclosures
UWM’s Process:

• Interdisciplinary team
• Formed by Vice Chancellor for Administration
  – Legal Counsel
  – Bursar’s Office
  – Financial Aid Office
  – Internal Audit
  – CIO Office

UWM’s Process:

• I. Privacy Notices
  – Identified programs that handled PIFI
  – Survey of Unit Business Managers

UWM’s Process:

• I. Privacy Notices
  – 1. A Low Income Tax Clinic
  – 2. The Bookstore check cashing service
  – 3. A deferred payment plan offered by Parking and Transit
  – 4. Salary advances to new, unclassified employees

UWM’s Process:

• I. Privacy Notices
  – The team worked with the identified programs to craft customer privacy notices that meet the aforementioned requirements

UWM’s Process:

• I. Privacy Notices
  – Legal Affairs and Internal Audit worked with the programs to refine their PIFI practices
    • PIFI training for employees
    • Employees initialed confidentiality statements

UWM’s Process:

• II. Safeguarding of Information
  – GLB Act requires a written security program
  – Recognized opportunity to align with other burgeoning campus security initiatives
UWM’s Process:

II. Safeguarding of Information
   - Formed 4 sub-teams:
     • Security Awareness
     • Human Resources
     • Information Security Response
     • Procurement

UWM’s Process:

II. Safeguarding of Information
   - Security Awareness Sub-Team Membership
     • i. University Relations
     • ii. Internal Audit
     • iii. Human Resources
     • iv. Faculty technology committee
     • v. University business managers
     • vi. University personnel managers
     • vii. Student Association
     • viii. Community engagement program

UWM’s Process:

II. Safeguarding of Information
   - Human Resources Sub-Team Membership
     • i. Human Resources
     • ii. University personnel managers
     • iii. Classified Staff
     • iv. Internal Audit
     • v. Legal Affairs
     • vi. CIO Office

UWM’s Process:

II. Safeguarding of Information
   - Information Security Response Sub-Team Membership
     • i. Security Incident Response Team (SIRT)
     • ii. Computer Security Incident Response Team (CSIRT)
     • iii. Desktop Security Core Team
     • iv. Server Security Core Team
     • v. Internal Audit
     • vi. Records Retention/Archivist

UWM’s Process:

II. Safeguarding of Information
   - Security Awareness Sub-Team Objectives
     • i. Develop activities
     • ii. Establish awareness campaign
     • iii. Target key individuals
     • iv. Allow for personal response
     • v. Reach broad audiences
     • vi. Develop secure habits
     • vii. Provide security training
     • viii. Assess the efforts

UWM’s Process:

II. Safeguarding of Information
   - Human Resources Sub-Team Objectives
     • i. Establish employee training
     • ii. Establish reference check procedures
     • iii. Draft position description language
     • iv. Develop code of conduct
     • v. Draft employee confidentiality statement
     • vi. Establish criminal background check procedures
     • vii. Establish credit check procedures
UWM’s Process:

II. Safeguarding of Information
– Information Security Response Sub-Team Objectives
  • i. Respond to security incidents
  • ii. Establish risk assessment activities
  • iii. Proactive response to vulnerabilities
  • iv. Develop security manual
  • v. Reporting of incidents
  • vi. Mission resumption planning

UWM’s Process:

II. Safeguarding of Information
– Procurement Sub-Team Membership
  • i. Purchasing Office
  • ii. A Unit Business Managers
  • iii. Legal Counsel
  • iv. E-Payment Core Service Team

Outcomes:

I. Privacy Notices
– Four programs that handle PIFI now provide their customers with Privacy Notices

Outcomes:

II. Safeguarding of Information
– Security Awareness Sub-Team launched campus-wide campaign, including:
  • Front page article in campus newspaper
  • Email reminders
  • CDs with anti-virus and anti-spyware
  • Free training courses

Outcomes:

II. Safeguarding of Information
– Human Resources Sub-Team identified codes of conduct for IT staff:
  • State of Wisconsin Employment Code of Ethics
  • American Association of University Professors Statement of Professional Ethics
  • UW System Unclassified Staff Code of Ethics
  • IT Professional Conduct Guidelines
Outcomes:

• II. Safeguarding of Information
  – Human Resources Sub-Team developed a confidentiality agreement for IT staff to sign

Outcomes:

• II. Safeguarding of Information
  – Human Resources Sub-Team drafted position description language regarding criminal background checks:
    "Please note: This position requires a criminal records review consistent with the Wisconsin Fair Employment Act."

Outcomes:

• II. Safeguarding of Information
  – Human Resources Sub-Team identified State of WI resources for checking references and conducting interviews
    – [Web Link]

Outcomes:

• II. Safeguarding of Information
  – The Procurement Sub-Team drafted language that is now included on all POs:
    "RELEASE OF INFORMATION: Contractor shall not report or release information concerning UWM or its students, employees or customers to third parties without UWM’s prior written approval. Any such report or release of information shall, at a minimum, comply with those requirements enumerated in the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., UWM’s standards for safeguarding such information, and all other applicable laws regarding consumer privacy."

Outcomes:

• II. Safeguarding of Information
  – As required by GLBA, a Security Program has been written in accessible language to meet the requirements of:
    • Designating responsible employees
    • Instituting employee training program
    • Assessing internal and external risks
    • Devising methods for detecting, preventing and responding to attacks
    • Oversees service providers (vendors)
    • Evaluates and adjusts itself
Outcomes:

• II. Safeguarding of Information
  – Our security program:
  • Incorporates the aforementioned outcomes
  • Is based on a template provided by the Council
    On Law In Higher Education,
    www.clhe.org/programs/fedtrade/safeguardsoutline.pdf

Resources:

– UW–Milwaukee security website
  security.uwm.edu
– EDUCAUSE GLB resource page
  http://www.educanse.edu/Browse/645/?PARENT
  T_ID=673
– Other professional societies also have GLB
  resources and templates
PRIVACY NOTICE

As an institution of higher learning, the University of Wisconsin—Milwaukee (UWM)’s duties extend beyond offering degree programs. UWM supports activities designed to promote the economic development of the community and provides hands-on learning opportunities for its students. The UWM Low Income Taxpayer Clinic fulfills both these goals.

In the course of making the services of the Low Income Taxpayer Clinic available to you, we must collect certain financial information about you. This notice of our privacy policy is meant to assure you of our commitment to maintaining the confidentiality of this information. It explains how we may collect this information, the type of information we collect, and what information we may disclose about you.

THE INFORMATION WE MAY COLLECT

In conjunction with your use of the Low Income Taxpayer Clinic, we may collect your social security number, information about your wages, assets, household, and demographic make-up, and related correspondence to or from the Internal Revenue Service and the Wisconsin Department of Revenue.

HOW YOUR INFORMATION IS PROTECTED

We restrict access to information about you to Low Income Taxpayer Clinic staff. All Low Income Taxpayer Clinic staff members are bound by contract to maintain the confidentiality of such information. Additionally, we maintain physical and electronic safeguards that comply with federal and state laws and UWM policies to protect this information.

INFORMATION WE MAY DISCLOSE

In the course of working on your behalf, we may disclose information we collect to the Internal Revenue Service and the Wisconsin Department of Revenue.

QUESTIONS

If you have any questions concerning this Privacy Notice, please contact ____________ at (414) 229-__.
UNIVERSITY OF WISCONSIN - MILWAUKEE
Department of __________________
Employee Confidentiality Agreement

In consideration of my employment and/or continued employment at the University of Wisconsin-Milwaukee (UWM), Department of Financial Aid, I agree as follows:

1. For purposes of this Agreement, "confidential information" is defined as information that is (a) information disclosed to me or known by me as a consequence of my employment, and not generally known outside UWM or the Department; or (b) protected by State or Federal laws. Confidential information may include records or data protected by laws such as the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act, and the following Wisconsin Statutes: Section 19.21-19.39 (public records laws) and Section 19.81-19.98 (open meetings laws).

2. During my employment and after the termination of my employment, I will hold the confidential information of UWM and the Department in trust and confidence. I will safeguard confidential records, and will not use or disclose it or any embodiment thereof, directly or indirectly, except as may be necessary in the performance of my duties for UWM and the Department. I understand that any unauthorized disclosure could be highly damaging to UWM, its employees, students, donors, or others.

3. I will not remove materials containing confidential information from UWM or the Department unless authorized to do so by my supervisor. Any and all such materials are the property of UWM and/or the Department. Upon termination of any assignment or as requested by my supervisor, I will return all such materials and copies thereof to the Department.

4. I understand that I should contact my supervisor if I am asked to disclose confidential information or if I have questions relating to what constitutes a confidential record.

5. I understand that if I violate this Agreement, I may be subject to disciplinary action, including termination or legal action, or both.

IN WITNESS WHEREOF, and intending to be legally bound, I have hereunto set my hand on this ___ day of ________________, 20___.

EMPLOYEE: ___________________  SUPERVISOR: ___________________
DRAFT

University of Wisconsin Milwaukee
Information Security Program
Revised 3/21/05

Prepared by
Security/Graham-Leach-Bliley Act Core Team
University of Wisconsin Milwaukee
Information Security Program

INTRODUCTION
Numerous pieces of legislation have been passed in recent years in response to the increasing
digitization of information. The Gramm-Leach-Bliley Act (GLBA), the Health Insurance
Portability & Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act
(FERPA) are among those laws which attempt to protect consumer privacy by requiring
institutions to adopt certain commonsense safeguards. Moreover, as network-based information
storage becomes more common, certain concerns regarding data-safekeeping practices become
more acute. This document was developed in response to these legislative requirements and
practical challenges.

The University of Wisconsin – Milwaukee has a decentralized structure in terms of IT support
and data handling. While this provides the flexibility to meet the needs of diverse educational
missions and research goals, it also presents the University with unique security challenges,
many of which can only be satisfied through centralized coordination and the collaboration of a
broad campus constituency. This document, which was formulated through such collaboration,
attempts to achieve that coordination. It describes administrative, operational, and technical
security safeguards that must be implemented across all systems on campus.

This plan is intended to provide the campus with tangible, practical information as to the
maintenance of electronic data as well as outline the University’s broad, long-term strategic
goals regarding information security.

DESIGNATION OF REPRESENTATIVES
The Institution’s Chief Information Officer (CIO) is designated as the Program Officer
responsible for coordinating and overseeing the Program. The Program Officer is responsible for
the strategic leadership of information technology planning and is ultimately responsible for all
central IT functions of the Institution, which include: ensuring that all security incidents are
investigated, documented, remediated and reported to the appropriate parties. Any questions
regarding the implementation of the Program or the interpretation of this document should be
directed to the Program Officer or his or her designees.

The Information Security Officer (ISO) is the focal person for implementing the Institution’s IT
Security Program. The ISO reports directly to the CIO regarding IT security issues.

The Institution’s Chief of Police coordinates the engagement of law enforcement in information
security compliance and is a partner in ensuring both information and physical security.

College and Divisional Leaders coordinate their efforts with the ISO and others as necessary to
ensure reasonable compliance with legislation and policy.

University Legal Counsel provides legal guidance as necessary to help ensure that the Program’s
compliance plans and activities meet legislative requirements.
The Information Systems Auditor provides assessment services for departments and divisions to gauge compliance with legislation and best practices in an independent, non-biased and uniform manner.

The Institution’s Archivist advises departmental and other administrative officers on the control and disposition of records as defined by state law.

**SCOPE OF PROGRAM**

It is the responsibility of all University of Wisconsin Milwaukee employees to ensure the security and confidentiality of university records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any individual.

**ELEMENTS OF THE PROGRAM**

I. Risk Identification and Assessment

The University of Wisconsin Milwaukee intends, as a part of this Program, to identify and assess external and internal risks to the security, confidentiality, and integrity of university records and information as well as to prevent risks by the use and implementation of the following.

A. Employee Training and Management:

*Awareness Initiatives*

Even with proper technical controls governing access, segregation of duties, and security over application and database environments, data and information are still vulnerable to compromise at UWM. Lack of security awareness among UWM employees and students could allow for the compromise of information, data integrity and information assets. These are serious issues with potential financial and legal implications. To effectively mitigate this risk, UWM has established an Information Security Awareness Committee that is responsible for an awareness campaign and program.

The primary objective of UWM’s Information Security Awareness Committee is to change behavior among employees and students. It creates sensitivity to treats and vulnerabilities of information systems. It encourages habits that will turn employees and students into a “human firewall.” The campaign is on-going, motivational, lighthearted and non-technical with the objective of focusing attention so that learning will be incorporated into conscious decision making. Please see [http://security.uwm.edu](http://security.uwm.edu) for more information related to activities that have taken place to date.

*Resource Guide for Conducting Interviews and Checking References (See [http://oser.state.wi.us/docview.asp?docid=1816](http://oser.state.wi.us/docview.asp?docid=1816)).* The State of Wisconsin Office of State Employment Relations has developed a resource guide to be used for all State employees. This guide describes the importance of the interview and the planning of its process. It provides information about how to properly select an interview panel; schedule and conduct the interview; and evaluate the interview results. How to properly check references is also included as well as a list of common mistakes to avoid when evaluating candidates. Successfully selecting a candidate is crucial to ensuring the most qualified and responsible hire. It is at the hiring process juncture that the expectations of the University must be communicated - that being protecting the security and confidentiality of customer records and information.
Criminal Background Checks
To ensure that UWM accomplishes its mission and complies with Wisconsin Fair Employment Act (s. 111.3.1 et seq., Wis. Stats.), the Public Employee Safety and Health requirements under s. 101.11 Wis. Stats., the Drug-Free Workplace Act (41 U.S.C. Sec. 701 et. seq.) and UWM's Drug-Free Workplace Policy, and other state, federal and constitutional requirements for the protection of applicants, employees, students and all other University and community stakeholders, records of pending criminal charges and convictions may be considered in employment decisions when the circumstances of the pending charge or conviction are substantially related to the job. Please note that certain divisions or units have made this required based on business needs and/or State requirements.

This practice should be considered for the following new hires and permissive reinstatements in at UWM:

- Classified appointments.
- Non-teaching academic staff positions.
- Limited Term Appointments.
- Student employees hired in certain sensitive units. Contracted hourly workers in those same units.

For recruitments, where it is the intent to conduct a criminal records review, advertisements and position vacancy announcements must include a statement:

Sample language: "Please note: This position requires a criminal records review consistent with the Wisconsin Fair Employment Act."

For recruitments involving faculty and teaching academic staff, UWM will observe principles of the American Association of University Professors Statement of Professional Ethics (University of Wisconsin Milwaukee Faculty Document No. 2229, February 17, 2000).

Current UWM employees will not be subject to a criminal records review under this policy, unless the Chancellor or designee determines otherwise.

Position Description Language
Position descriptions for all employees of the University must clarify the responsibility of protecting the security and confidentiality of customer records and information. Therefore, each position description must include the following:

It is my responsibility, as a University of Wisconsin Milwaukee employee, to ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

Employee Confidentiality Agreement (Attachment A)
Given the utmost importance of maintaining and ensuring security and confidentiality of customer records and information, each University of Wisconsin Milwaukee employee must be provided with and required to sign an Employee Confidentiality Agreement. This agreement outlines what confidential information is; references the federal statutory language that regulates
or protects records and data; describes the expectations and responsibilities related to protecting information and data; and provides an understanding of the consequences for not complying with the requirement.

**Employee Training Recommendations**

It is necessary that new and existing employees be trained in the area of maintaining confidentiality and ensuring the security of records and data. The University provides information and training electronically through Legal Affairs and the Department of Enrollment Services for University employees. Access to this information can be found by logging on to the University’s web site at [www.uwm.edu](http://www.uwm.edu). Family Educational Rights & Privacy Act of 1974 (FERPA) information, as well as a FERPA Tutorial, is provided by the Department of Enrollment Services. Information can be accessed by logging on to [www.uwm.edu/Dept/DES/quicklinks/ferpa.html](http://www.uwm.edu/Dept/DES/quicklinks/ferpa.html). Additional training is available through university Professional Development Opportunities that focus on various aspect of maintaining security e.g. “Information Security Basics and Identity Theft/Fraud Prevention” provided by Information & Media Technologies’ IT Information Security Officer (ISO).

**Employee Codes of Conduct**

- IT Professional Conduct Guidelines. Found at [www.sage.org/ethics.mm](http://www.sage.org/ethics.mm)
- Other departmental, unit, or professional organization specific code of ethics may apply.

**B. Information Systems and Information Processing:**

The Program Officer coordinates with the Information Security Auditor, representatives of Information & Media Technologies and representatives of the IT staff employed by other Institutional units to assess the risks to nonpublic, personal information associated with the Institution’s information systems including: network and software design, information processing, and the storage, transmission and disposal of nonpublic information. This ongoing evaluation is based upon school/college/division self-assessments of their compliance of the requirements of applicable legislation, including the GLB Act, FERPA, and HIPAA. Previous evaluations included a survey of departmental procedures concerning personally identifiable financial information (PIFI), an outside audit of the Institution’s student information systems and an internal audit of LAN security practices in Business and Financial Services. Since November 2004, surplus computers and computer-related devices are collected and processed for disposal through a contract with an outside vendor who ensures that the disposal is handled in an environmentally responsible manner and that any data are securely removed from electronic media.

**C. Records Retention and Disposal:**

University specific requirements and policies found at [www.uwm.edu/Libraries/arch/records.htm](http://www.uwm.edu/Libraries/arch/records.htm) and [www.uwsa.edu/fadmin/acctrda.htm](http://www.uwsa.edu/fadmin/acctrda.htm).
D. Detecting, Preventing and Responding to Attacks:
The Program Officer coordinates with the Information Security Officer and the Information Systems Auditor to develop and evaluate procedures for and methods of detecting, preventing and responding to attacks and other system failures. They are also responsible for reviewing and recommending changes to existing network access policies and procedures, as well as developing procedures for coordinating responses to network attacks and overseeing the activities of the Computer Security Incident Response Team (CSIRT). In this regard, the Program Officer may elect to delegate to the Information Security Officer and/or the Information Systems Auditor the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.

The Program Officer, Information Security Officer and members of the Computer Security Incident Response Team (CSIRT) will develop and evaluate procedures for, and methods of, detecting and responding to attacks and other system failures.

II. Contingency Planning
UWM depends on certain functions such as building operations, financial transactions, communications and information systems applications and infrastructure; if they are not operational, the University cannot conduct its business. Accordingly, UWM will develop comprehensive contingency plans to support mission critical functions.

UWM has already implemented an Emergency Operations Plan developed by the Department of Environmental Health Safety and Risk Management. See <http://www.uwm.edu/Dept/EHSRM/EMERGENCY/EOP.html>. This plan is designed to provide quick and professional support when an emergency situation is confronted.

The responsibility for continuity of a function at UWM, in the absence of a critical resource, rests with the user of the resource. Responsibility for the recovery of the resource rests with the provider. As a result, providers and users of mission critical functions at UWM are expected to have a Mission Resumption Plan. This plan will identify high likelihood and high impact risks so that specific actions steps can be developed to ensure readiness, response, recovery and restoration. All plans will be periodically tested, reviewed and updated. A template for departments to draft a mission resumption plan is available (Attachment B).

III. Designing and Implementing Safeguards
The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Information Security Officer and Information Systems Auditor will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

IV. Overseeing Service Providers
It is the responsibility of the University of Wisconsin Milwaukee Purchasing Office to oversee service providers by contractually obligating them to implement and maintain appropriate safeguards that adhere to the Gramm-Leach Bliley Act. To comply with GLBA, the State of Wisconsin Purchase Order Standard Terms and Conditions had language added for service
providers to comply with GLBA. Effective July 1, 2004, this language appears on the back of every purchase order sent out by the university.

**State of Wisconsin Purchase Order Language:**

“**RELEASE OF INFORMATION:** Contractor shall not report or release information concerning UWM or its students, employees or customers to third parties without UWM’s prior written approval. Any such report or release of information shall, at a minimum, comply with those requirements enumerated in the Gramm-Leach Bliley Act, 15 USC 6801 et seq., UWM’s standards for safeguarding such information, and all other applicable laws regarding consumer privacy.”

**V. Adjustments to Program**
The Information Security Officer and Information Systems Auditor is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the university’s operations or other circumstances that may have a material impact on the Program.
Attachment A

UNIVERSITY OF WISCONSIN - MILWAUKEE
Department of __________________
Employee Confidentiality Agreement

In consideration of my employment and/or continued employment at the University of Wisconsin-Milwaukee (UWM), Department of Financial Aid, I agree as follows:

1. For purposes of this Agreement, "confidential information" is defined as information that is (a) information disclosed to me or known by me as a consequence of my employment, and not generally known outside UWM or the Department; or (b) protected by State or Federal laws.

   Confidential information may include records or data protected by laws such as the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act, and the following Wisconsin Statutes: Section 19.21-19.39 (public records laws) and Section 19.81-19.98 (open meetings laws).

2. During my employment and after the termination of my employment, I will hold the confidential information of UWM and the Department in trust and confidence. I will safeguard confidential records, and will not use or disclose it or any embodiment thereof, directly or indirectly, except as may be necessary in the performance of my duties for UWM and the Department. I understand that any unauthorized disclosure could be highly damaging to UWM, its employees, students, donors, or others.

3. I will not remove materials containing confidential information from UWM or the Department unless authorized to do so by my supervisor. Any and all such materials are the property of UWM and/or the Department. Upon termination of any assignment or as requested by my supervisor, I will return all such materials and copies thereof to the Department.

4. I understand that I should contact my supervisor if I am asked to disclose confidential information or if I have questions relating to what constitutes a confidential record.

5. I understand that if I violate this Agreement, I may be subject to disciplinary action, including termination or legal action, or both.

IN WITNESS WHEREOF, and intending to be legally bound, I have hereunto set my hand on this ____ day of ________________, 20____.

EMPLOYEE: ________________________

SUPERVISOR: ______________________

________________________
________________________
The responsibility for continuity of a function at UWM, in the absence of a critical resource, rests with the user of the resource. Responsibility for the recovery of the resource rests with the provider.

1. **Date**
   January 2004

2. **School, College or Division**
   Administrative Affairs

3. **Department**
   Environmental Health, Safety and Risk Management

4. **Program or sub-unit**
   Animal Resource Center

5. **Functions of program or sub-unit and related tasks**

   A. Provide for the care, health and well being of animals used for research and education at UWM.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Schedule, Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   B. Administer to animal related needs of UWM researchers and educators through dissemination of knowledge and resources.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Schedule, Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   C. Serve the public by ensuring observance of all legal and ethical standards pertaining to the use of animals for research and education at UWM.
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Schedule, Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. High likelihood risks

A. Water outage
B. Steam (heat outage)
C. Mechanical failure

7. High impact risks

A. Long-term power outage
B. Fire
C. Vandalism (release animals, kill animals, sabotage research)
D. Terrorism
E. Epidemic
F. Tornado

8. Space

<table>
<thead>
<tr>
<th>Building</th>
<th>Lapham</th>
<th>Room #</th>
<th>Purpose</th>
<th>Animal</th>
<th>Cage wash</th>
<th>Procedures (labs)</th>
<th>Necropsy</th>
<th>Storage</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sq. footage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Lighting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Voice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Temperature</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Humidity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Electricity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HVAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Wiring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Generator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Water</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Floor drain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sinks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Plumbing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Steam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sewer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Garbage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Waste</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Acoustics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9. **Equipment**

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
<th>Use</th>
<th>Size</th>
<th>Model</th>
<th>Serial #</th>
<th>Supplier</th>
<th>Alternate supplier</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cage washers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cages</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Racks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Water bottles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Food dishes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Walk-in cooler</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Refrigerators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surgical and medical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pads</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lamps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specialized positioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specialized restraining</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10. **Inventory and supplies**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Average quantity on hand</th>
<th>Vendor</th>
<th>Alternate vendor</th>
<th>Unit cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rats</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rabbits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pigeons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Food</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bedding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cleaning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
11. Stakeholders

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>E-mail</th>
<th>V-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Researcher</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Instructor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Student</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12. Data files

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Medium</th>
<th>Software</th>
<th>Storage</th>
<th>Off-site storage location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LAMBS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Word</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Excel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FileMaker Pro</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13. Personnel

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Responsibilities</th>
<th>Keys/security</th>
<th>UWM phone</th>
<th>UWM pager</th>
<th>UWM cell phone</th>
<th>Home phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
14. Develop a plan to ensure “readiness” in the event that the relatively high probability risks cause disruption to key functions and tasks. Important elements of “readiness” are:

A. Negotiate formal contract with MCW, VA or MU to provide back-up facilities
B. Prevention
C. Avoidance
D. Reducing the probability of risk

15. Develop a plan to ensure “response” in the event of disruption. Important elements of “response” include:

A. Update current Animal Resource Center “Disaster Plan”
B. Draft plan to evacuate animals
C. Draft plan for euthanasia
D. Personnel evaluation
E. Safety
F. Damage Assessment
G. Security
H. Notifications

16. Develop a plan to address initial “recovery” in the event of disruption. This includes:

A. Alternate work sites
B. Workarounds
C. Personnel requirements
D. Training requirements
E. Identifying necessary resources and applicable costs

17. Develop a plan for “restoration” to return to business as usual. This includes:

A. Salvage operations
B. Facilities reconstruction
C. Resumption of all essential support functions
D. Systems and technology
E. Identifying necessary resources and applicable costs

18. All plans must periodically be:

A. Tested
B. Reviewed
C. Updated
D. Assigned an estimated cost

REFERENCES
FERPA (Family Educational Rights and Privacy Act)
- Overview http://www.uwsa.edu/gc-off/deskbook/ferpa.htm
- UWM FERPA Tutorial http://www.uwm.edu/Dept/DES/ferpa/

HIPAA (Health Information Portability and Accountability Act)
- Department of Health and Human Services HIPAA Compliance Materials http://www.hhs.gov/ocr/hipaa/

Gramm-Leach-Bliley (Financial Services Modernization Act of 1999)
- Gramm-Leach-Bliley Privacy Regulations http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=b69486e1722de82d13a476cb6808389a&rgn=div5&view=text&node=16:1.0.1.3.38&idno=16
- Gramm-Leach-Bliley Safeguarding Regulations http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=b69486e1722de82d13a476cb6808389a&tpl=/ecfrbrowse/Title16/16cfr314_main_02.tpl

DMCA (Digital Millennium Copyright Act)
- DMCA Statute http://assembler.law.cornell.edu/uscode/html/uscode17/usc_sec_17_00001201----000.html

USA PATRIOT Act
- Department of Justice USA PATRIOT Act Homepage http://www.lifeandliberty.gov/
Members of the **Security/Graham-Leach-Bliley Act Core Team** include:

- Steve Brukbacher, Information Systems Technology Services Specialist
- Suzanne Carter, University Legal Counsel
- Jane Hojan-Clark, Financial Aid Department Director
- Paul Rediske, Internal Audit Director
Michelle Schartner, Financial Management Supervisor (formerly)
David Stack, Computer Services Director