

Mississippi University for Women

Confidentiality and Security Agreement

Effective Date 12/01/2013

Mississippi University for Women regards security and confidentiality of data and information to be of utmost importance. Each individual granted access to electronic and/or hard copy data holds a position of trust and must preserve the security and confidentiality of the information to which they are granted access. Therefore, it is the intent of this policy to ensure that University data, in any format, is not divulged outside of Mississippi University for Women without explicit approval to do so by the cabinet member who has responsibility for the data in question. As such, the University requires all users of data to follow the procedures outlined below:

Policy on Confidential Information

Users of University data are required to abide by all applicable Federal and State guidelines and University policies regarding confidentiality of data, including, but not limited to the Family Education Rights and Privacy Act (FERPA); Gramm Leach Bliley (GLB); and The Health Insurance Portability and Accountability Act of 1996 (HIPAA). All users of University data and information must read and understand how the FERPA, GLB and HIPAA policies apply to the confidential information they are accessing. All users with access to Banner or other university computer systems acknowledge that they have read and agree to abide by the University's Appropriate Use of Electronic Communication and Information Network Resources found at: <http://www.muw.edu/images/admin/policy/PS3302.pdf>.

Confidential Information shall be defined as:

- regarding student, faculty or staff: any personally-identifiable records, financial records (including social security and credit card numbers), health records; contracts, research data; alumni and donor records; personnel records other than an individual's own personnel record;
- regarding the University: University financial data; computer and system passwords, University issued PINS, University proprietary information/data; and
- any other information for which access, use, or disclosure is not authorized by: 1) federal, state, or local law; or 2) University policy.

The individual receiving the Confidential Information shall have no obligation under this Policy with respect to Confidential Information which:

- is or becomes publicly available without breach of this Policy by the recipient;
- is rightfully received by the recipient without obligations of confidentiality; or
- is disclosed in accordance with any "whistle blower" action as provided in the U.S. False Claims Act or similar legislation (MUW Whistleblower Policy may be found at <http://www.muw.edu/images/admin/policy/PS6708.pdf>.)

Any individual with authorized access to the Confidential Information is given access solely for the business of the University and must not divulge the Confidential Information outside of the University except for University business requirements approved by the President of the University or cabinet

member responsible for the data in question. Specifically, with respect to Confidential Information, individuals must:

1. Access Confidential Information solely in order to perform their job responsibilities.
2. Not seek personal benefit or permit others to benefit personally from any Confidential Information that has come to them throughout their work assignments.
3. Not make or permit unauthorized use of any Confidential Information in the University's information system or other records.
4. Not enter, change, delete or add data to any information system or files outside of the scope of their job responsibilities.
5. Not include or cause to be included in any record or report, a false, inaccurate or misleading entry known to the user as such.
6. Not alter or delete or cause to be altered or deleted from any records, report or information system, a true and correct entry.
7. Not release Confidential Information other than what is required in completion of job responsibilities which is consistent with this Policy.
8. Not exhibit or divulge the contents of any record, file or information system to any person unless it is necessary for the completion of their job responsibilities.

It is the individual's responsibility to immediately report, as outlined under "Information Security Breach and Violation Reporting" at the end of this Policy, if the individual has violated this Policy. Additionally, given the potential harm that the University may suffer with the release of any Confidential Information, all employees are strongly encouraged to report any suspected violation of this policy or any other action, which violates confidentiality of data, as outlined at the end of this policy.

Security Measures and Procedures

All users of University information systems, including Banner, Degree Works, Slate, Canvas, and MUW email accounts, are supplied with an individual user account to access the data or systems necessary for the completion of their job responsibilities. Users of the University information systems are required to follow the procedures outlined below:

1. All transactions, processed by a user ID and password, or PIN, are the responsibility of the person to whom the user ID was assigned. The user's ID, password, and PIN must remain confidential and must not be shared with anyone.
 - Using someone else's user ID, password or PIN is a violation of policy, no matter how it was obtained.
 - Your user ID, password or PIN provides access to information that has been granted specifically to you. To reduce the risk of shared passwords – remember not to post your password or PIN on or near your workstation or share your password or PIN with anyone.
 - It is your responsibility to change your password immediately if you believe someone else has obtained it.

Note: If you need your Password or PIN changed, please contact Information Technology Services (ITS) immediately. 662-329-7282.

2. Access to any student or employee information (in any format) is to be determined based on specific job requirements. The appropriate data owner (Department Chair, Department Director/Manager, Dean, Provost, and/or Vice President/Cabinet Member) is responsible for ensuring that access is granted only to authorized individuals, based on their job responsibilities. Written authorization must be received by ITS prior to granting system access.

You are prohibited from viewing or accessing additional information (in any format) unless you have been authorized to do so. Any access obtained without written authorization is considered unauthorized access.

In order to prevent unauthorized use, the user shall log off of all applications that provide access to confidential information, or lock their computer when leaving their workstation. This is especially important during breaks and lunch. Unless there is a specific business need, all workstations should be shut down at the end of the workday.

Note: If you require assistance in establishing your workstation password, please contact ITS at 662-329-7282.

3. If you have any reason to believe your password or PIN has been compromised or revealed inadvertently, you should change your password and immediately notify one of the individuals as outlined under "Information Security Breach and Violation Reporting" at the end of this policy.
4. Upon termination of an employee, Human Resources will notify ITS, who in turn will notify the appropriate areas.
5. Generally, students, temporary employees and consultants should not have access to the University record system. Written approval by the Department Chair, Department Director/Manager, Dean, Provost, and/or Vice President/Cabinet Member in charge of the respective area is required if it is determined that access is required. The student, temporary employee or consultant is to be held to the same standards as all University employees, and must be made aware of their responsibilities to protect student and employee privacy rights and data integrity. Written authorization must be received by the ITS prior to granting system access.
6. You agree to properly secure and dispose of any outputs or files you create in a manner that fully protects the Confidential Information.

Information Security Breach and/or Policy Violation Reporting

If you suspect an Information Security Data Breach or a violation of this policy, report such an event to your department chair or staff supervisor and send an immediate email to securityadmin@muw.edu. If you do not have immediate access to email, contact ITS at 662.329.7282 and indicate that the call is in reference to an information security data breach or policy violation.

Employee Agreement

I have read, understand and acknowledge receipt of this Mississippi University for Women Confidentiality Agreement and Security Policy. Additionally, I understand that if granted access to process transactions via Banner data entry screens, any information I enter or change will be effective immediately. Accordingly, I understand that I am responsible for any changes made using my ID.

I understand that my access to University data is for the sole purpose of carrying out my job responsibilities and Confidential Information is not to be divulged outside of The University, except as previously stated. Breach of confidentiality, including aiding, abetting, or acting in conspiracy with any other person to violate any part of this policy, may result in sanctions, civil or criminal prosecution and penalties, employment and/or University disciplinary action, and could lead to dismissal, suspension or revocation of all access privileges. I understand that misuse of University data and any violation of this policy or the FERPA, HIPAA or GLB policies are grounds for disciplinary action, up to and including dismissal. This Agreement shall not abridge nor supersede any rights afforded faculty members under the Faculty Handbook.

Individual's Name (Please Print): _____

Department (Please Print): _____

Signature: _____ Date: _____

Recordkeeping Requirements

- Supervisors should **maintain the original in departmental files** and readily available upon request during an audit.
- Do not forward this form to Human Resources or ITS.
- ALL employees and student workers are required to read and sign this agreement.
- Agreement must be retained for length of employment and for three years after employment with the department and/or university ends.
- Agreement is not transferable between departments and a new agreement is required in the event an employee and/or student worker transfers to another department.
- For student workers with multiple jobs, each department is required to have a signed form on file.