WAYNE STATE UNIVERSITY

07-02 Confidential Information Policy

1.0 Purpose

1.1 This policy provides Wayne State University with a framework for dealing with the challenge of maintaining private and confidential data. The risks of identity theft, unauthorized data modifications and financial manipulations are associated with access to confidential electronic and paper-based information the university collects in the course of its operations. Because universities are dispersed organizations with a commitment to the free exchange of information, every person at the university who is entrusted with confidential data has an obligation to keep those data safe from theft or unauthorized access.

2.0 Definition of Confidential Information

2.1 Data held by the University that could harm the person to whom it refers/belongs if seen or acquired by a person not authorized by university policy, procedure or applicable external regulations.

2.2 Data that are protected by federal or state legislation dealing with data privacy. (See appendix for current examples).

2.3 Examples of such confidential information include but are not limited to: social security numbers, credit card numbers, bank account information, student records other than university-designated directory information, protected health information, Access ID/ password combinations that permit access to restricted university electronic resources, personal information that is collected for research purposes pursuant to the terms of an IRB-approved research protocol or that is collected with a promise obligation to keep it private, or data which is proprietary or classified.

2.4 Data that are legally excluded from release under the Freedom of Information Act.

3.0 Definition of User

3.1 A user is any Wayne State University officer, employee, or student who has access to confidential data, and any non-employee given such access on a contractual or business basis. Access to confidential data will be limited to people whose job duties, as defined by University policies and procedures, require such access.

4.0 Storage of Confidential Information

4.1 Physical records, such as paper documents, should be kept in secure/locked storage if the location is unattended or if there is a significant potential for unauthorized acquisition. Confidential information should not be stored in locations such as filing cabinets located in hallways.

4.2 Electronic devices, including both desktop computers and portable devices, that store confidential information should be password-protected.

4.3 Portable electronic equipment such as laptops and other devices that are easily misplaced or stolen, such as smartphones, removable flash drives or other high capacity portable units must be stored so as to prevent unauthorized acquisition or else must be purged of confidential data.

4.4 When feasible, the storage media and/or the files themselves should be password-protected and/or encrypted.

5.0 Transmission of Confidential Information

5.1 Physical records such as paper documents should be transmitted in a secure manner, such as sealed envelopes, and should be transported by authorized couriers.

5.2 Electronic documents and other digitally-maintained data should be encrypted if sent in a digital format.

6.0 Disposal of Confidential Information

6.1 Physical records such as paper documents should be shredded when no longer needed or required to be maintained.

6.2 Electronic documents and other digitally-maintained data should be permanently deleted when no longer needed.

6.3 Digital storage media should be degaussed and/or destroyed when no longer needed.

7.0 User Responsibilities and Obligations

7.1 Users should ensure that machines in their care (desktop computers, laptops, other devices) are operated and maintained in a secure manner, using recognized best security practices, with up-to-date operating systems, anti-virus software, anti-spyware software and firewalls as appropriate and feasible. Users should seek technical assistance if necessary to ensure compliance.

7.2 User must immediately report any discovery that confidential information has fallen into unauthorized hands or a machine or storage device has been hacked, lost, stolen or misplaced.

8.0 Disciplinary Actions

8.1 Violation of this policy may lead to appropriate action as provided for by the disciplinary processes relevant to that individual. Nothing in this policy shall be construed to modify the terms of any collective bargaining agreement.

8.2 Faculty, staff and students are responsible both to civil authorities and to the University for acts that constitute violations of both law and this policy. Administrative remedies taken under this policy will not be subject to challenge on the grounds that civil or criminal charges involving the same incident have been invoked, dismissed, or are pending.

9.0 Duration and Effective Date

9.1 This University Policy is revocable by the President at any time and without notice.

9.2 This university policy is effective upon issuance.

Signed by President Irvin D. Reid November 30, 2007.