TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

Data Confidentiality Policy

Purpose

The purpose of this policy is to outline essential roles and responsibilities within the University community for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interests

Users. Users include virtually all members of the Tuskegee University community to the extent they have authorized access to University Information Reso

planning information, legally privileged information, invention disclosures and other information concerning pending patent applications.

Without limiting the generality of the foregoing, Confidential information shall include "personal information" such as, first name or first initial and last name in combination with any one or more of the following: (a) social security number; (b) driver's license number or state–issued identification number; (c) financial account number, or credit card or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to the resident's financial account and Confidential information also includes "customer information," defined by the safeguards rule under the Gramm-Leach-Bliley Act to mean any information containing personally identifiable information that the University obtains in the process of offering a financial product or service.

Internal Use Only information includes information that is less sensitive than Confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of Tuskegee University. Examples of this type of data from an institutional perspective include internal memos meant for limited circulation, or draft documents subject to internal comment prior to public release.

Public information is information that is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on individual members of the University community or upon the finances, operations, or reputation of Tuskegee University.

2. All Information Resources, whether physical documents, electronic databases, or other collections of information, are to be assigned to a security classification level according to the most sensitive content contained therein.

3. Where practicable, all data is to be *explicitly classified*, such that Users of any particular data derived from an Information Resource are aware of its classification.

4. In the event information is not explicitly classified, it is to be treated as follows: Any data which includes any personal information concerning a member of the University community (including any health information, financial information, academic evaluations, social security numbers or other personal identification information) shall be treated as Confidential. Other information is to be treated as Internal Use Only, unless such information appears in form accessible to the public (i.e., on a public website or a widely distributed publication) or is created for a public purpose.

5. The Data Security Committee may from time to time provide clarifications relating to the security classifications, and may, through issuance of Data Security Directives establish more detailed requirements concerning the classification of Information Resources or specific data.

ROLE OF THE DATA SECURIT

Users must log off from all applications, computers and networks, and physically secure printed material, when not in use.

To the extent possible, making sure that any Tuskegee Personal Information accessed by the User is stored only on secure servers maintained by the University and not on local machines, unsecure servers, or portable devices.

Tuskegee University Confidential or Internal Use Only data, when removed from the campus or when accessed from off-campus, is subject to the same rules as would apply were the data on campus. Sponsors and Users will comply with (c)Tjo a1.69 0 Td (a)Tj -0.002 Tw 0.

Immediately upon becoming aware of a likely Security Breach, the Security Officer shall notify the Office of the General Counsel and the Chief Information Officer. An immediate investigation will ensue. The General Counsel shall determine what, if any, actions the University is required to take to comply with applicable law, including whether any notification is required under Alabama law. The General Counsel shall work with other administrators as appropriate to ensure that any notifications and other legally required responses are made in a timely manner. If the event involves a criminal matter, the Tuskegee Police Department shall be notified and shall coordinate its response with the Office of the General Counsel.

The Security Officer shall investigate and review the incident and provide a formal report that will be distributed to the Data Security Committee and appropriate department members immediately after the investigation is finalized.

Quarterly, the Data Security Officer will present a summary of data security investigations and/or relevant data security updates to the Data Security Committee, who shall conduct a post-incident review of events and determine, what, if any changes should be made to University practices or policies to help prevent similar incidents. The Committee shall document the University's actions in response to a Security Breach and its post-incident review in the minutes of the meeting in which the breach is discussed.