APPENDIX C: The University of Texas System Administration Identity Theft Prevention, Detection and Mitigation Program – Approved by the Chancellor on 10.29.09

OVERVIEW

This document constitutes The University of Texas System Administration’s written Identity Theft Prevention, Detection & Mitigation Program (Program) adopted in accordance with INT 162, Identity Theft Prevention, Detection & Mitigation Policy and 16 CFR 681.1, the “Red Flags Rule” issued by the Federal trade Commission pursuant to Section 114 and 315 of the Fair Credit Reporting Act (FACTA) which amended the Fair Credit Reporting Act (FCRA) (Red Flags Rule).

The University of Texas System Administration (System Administration) consists of a variety of offices, some of which are responsible for the central management and coordination of the academic and health institutions; some of which provide centralized services on behalf of The University of Texas System (System) institutions and some of which serve as consultants to System institutions.

System Administration has determined that the following System Administration departments or offices currently house departments that hold Covered Accounts, as defined by INT 162 that require compliance with the Red Flag Rules:

- Accounting and Purchasing Services within Operations and Support Services;
- The Claims and Financial Litigation Section within the Office of General Counsel;
- The Office of Employee Benefits.

Because of the diversity of the missions and services provided by these respective offices and departments, System Administration has determined that each of these offices and departments require customized programs. Accordingly, the Program shall consist of three separate sub-programs.

All three sub-programs shall be overseen by the Vice Chancellor for Administration and will be subject to the same general requirements described in INT 162. As required, System Administration will conduct periodic reviews for Covered Accounts. If additional offices or departments housing Covered Accounts are identified, additional sub-programs may be developed or an existing sub-program may be expanded to include those Covered Accounts.

EFFECTIVE DATE

This program takes effect on November 1, 2009.

RESPONSIBLE PARTY

The Vice Chancellor for Administration is the Responsible Party for the Program. The duties of the Vice Chancellor under the Program include:
• Ensuring that each department or office within System Administration conducts a risk assessment no less than annually to determine whether the department or office has become responsible for a Covered Account;
• Revising the Program to cover all such newly identified Covered Accounts;
• Ensuring that all System Administration employees with responsibility under the Program receive initial and periodic training as necessary to ensure compliance with the Program;
• Reviewing and, as warranted by such reviews, updating the Program to reflect the risks associated with Identity Theft no less than annually;
• Making periodic reports, no less than annually, to the Chancellor to ensure compliance with the program. The first report shall be delivered no later than one year after the date upon which this Program takes effect, or November 1, 2010;
• Any other action required to implement and enforce this Program.

OFFICES AND DEPARTMENTS REQUIRED TO COMPLY; DESIGNATED OFFICE OR DEPARTMENT OFFICIAL

The following departments and/or office hold Covered Accounts that require compliance with the Red Flag Rules and the position within each office or department responsible for oversight are:

• Accounting and Purchasing Services within Operations and Support Services [Director of Accounting and Purchasing Services]
• The Claims and Financial Litigation Section within the Office of General Counsel [Claims and Financial Litigation Section Manager]
• The Office of Employee Benefits [Director of Employee Benefits]