April 6, 2005

NETWORK & INFORMATION SYSTEMS MEMORANDUM 05-03

TO: TTI Information System (TTI-IS) Data Owners

SUBJECT: Ownership of TTI’s Information Resources

As a follow-up to an audit point noted by the Texas A&M University System auditors, Network & Information Systems (NIS), as custodial of the agency’s central database (TTI-IS), is tasked with formally insuring that all data contained within the database has designated owners, custodians and users. All production systems and applications designed, implemented and maintained by NIS incorporate data ownership and access controls into the application design and require appropriate approval prior to granting access to any application. To help you understand the process, a few definitions are provided here for clarification:

Roles

**Owner:** The manager responsible for the business function which is supported by the information resource (information system, application, database, server etc.), the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls (see example below) that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

**Custodian:** Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications Information Services is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

Data Classification

**Sensitive:** This classification applies to information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness. Sensitive information might include organization financial transactions and regulatory actions.

**Confidential:** This classification applies to the most sensitive business information that is intended strictly for use within the organization. This information is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations. Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners, and/or its customers. For example, health care related information should be considered at least confidential.

**Private:** This classification applies to personal information that is intended for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees.

**Public:** This classification applies to all other information that does not clearly fit into any of the above three classifications. While its unauthorized disclosure is against policy, it is not expected to impact seriously or adversely the organization, its employees, and/or its customers.
Example

The Human Resources System (HRS), a module of TTI-IS, is used by TTI’s Human Resources department. The person table contains data used by the HRS, most fields in this table are classified as sensitive. The one exception is social security number, which is classified as confidential. As a result of this classification, the data custodian (NIS), blocks display and entry of this number, except as authorized by the owner of the HRS information, HR - Greg Richmond. In addition, the custodian also incorporates high-level data encryption techniques for this field in the database to prevent unauthorized access. The application level logic and data encryption techniques are considered controls.

As a data owner, you are also responsible for defining all information classification categories (see above definitions) except confidential information (Information that is exempt from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act) and establishing the appropriate controls for each. This is usually accomplished during the design phase of application development by insuring that application developers incorporate the appropriate controls and audit trails into the application.

To confirm your ownership responsibilities, the attached report has been prepared and contains information related to tables in the database where you are designated as the owner. The report contains a listing of tables in TTI-IS where you are designated as the owner. If a table contains a field that is classified as “sensitive” or “confidential”, all fields are listed for that table, otherwise, only the table name and ownership information is listed. The information on data ownership will be presented to the TTI Management Team this quarter. If there are changes to ownership or data classification, please notify me by April 15, 2005. You can find complete information from the Texas Administrative code as it relates to data ownership roles and responsibilities on the web at [Information Security Standards for Institutions of Higher Education](https://www.texas.gov/InformationSecurityStandardsforInstitutionsofHigherEducation).

Please take time to review the information contained in the attached report. If you have questions about any information contained in the report or if you’d like a detailed report of all fields contained in the tables you own, please let me know. Your assistance in this important effort is appreciated.

Kassandra Agee-Letton
Chief Information Officer

xc: Don Bugh, Executive Associate Director