# Change and Configuration Management

## Audit Report # 18-115
## February 14, 2019

The University of Texas at El Paso

**Office of Auditing and Consulting**

"Committed to Service, Independence and Quality"

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU

February 14, 2019

Dr. Diana Natalicio
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited-scope audit of Change and Configuration Management. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by Enterprise Computing staff and the Chief Information Security Officer during our audit.

Sincerely,

Lori Wertz
Chief Audit Executive

# Report Distribution:

**University of Texas at El Paso:**
Mr. Richard Adauto III, Executive Vice President
Dr. Stephen Riter, Vice President for Resources and Planning
Mr. Luis Hernandez, Assistant Vice President and Director, Enterprise Computing
Ms. Mary Solis, Director and Chief Compliance and Ethics Officer

**University of Texas System (UT System):**
System Audit Office

**External:**
Governor's Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor's Office
Sunset Advisory Commission

**Audit Committee Members:**
Mr. Fernando Ortega
Dr. Carol Parker
Mr. Benjamin Gonzalez
Dr. Gary Edens
Dr. Roberto Osegueda
Mr. Mark McGurk

**Auditors Assigned to the Audit:**
Victoria Morrison

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of change and configuration management for Banner Student Information System (Banner) and an overview of change management governance in the Enterprise Computing Department (EC).

We concluded that the Enterprise Computing Department has a formal written change management process that meet regulations, standards and guidelines for Banner.

During the change management governance review and discussion with the Assistant Vice President of Enterprise Computing and the Chief Information Security Officer, we noted the following:

- Management oversight and monitoring of changes: no exceptions were noted

- Change management for systems that interface with Banner: no exceptions were noted

- Departmental change management policies and procedures:
  EC identified The University of Texas at El Paso's mission critical systems in their *Business Continuity Plan*; however, Banner is the only one having formal change management documentation. As stated in UT System Policy 165 (UTS 165) *Information Resources Use and Security Policy,* formal written change management policies and procedures are required for all mission critical systems. We did identify that there are change management controls present for application development (e.g. application code, websites, in-house application development) and infrastructure changes (e.g. operating system, databases, hardware, mail system).

# BACKGROUND

Change management is an Information Technology standard operating practice. The Institute of Internal Auditors Global Technology Audit Guide 2: *Change and Patch Management Controls: Critical for Organization Success*" defines IT change management as:

> *"…the set of processes executed within the organization's IT department designed to manage the enhancements, updates, incremental fixes, and patches to production systems, which include:*
>
> - *Application code revisions.*
> - *System upgrades (e.g., applications, operating systems, and databases).*
> - *Infrastructure changes (e.g., servers, cabling, routers, and firewalls).*
>
> *Stable and managed IT production environments require that implementation of changes be predictable and repeatable, as well as follow a controlled process that is defined, monitored, and enforced. Segregation of duties (e.g., separation of preparer, tester, implementer, and approver roles) and monitoring controls will reduce the risk of fraud and errors in the process. "*

Change management controls reduce the risk of

- unavailability or disruptions of information systems,
- unauthorized and/or un-approved changes to systems and confidential data,
- changes not being recorded and tracked,
- emergency changes being implemented without adequate management oversight, and
- failure to comply with regulations, standards, and guidelines.

# AUDIT OBJECTIVES

The objectives were to perform an audit of the change management process (including change management governance) currently in place in the Enterprise Computing Department (EC) to provide management assurance that the Banner Student Information System (Banner) meets state regulations and UTEP standards and guidelines.

# SCOPE AND METHODOLOGY

The audit is conducted in accordance with the International *Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors (IIA).

The criteria for the audit included:

- Texas Department of Information Resources, *Security Control Standards Catalog Version 1.3*
- UT System Policy 165 (UTS 165) Information Resources Use and Security Policy
- UTEP Information Resources Use and Security Policy and Standards, *UTEP Standard 7: Change Management*
- UTEP Information Security Office Change Management Guidelines

Audit procedures included:

- interviewing and requesting information from key personnel,
- reviewing applicable laws, regulations, policies and procedures,
- verifying the existence of appropriate institutional policies and procedures

The scope included transactions, policies and procedures from July 1, 2017 to July 1, 2018.

# RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

**Priority** - an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

**High** – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

**Medium** – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

**Low** – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level

# AUDIT RESULTS

## A. Change Management for Banner Student Information System

Internal Audit performed an assessment of the Banner change management process. UTEP Banner change management has formal written policies and procedures for change management. These policies were updated as of February 2018. EC consistently communicates to users about Banner changes.

The following tables contain a summary of the results:

| **UTEP Standard 7 Change Management**<br>**7.1 Change Management Requirement** | **Results** |
|---|---|
| *(a) Ensure that approved change management procedures and processes are performed* | No exceptions noted |
| *(b) Emergency Changes are identified and deployed* | No exceptions noted |
| *(c) Impacts of changes are assessed* | No exceptions noted |
| *(d) Changes are approved and authorized* | No exceptions noted |
| *(e) Changes are tested* | No exceptions noted |
| *(f) Change implementation (back-out plan, communication, schedule) occurs and is effective* | No exceptions noted |
| *(g) Changes are documented and tracked* | No exceptions noted |

| **UTEP Standard 7 Change Management**<br>**7.4 A Change Management Log must be maintained for all significant changes, including emergency changes. The log must contain, as a minimum, the:** | **Results** |
|---|---|
| *(a) Date of the submission and date of the change* | No exceptions noted |
| *(b) Owner and custodian contact information* | No exceptions noted |
| *(c) System administrator contact information* | No exceptions noted |
| *(d) Nature of the change* | No exceptions noted |

## B. Change Management Governance

Change management governance was evaluated through discussions with the Assistant VP of the Enterprise Computing Department and the Chief Information Security Officer and a review of support documentation.

### Management Oversight and Monitoring of Changes

- Unauthorized changes are controlled through segregation of duties between software development, data management and system support sections. The Data Management team; specifically, the data base administrator implements changes into production. The procedure was verified by reviewing approvals on Help Desk service tickets.

- The Information Security Office monitors unauthorized changes to mission critical resources or systems. Evidence of active monitoring was provided.

### Change Management for Systems That Interface with Banner

Systems that interface with Banner are hosted solutions; consequently, change management procedures are managed by the vendors.

## B.1 Departmental Change Management Policies and Procedures

Change management policies and procedures protect data integrity, impact the availability of the production system and are required by UTS165 (See APPENDIX A CRITERIA).

- Change management standards and guidelines are located on the UTEP Information Security Office website.

- Enterprise Computing has formal written change management policies and procedures for Banner, but not for other mission critical systems in the Enterprise Computing Business Continuity Plan. However, identifiable change management controls are present for application development (e.g. application code, websites, in-house application development) and infrastructure changes (e.g. operating system, databases, hardware, mail system).

### Recommendation:

*Establish formal written departmental change management policies and procedures for all mission critical systems and systems that process confidential data and review periodically. Verify that change management policies and procedures meet the requirements for UTS165, and the UTEP Information Resources Use and Security Policy.*

**Level:** This finding is considered **MEDIUM** due to the fact that changes could be made to production systems without a formal change process affecting data integrity and availability of productions system(s)

### Management Response:

*There is currently a procedure for departmental change management for mission critical systems, however it has not been formally documented. This procedure is currently being reviewed, updated and will be formally documented.*

### Responsible Party:

*Gerard D. Cochrane Jr., Chief Information Security Officer and*
*Luis E. Hernandez, Assistant Vice President, Enterprise Computing*

### Implementation Date:

*March 31, 2019.*

# CONCLUSION

Based on the results of audit procedures performed, we conclude that Enterprise Computing IT operations will be enhanced by implementing the recommendations.

We wish to thank the management and staff of Enterprise Computing and Information Security Office for their assistance and cooperation provided throughout the audit.

# APPENDIX A: CRITERIA:

## STATE

Texas Administration Code Title 1, Part 10, Chapter 202, Subchapter C, RULE §202.76 Security Control Standards Catalog:

### *Texas Department of Information Resource Security Control Standards Catalog Version 1.3*

#### *CM-1 Configuration Management Policy and Procedures*

*"RISK STATEMENT*
*The change management process in place does not adequately protect the environment from disruptive changes in production.*
*CONTROL DESCRIPTION*
*The organization:*
*a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:*
*1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and*
*2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and*
*b. Reviews and updates the current:*
*1. Configuration management policy [Assignment: organization-defined frequency]; and*
*2. Configuration management procedures [Assignment: organization-defined frequency]*
*STATE:*
*The organization establishes the process for controlling modifications to hardware, software, firmware, and documentation to ensure the information resources are protected against improper modification before, during, and after system implementation.*
*EXAMPLE*
*The organization has written, documented configuration management policies and procedures in place."*

#### *CM-2 Baseline Configuration*

*"RISK STATEMENT*
*Changes to systems and applications are executed inconsistently in the production environment due to ill- defined procedures.*
*CONTROL DESCRIPTION*
*The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.*
*STATE*
*The state organization develops, documents, and maintains a current baseline configuration of the information system.*
*EXAMPLE*
*The organization uses configuration policies and procedures to manage the change lifecycle."*

#### *CM-3 Configuration Change Control*

*"RISK STATEMENT*
*Changes to the production environment that are inadequately tested disrupt production environment. Management does not accept changes to the operating environment prior to implementation into production.*
*CONTROL DESCRIPTION*
*The organization:*
*a. Determines the types of changes to the information system that are configuration-controlled;*

*b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;*
*c. Documents configuration change decisions associated with the information system;*
*d. Implements approved configuration-controlled changes to the information system;*
*e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];*
*f. Audits and reviews activities associated with configuration-controlled changes to the information system; and*
*g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].*

*STATE*
*No statewide control*
*EXAMPLE*
*Configuration changes are accepted prior to implementation. "*

### *CM-4 Security Impact Analysis*

*"RISK STATEMENT*

*Effects from changes to systems or applications are undetected in the production environment.*

*CONTROL DESCRIPTION*

*The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.*

*STATE*

*• All security-related information resources changes shall be approved by the information owner through a change control process.*

*• Approval shall occur prior to implementation by the state organization or independent contractors.*

*EXAMPLE*

*The organization considers and documents consideration of the potential impact to information security prior to the completion of a change. "*

### *CM-5 Access Restrictions for Change*

*"RISK STATEMENT*

*Operations handle emergency situations that require a change to the production environment consistently.*

*CONTROL DESCRIPTION*

*The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.*

*STATE*

*EXAMPLE*

*Access control restrictions for the purposes of change are defined. "*

### *CM-8 Information System Component Inventory*

*"RISK STATEMENT*

*Information and assets associated with information processing facilities are not owned by a designated part of the organization.*

*CONTROL DESCRIPTION*

*The organization:*

*a. Develops and documents an inventory of information system components that:*

*1. Accurately reflects the current information system;*

*2. Includes all components within the authorization boundary of the information system;*

*3. Is at the level of granularity deemed necessary for tracking and reporting; and*

*4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and*

*b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].*

*STATE*

*The state organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.*

*EXAMPLE(S)*

*The organization has an inventory of information system components and a process to keep the information current. "*

### *CM-9 Configuration Management Plan*

*"RISK STATEMENT*

*IT assets and configurations are managed ineffectively due to the lack of a configuration management process.*

*CONTROL DESCRIPTION*

*The organization develops, documents, and implements a configuration management plan for the information system that:*

*a. Addresses roles, responsibilities, and configuration management processes and procedures;*

*b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;*

*c. Defines the configuration items for the information system and places the configuration items under configuration management; and*

*d. Protects the configuration management plan from unauthorized disclosure and modification. "*

*STATE*

*EXAMPLE*

*Written, document configuration plan is available relevant to application systems. "*

### *PM-5 Information System Inventory*

*"RISK STATEMENT*

*Important assets have not been clearly identified and inventoried.*

*CONTROL DESCRIPTION*

*The organization develops and maintains an inventory of its information systems.*

*STATE*

*EXAMPLE*

*The organization conducts an automated or manual inventory of information systems bi-annually."*

### *SA-3 System Development Life Cycle*

...

*EXAMPLE*

*a. The existing system development lifecycle includes consideration for information security.*

*b. Test environments are kept either physically or logically separate from production environments.*

*c. Copies of production data are not used for testing unless the data has been authorized for public release or unless all custodians involved in testing are otherwise authorized access to the data. "*

### *SA-5 Information System Documentation*

*"RISK STATEMENT*

*Sensitive system configuration information is accessed by unauthorized parties due to inadequate security of system documentation.*

*CONTROL DESCRIPTION*

*The organization:*

*a. Obtains administrator documentation for the information system, system component, or information system service that describes:*

*1. Secure configuration, installation, and operation of the system, component, or service;*
*2. Effective use and maintenance of security functions/mechanisms; and*
*3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;*

*b. Obtains user documentation for the information system, system component, or information system service that describes:*

*1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;*
*2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and*
*3. User responsibilities in maintaining the security of the system, component, or service;*

*c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;*

*d. Protects documentation as required, in accordance with the risk management strategy; and*

*e. Distributes documentation to [Assignment: organization-defined personnel or roles].*

*STATE*

*The state organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.*

*EXAMPLE*

*The organization effectively secures system security documentation and configuration settings."*

### *SA-10 Developer Configuration Management*

*"RISK STATEMENT*

*Changes are made to production systems without a formal change process.*

*CONTROL DESCRIPTION*

*The organization requires the developer of the information system, system component, or information system service to:*

*a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation];*

*b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];*

*c. Implement only organization-approved changes to the system, component, or service;*

*d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and*

*e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].*

*STATE*

*All security-related information resources changes shall be approved by the information owner through a change control process. Approval shall occur prior to implementation by the state organization or independent contractors.*

*EXAMPLE*

*The organization should have documented change control procedures that:*

*a. require approval for making changes;*
*b. take into account impact on information security and related configurations;*
*c. perform appropriate level of testing of changes, including information security, as applicable;*
*d. track defects and security flaws; and*
*e. require approval from appropriate level of management"*

## UT SYSTEM INFORMATION RESOURCES USE AND SECURITY POLICY, SEC 5 INFORMATION SECURITY STANDARDS

### *UTS165 Standard 7: Change Management*

*"7.1 Change Management Requirement. All Institutions must adopt Change Management processes to ensure secure, reliable, and stable operations to which all offices that support Mission Critical Information Resources or Network Infrastructures are required to adhere. The Change Management process must incorporate Procedures for:*

*(a) formal identification, classification, prioritization, and request of Scheduled Changes;*

*(b) identification and deployment of Emergency Changes;*

*(c) assessment of potential impacts of changes, including the impact on Data classification, Risk assessment, and other security requirements;*

*(d) authorization of changes and exceptions;*

*(e) testing changes;*

*(f) change implementation and back-out planning; and*

*(g) documentation and tracking of changes.*

*7.2 Information Resources Custodians. All Custodians must implement and adhere to approved institutional Change Management processes to ensure secure, reliable, and stable operations."*

### *UTS165 Standard 21: System Development and Deployment*

...

*"(b) maintaining separate production and development environments to ensure the security and reliability of*

*the production system;"*

...

*for authorizing changes into production. "*

## UTEP INFORMATION RESOURCES USE AND SECURITY POLICY AND STANDARDS

### *UTEP Standard 7: Change Management*

*"The purpose of the Change Management Standard is to manage and document changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources. Please refer to The University of Texas at El Paso Change Management Guidelines for additional information and requirements, as warranted by The University of Texas at El Paso Data Classification Standard and commensurate with the risk and value of the system/data.*

*7.1 Change Management Requirement. All changes to UTEP Information Resource infrastructure such as, but not limited to, operating systems, computing hardware, networks, and applications must follow Change Management Procedures and adopt Change Management processes to ensure secure, reliable, and stable operations to which all offices that support Mission Critical Information Resources or Network Infrastructures are required to adhere.*

*(a) Colleges, schools, or units responsible for Information Resources will ensure that the change management procedures and processes they have approved are being performed;*

*(b) identification and deployment of Emergency Changes;*

*(c) assessment of potential impacts of changes, including the impact on Data classification, Risk assessment, and other security requirements;*

*(d) authorization of changes and exceptions;*

*(e) testing changes;*

*(f) change implementation and back-out planning; and*

*(g) documentation and tracking of changes.*

...

*7.3 Colleges, schools, or units may object to a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backup plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events. The responsible party will review all objections. A security exception request may be submitted to the CISO if there are objections to a planned change that is triggered by security requirements;*

*7.4 A Change Management Log must be maintained for all significant changes, including emergency changes. The log must contain, as a minimum, the:*

*(a) date of the submission and date of the change*

*(b) owner and custodian contact information;*

*(c) system administrator contact information;*

*(d) nature of the change*

*7.5 Information Resources Custodians. All Custodians must implement and adhere to approved UTEP Change Management processes to ensure secure, reliable, and stable operations."*

...

## *UTEP Standard 21: System Development and Deployment*

...

*"(b) Separate production and development or test environments will be maintained to ensure the security and reliability of the production system. Whenever possible, new development or modifications to a production system will be made first in a test environment. These changes should be thoroughly tested for valid functionality prior to being released into the production environment;"*

...

## *The University of Texas at El Paso Information Security Office Change Management Guidelines*

...

***"Scope***

*These guidelines should be applied in proportion to the respective data classification category, the availability requirements of the data, and the impact of the change on the user community. (See Data Classification Standard)*

...

***Obtain Approval to Move Forward with the Change***

*The Change Management Request Form (Full or Abbreviated) and the results of testing should be presented to the change committee.*

*The change committee should weigh the risks and benefits of making the change as well as the risks and benefits of not making the change.*

*The change committee may alter the plan or send it back for revision, if it determines that certain aspects of the change proposal are unacceptable or need more work.*

...

***Maintain a Record of the Change***

*Maintaining a record of the change management process may help determine the history of an information resource, as well as provide proof that the change was approved.*

*After the change has been implemented, record it in the change log. Sample change logs are provided below to help you decide how to document your changes.*

*Archive the change management documents that were completed during the process. This does not meant to imply that actual paper copies of the associated documents must be kept.*

...

***Full Change Management Request Form***

*A full change management request form provides detailed information about the change and is appropriate for changes affecting data classified as Category I (highest, most sensitive) where protection is required by law, the asset risk is high and is information which provides access to resources, physical or virtual. (See Data Classification Standard.) A record of when the change was performed must be maintained. The sample change log below may be used to do this."*

...

# APPENDIX B: GLOSSARY

| TERM | DEFINITION |
|---|---|
| **Change Management** | ISACA (Information Systems Audit and Control Association Institute) defines change managements as<br>*"Change management is the process that ensures that all changes are processed in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. The main purpose of change management is to enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment. "* |
| **Change Request** | Records the details of the change who, what, when, and why. Documents the alteration to software, hardware or data. |
| **Change Log** | Record and track change requests and approvals |
| **Confidential data** | *Data protected specifically by Federal or State or University of Texas rules and regulations (e.g., HIPAA; FERPA; U.S. Export Controlled information; Sarbanes-Oxley, GrammLeach-Bliley; the Texas Identity Theft Enforcement and Protection Act; University of Texas System Policies; specific donor and employee data). University data that are not otherwise protected by a known civil statute or regulation, but which must be protected due to contractual agreements requiring confidentiality, integrity, or availability considerations (e.g., Non-Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements, etc.). Previously referred to as Category I.*<br>***Reference: UTEP Standard 9: Data Classification*** |
| **Controlled data** | *Data not otherwise identified as Confidential data, but which are releasable in accordance with the Texas Public Act (e.g., contents of specific e-mail, date of birth, salary, etc.). Such data must be appropriately protected to ensure a controlled and lawful release. Previously referred to as Category II.*<br>***Reference: UTEP Standard 9: Data Classification*** |
| **Controlled and Confidential data list** | *Controlled*<br>*Employee names*<br>*Employee salary information*<br>*Employee performance review information*<br>*Unpublished research data (at data owner's discretion)*<br>*Non-public University policies and policy manuals*<br>*Internal memos and email*<br>*Confidential*<br>*Social Security numbers*<br>*Access device numbers (ISO number, building access code, etc.)*<br>*Biometric identifiers (eye images, full face images, fingerprints, etc.)*<br>*Date of birth*<br>*Personal vehicle information*<br>*Financial information and records (credit card numbers, account numbers, etc.), including non-University income level and sources*<br>*Information pertaining to the Office of Institutional Relations and Legal Affairs* |

| | |
|---|---|
| | *Contracts*<br>*Certain management information*<br>*Critical infrastructure detail*<br>*User account passwords*<br>*User Identification Number*<br>*Health Information, including Protected Health Information (PHI)*<br>*Health Insurance policy ID numbers*<br>*Credit card numbers*<br>*Financial account numbers*<br>*Export controlled information*<br>*Driver's license numbers*<br>*Passport and visa numbers*<br>*Physical plant detail: Engineering, design, and operational information regarding University infrastructure*<br>**Define:** https://security.utexas.edu/policies/data_classification#data-examples |