

**Drake University  
Computer Information Systems  
Security Policy and Procedure**

This document describes how security policies and procedures are applied to the application environments.

Applications Covered Under this procedure are:

DUSIS which includes: SCT Banner including Self Service, Bookshelf and Online Help, SCT Banner Xtender Solutions, SCT Workflow, Eprint

Blackboard

Luminis which includes: SCT Luminis Content Management System, SCT Luminis Platform System

AdAstra Room Scheduling

RDBMS and Application Servers such as Oracle, Oracle Application and MS SQL Server.

## **Production**

### ***Access to the Production Environments***

#### **Users of Applications**

Users have access to a Production Environment through the Application itself, through secured ODBC or through limited FTP capability only.

#### **OIT Personnel**

Only the following OIT personnel have access to a production environment.

1. The DBA – The DBA requires access to a production environment to perform routine maintenance on database instances and the application objects.
2. System Administrators – System Administrators require access to a production environment to perform routine maintenance at the Operating System level. They do not have access to database instances.
3. Security Administrator – The persons who applies security in a Production Environment. The Security Administrator is a role and not a position. This role may be filled by a DBA.
4. Director of Computer Information Systems – Has access as backup to all of the above.

### ***Security Processes – Controlling Access to Production***

These processes cover Drake University employees, student employees or contractors and are designed to control access to a production environment.

**Drake University  
Computer Information Systems  
Security Policy and Procedure**

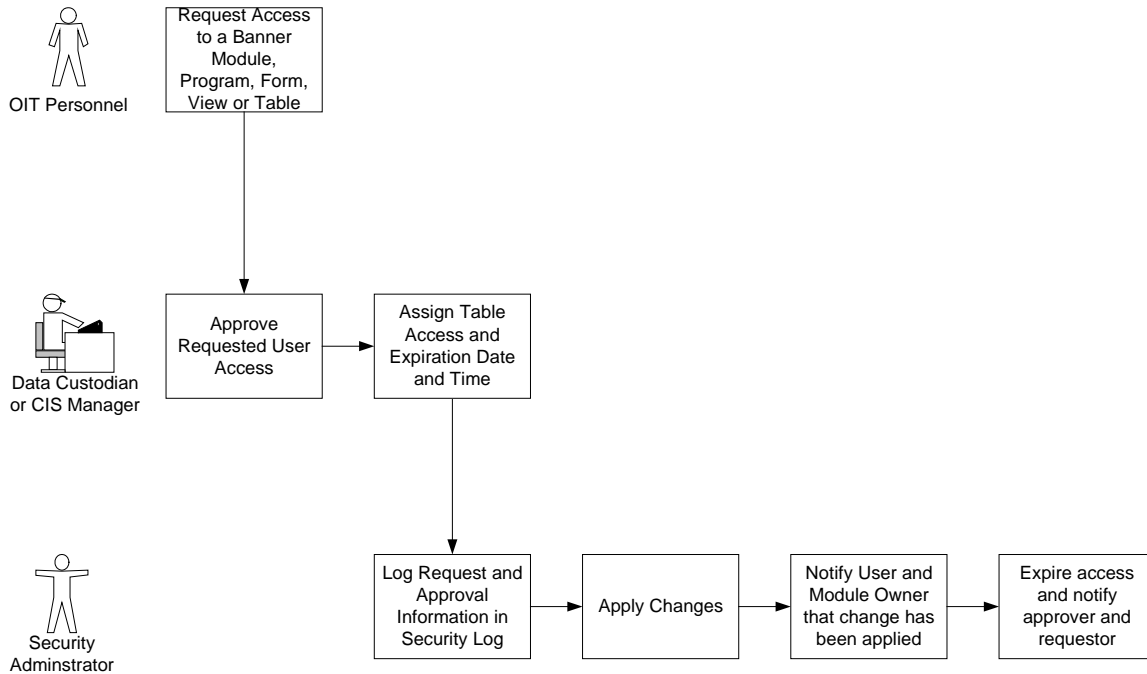
**Employees, Student Employees and Contractors**

Business Unit or College personnel, whether they are employees, student employees or contractors, require access to a production environment to perform their job function for Drake University. When new employees or contractors need access to an application, or existing employees or contractors who already have access to an application need a change in what they can access in that application, the policy and procedure for establishing a log-in as described in the Drake University Data Standards document for that application should be followed.

**Drake University  
Computer Information Systems  
Security Policy and Procedure**

**Office of Information Technology Personnel**

There will be situations where problems arise within a production environment and OIT personnel who do not have access to that production environment will need it to resolve the problem. These personnel will be granted temporary access through the following process.



**Username Rules**

All users in any application should be associated with a named person that has been created as a person in Banner. A GOBEACC record (ties username and Banner record together) will be created by the Security Administrator for each Username.

Any request for a generic username, a username that cannot be associated with a named person in any application, needs to be approved by the Director of Computer Information Systems.

**User Access and Security Audits**

Security audits will be performed on a semi-annual basis (June and December) by Data Custodians for each module in each application to ensure that users have appropriate access to information according to their position with the University. Any changes that need to be made based on the security audit will be reported via email to the OIT Security Administrator. The OIT Security Administrator will apply the changes requested by the data custodian. In the event that a terminated employee still has access the Security

**Drake University  
Computer Information Systems  
Security Policy and Procedure**

Administrator will need to determine whether a security breach has occurred and report back to the impacted Data Custodians.

OIT will also audit users to ensure that user accounts are in use. In DUSIS, any user account left expired for 9 months or more will be dropped and the user notified via email. To reinstate an account the user will need to contact their DUSIS Unit Security Manager. Additionally when users are terminated, their account is locked so that they may no longer access Banner. These accounts will be left locked in for a period of 90 days after which they will be dropped.

OIT will handle account usage in applications other than DUSIS on a case by case basis.

## **Data leaving the Drake Network**

Drake uses service providers to host systems or provide services used for official university business. It is therefore necessary for Drake to send and receive data beyond the boundaries of the Drake network. Confidential data should be sent and/or received via a secure method. Confidential data is data which is protected by laws that govern Drake's dissemination of data (such as FERPA and HIPPA) and data that, if stolen, conveys a quantity of personally identifiable information sufficient to recreate a person's identity for illegal purposes. This includes credit card information.

Approved methods for sending and/or receiving confidential data are SCP (secure copy), PGP encryption, SSL, or any other means where the data is encrypted using a key that is only available to the sender and receiver of the data. FTP and Email are not acceptable means of sending confidential data outside of the Drake network.

Sensitive data which in mass, could cause potential harm to those persons included in the data and Drake University (for example a list of e-mail addresses could be used for unapproved spamming purposes), should be handled carefully and, in most cases, treated with the same care and using the same procedures as confidential information.

Thumb drives, flash drives, pen drives, external drives, etc. are devices often used by Drake faculty and staff to store Drake data for transport and use on other computers. Drives of this type that are not password protected and encrypted pose a security risk as they may be easily lost or stolen and are therefore prohibited from use. Drives of this type that are password protected and encrypted are approved for use.

## **Security Breaches**

The following are considered security breaches at Drake University.

1. Unauthorized access to any application environment by any persons, whether a Drake University employee, student employee or contractor or any outside party,

**Drake University  
Computer Information Systems  
Security Policy and Procedure**

- related to or unrelated to the University. Unauthorized access includes, but is not limited to:
- a. Hacking into the application environment by obtaining by any means username and password/pin information from authorized users of the system.
  - b. Hacking into the application environment through loopholes in the operating system or RDBMS.
  - c. Logging in and accessing information outside of authorized times. Authorized times are defined and monitored by individual University departments.
  - d. Granting of access to unauthorized persons by Data Custodians or OIT personnel.
  - e. Accessing data from an unattended workstation where the authorized employee has logged into the application.
2. Unauthorized use of data or information by any Drake University employee, student employee or contractor. Unauthorized use of information or data includes but is not limited to:
- a. Distributing data or information gained through authorized use to unauthorized persons.
  - b. Distributing data or information gained through unauthorized use to unauthorized persons.
3. Any violation defined in the [Drake University Policy on Acceptable Use of Computer Technology](#).

## **Monitoring for Security Breaches**

Data Custodians are expected to monitor users to ensure only authorized users have access to data. Any suspected breach should be reporting immediately to the OIT Security Administrator and Director of Computer Information Systems.

Inactive user sessions will be terminated after 4 hours between the hours of 8:30 a.m. and 4:30 p.m. During other times, inactive sessions will be terminated after 30 minutes.

OIT will screen logs for unusual activity and report any such activity to Data Custodians for identification of a security breach.

## **What to Do in the Event of a Security Breach**

In the event that a security breach is detected, the following process should be followed by the OIT security team.

The security team is defined as:

1. Director of Computer and Network Services
2. Director of Computer Information Systems

**Drake University  
Computer Information Systems  
Security Policy and Procedure**

3. DBA
4. Network Administrator
5. Systems Administrators

Step 1: Plug the hole. The Security Administrator will disable the username and password. If the breach occurs outside of username and password access, the Network Administrator will remove the server from the network.

Step 2: Assess the damage. Determine whether or not any data, file or operating system values were modified or eliminated during the breach. Determine if data was stolen off of the server.

Step 3: Notify the authorities. Notify the Banner Data Owners and Data Custodians. Call the local police department to report a crime if the scope of the breach warrants.

Step 4: Notify affected parties as required by the FTC Red Flags rule.

Step 5: Notify third parties such as banks or government agencies. Any financial data that may have been taken from the server might allow the theft of money through bank accounts and credit cards.

Step 6: Build a Plan: Meet with Data Owners and Data Custodians to discuss what happened, why, what should be done, who should do what and who should be notified.

Step 7: Communicate the Plan.

Step 8: Execute the Plan.

Step 9: Follow Up.