

IMMACULATA ADMINISTRATIVE DATA SECURITY POLICY

EFFECTIVE DATE:

- Authority** This Policy was approved by the President.
- Policy Statement** Users of the Immaculata University ("IU") network and computer resources have a responsibility to properly use and protect those information resources and to respect the rights of others.
- Policy Purpose** The purpose of this policy is to protect IU Institutional Data.
- Summary** IU has a responsibility under federal law to protect Institutional Data. Such protection entails ensuring the physical, technical and administrative security of the Institutional Data, and in particular Private Information. This policy creates a basic organizational framework for the granting of Administrative Access, the responsibilities of those who have such access, minimum security requirements for computers and networks that utilize Private Information and responsibilities of OTS and Data Stewards at IU.

Section headings are:

1. POLICY SCOPE AND APPLICABILITY
2. DEFINITIONS
3. LOCATION OF INSTITUTIONAL DATA
4. DESIGNATION OF A DATA STEWARD IN EACH DEPARTMENT
5. ADMINISTRATIVE ACCESS
6. DATA: EXTRACTION OF INSTITUTIONAL DATA
7. SEMI-ANNUAL REVIEW OF DATA SECURITY CONFIGURATIONS
8. REPORTING DATA SECURITY BREACHES
9. BASELINE REQUIREMENTS AND RESPONSIBILITIES OF IU COMPUTERS AND NETWORKS AND OTS

I. POLICY SCOPE AND APPLICABILITY

This policy governs the handling, dissemination and protection of IU Institutional Data. It is effective at all IU locations and applies to all Users of Institutional Data, in paper copy and electronic form, at any location, including privately owned computers or systems that connect to an IU computer, such as third parties providing hosting and maintenance services to IU.

II. DEFINITIONS

"Administrative Access" is defined as a level of access above that of a normal User. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. Among other things, this access includes any access that allows a User to access Private Information.

"Directory Information" is student information that includes the address, email address, telephone number, major, grade level, enrollment status (full or part-time,

undergraduate or graduate), dates of attendance, Degrees(s) and awards received, most recent previous school attended, photograph, date and place of birth, participation in officially recognized activities of students and sports and height and weight of students who are athletes.

“Institutional Data” is any information, including Directory Information, Private Information and Public Information, that can be linked to any individual, including but not limited to, students, faculty, staff, patients or contractors. Such data resides in applications such as Banner. Institutional Data and all applications storing and transmitting such data are valuable assets which IU has an obligation to manage, secure and protect.

“OTS Administrator” is the person in the Office of Technology Services (“OTS”) who is responsible for granting new Users Administrative Access and other levels of access to Institutional Data.

“Private Information” is any information, including Non-Public Confidential Customer Information as defined in the IU GLBA Required Information Security Policy, all information that is considered personally identifiable information such as social security numbers, trade secrets or intellectual property such as research activities, home phone number and address, health information, student grades, location of assets, passwords, parking leases, anonymous donors, gender, ethnicity, citizenship, citizen visa code and veteran and disability status. Private Information and all applications storing and transmitting such data are valuable assets which IU has an obligation to manage, secure and protect.

“Public Information” is information, including Directory Information (unless a student has expressly requested non-disclosure pursuant to the IU Confidentiality of Student Records Policy) that is available to the general public.

“User” includes any individuals, entities such as third party hosting contractors, staff, faculty, or employed students, given electronic access to IU’s Institutional Data.

III. LOCATION OF INSTITUTIONAL DATA

IU’s Institutional Data is stored on central servers on the campus and on servers located off-campus and maintained by remote hosting service providers, as well as on individual computers and electronic devices, including but not limited to, laptops and desktops. Such a diverse networked environment poses risks to the security of Institutional Data. Protecting Institutional Data is a shared responsibility between the OTS and the Users of that information.

IV. DESIGNATION OF A DATA STEWARD IN EACH DEPARTMENT

Each administrative department shall designate a Data Steward, typically the head of the department, who is responsible for Institutional Data and specific administration applications in his/her functional area. The Data Steward’s specific responsibilities include:

- Review and approval of all requests for access to and updating of Institutional Data and all applications that support Institutional Data;
- Ensuring that departmental use of Institutional Data is consistent with this policy and other related IU policies, including the IU Confidentiality of Student Records Policy and the IU GLBA Required Information Security Policy;
- Ensuring that all individuals who are given access to Private Information are instructed about its confidential nature;
- Ensuring that administrative systems which are not managed by OTS but that store Institutional Data are secured and protected from unauthorized use, improper disclosure, accidental alteration, and that such systems are properly maintained and backed up; and
- The facilitation of Administrative Access for the appropriate Users through training new Users and collaboration with the OTS Administrator.

Although some of the responsibilities of the Data Steward may be delegated to others in his/her functional area, the Data Steward continues to have overall accountability for the use and security of the data.

V. ADMINISTRATIVE ACCESS

A. Obtaining Administrative Access

Requests for access to Institutional Data for a User should **be submitted electronically or in writing in the form of a *Security Request Form* to the OTS Administrator**. Only the requested and approved access that is specific to a particular User's responsibilities will be granted. The following procedure must be followed to grant Administrative Access to new Users:

1. The relevant Data Steward must review and explain the IU Administrative Data Security Policy;
2. The relevant Data Steward must complete the *Security Request Form*, which will request specific grants of Administrative Access for the new User. This Security Request Form will be electronically delivered to the OTS Administrator;
3. The OTS Administrator creates the login and assigns the level of access to the new User; and
4. The Data Steward trains the new User to comply with this policy.

B. Appropriate Use Of Administrative Access

Administrative Access should only be used for official IU business and then only on a "need to know" basis. Such access may only be engaged using the tools

and means prescribed by OTS, for the stated purpose. Administrative Access should be consistent with a User's role or job responsibilities as prescribed by the appropriate Data Steward. When a User's role or job responsibilities change, Administrative Access should be appropriately updated or removed. In situations where it is unclear whether a particular action is appropriate, and within the scope of current job responsibility, the situation should be discussed with the appropriate Data Steward or the OTS Administrator

C. Inappropriate Use of Administrative Access

In addition to those activities deemed inappropriate in the IU Acceptable Use Policy, the IU Confidentiality of Student Records Policy and the IU Gramm Leach Bliley Required Data Security Policy, the following constitutes inappropriate use of Administrative Access to IU computing resources unless documented and approved by the OTS Administrator:

- Circumventing user access controls or any other formal IU security controls;
- Circumventing bandwidth limits or any other formal IU computing controls;
- Circumventing formal account activation/suspension procedures;
- Circumventing formal account access change request procedures; and
- Circumventing any other IU procedures that are in written form and/or approved by some level of management, the OTS Administrator or any Data Steward.

The following constitutes inappropriate use of Administrative Access to IU computing resources under any circumstances, regardless of whether the use has been approved:

- Unauthorized access to Private Information;
- Exposing or otherwise disclosing Private Information to unauthorized persons; and
- Any use or access of Institutional Data outside the scope of Administrative Access rights granted by the OTS Administrator, including using access to Institutional Data to satisfy personal curiosity about an individual, system, practice, or other type of entity.

D. Termination or Change of Status of Users

Administrative Department Heads and Academic Department Chairs are responsible for informing the Human Resources ("HR") Office, of an employee's change in status or termination. Changes in status may include leaves of absence, significant changes in positional responsibilities or transfer to another department. The HR Office is responsible for making a record of the change in status and notifying the appropriate organizations, including OTS. The OTS

Administrator is then responsible for modifying or terminating the User's Administrative Access.

VI. DATA: EXTRACTION OF INSTITUTIONAL DATA

Extraction/downloading of Institutional Data for processing on systems, including desktop PCs, laptops or any physical or electronic storage medium, other than networks and systems physically maintained by OTS, shall only be done with the permission of the OTS Administrator and the President of IU, and only if the confidentiality, integrity and accuracy of the Institutional Data can be ensured and the physical, technical and administrative safeguards outlined in the GLBA Required Information Security Policy can be maintained.

VII. PERIODIC REVIEW OF DATA SECURITY CONFIGURATIONS

On a periodic basis, Users' access and control to Institutional Data, including Private Information, specifically Banner, are reviewed. Such a review will be implemented by the OTS Administrator.

VIII. REPORTING DATA SECURITY BREACHES

If any User reasonably believes that of any violation of this policy or breach or potential breach of any Institutional Data may have occurred, he or she is required to immediately report to the OTS Administrator or Chief Information Officer of IU. Thereafter, the IU Incident Response Policy will be implicated.

IX. BASELINE REQUIREMENTS AND RESPONSIBILITIES OF IU COMPUTERS AND NETWORKS AND OTC

A. Requirements to Secure Computers that Store or Access Private Information

I. User Requirements

1. **Configuration:** Computers and other devices housing Institutional Data must be set up in accordance with applicable IU security guidelines and standards. Such security guidelines and principles are outlined in this policy. Computers and devices housing Institutional Data and controlled or operated by a third party User must, at a minimum, be subject to the same security guidelines and principles.
2. **Authentication:** Administrative Access and any access to Private Information must be authenticated (e.g. by using a strong and complex password) with file access privileges differentiated by user. Administrator Access passwords should be exceptionally strong and all PCs and laptops

must be password protected in accordance with the IU Password Policy.

3. **Encryption:** For Private information that is sent across the Internet (external to the IU's network) or other open network such as a wireless connection, both the authentication data (e.g. a user id and password) and the data itself must be encrypted. Encryption of Private Information stored on laptop computers or other portable devices is required. Such data may only be stored with OTS permission (see Section VI above). An offsite plain-text backup version in a secure location is recommended to protect against lost encryption keys. IU's wired network (MACnet) is not considered an open network. Consult with OTS to comply with this provision if you are sending or receiving Private Information on a network that is external to IU's network.
4. **Physical Security:** For Private Information that is stored in paper form, Users must properly secure the Private Information to avoid loss, theft or other misappropriation. Such forms of physical security include: proper filing of the Private Information in secure data storage compartments and using appropriate enclosures and labeling for the physical transmittal of Private Information within IU so that only authorized Users view the information.
5. **Anti-virus technology:** Desktop and laptop computers must have anti-virus software or filters installed and updated daily (automatic updates recommended). In addition, other Windows computers, including servers, must have anti-virus software installed and updated daily.
6. **Firewall or filtering:** A software firewall, hardware firewall, or other network filtering (e.g. port or IP address filtering) technology must be used to limit network access to the device storing Private Information.

I. Responsibilities Of OTS

1. **Technical support required:** Computers and other devices must be either continuously managed or reviewed on an ongoing basis for appropriate security measures by OTS. These reviews must include adherence to baseline security requirements outlined in this policy and other IU data security policies as well as additional strategies for protecting the information.

2. **Staffing level:** All departments and units that manage Users must have appropriately supervised professional technical support sufficient to maintain information security. The staffing level should be appropriate to the environment, i.e. the amount and type of Institutional Data, including Private Information for which they are responsible and the level of risk. Collaboration with OTS will be necessary to determine the appropriate level of staffing.
3. **Maintenance and patching:** Security vulnerabilities are regularly found and publicized for software. Regular patching, installation of newer versions, and other maintenance must be performed to protect Institutional Data. Automatic settings or centralized updating of security patches is recommended for most desktop computers.
4. **Access:** Physical access to computers must be restricted as much as possible. Devices not in use for extended periods (e.g. at night and on weekends) must be turned off. Laptops must be physically restrained (e.g. via an anchoring device) at work stations and servers must be in an appropriate and secure physical facility.
5. **Security event logging:** Host security log files must be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event (at least 90 days of logs). The Windows XP/2000 security setting in the QuickStart "Level-2" Security Wizard sets up security logging.
6. **Reporting Critical Servers:** Servers storing Private Information, including servers hosted by third parties, must be identified and scanned regularly with vulnerability testing software.
7. **Backups:** Periodic backup copies of software and data must be made, tested, and stored securely (not in staff cars, homes, etc). The physical security of the removable media must be maintained and plans made to allow recovery from unexpected problems.
8. **Disposal of data and equipment:** A "secure deletion" program must be used to erase data from hard disks and media prior to transfer or disposal of hardware. (See secure deletion). Permanent media (e.g., CD's, etc) must be physically destroyed.

9. **Secure Deletion:** Unless otherwise prescribed by OTS, the secure deletion program Identity Finder must be used for secure deletion of electronic data.
10. **Limit services:** Services available on computers or other devices must be as limited as possible. Web server, ftp server, mail server, peer to peer, and anonymous file sharing software can significantly raise the security risk to Private Information. Unless a high level of expertise is available and these services are closely monitored at all times, this higher risk software should not be installed.
11. **Training:** Training provided by IU on data security practices must be completed by both new and existing employees.
12. **Additional actions:** One or more of the following additional actions should be used to further protect Private Information, depending upon the situation and requirements:
 - Encryption of all Private Information that is stored on any IU server or network or host server or network (with a clear-text version on a removable medium stored in a safe place); and
 - Separate any Private Information from other Institutional Data and store independently (e.g. on a non-networked device).