

# Security & Access Policy

Approved by

Decision Support Steering Team on 5/25/05

## Change History

<b>Date of Change</b>	<b>Description of Change</b>	<b>Reason for Change</b>	<b>Approval/Review of Change</b>
5/30/05	Statement that the policy will be reviewed on a biennial basis was added to “Policy Development and Maintenance”	Decision Support Steering Team discussion on 5/2/05	Decision Support Steering Team authorized the change in its 5/2/05 discussion.
5/30/05	References to Decision Support Steering Team as review/approving body were generalized to terminology consistent with “appropriate administrative oversight group(s)”. In some places the Steering Team role was assigned to the Executive Sponsor.	Decision Support Steering Team will not be continued in FY 06.	Executive Sponsor Douglas Vinzant approved change on 5/2/05.

# Table of Contents

## **Philosophy**

## **Purpose/Scope**

## **Assumptions**

## **Relevant University Policies**

### **Administrative Controls: Data Access**

- Data Classification
- Authentication
- Authorization
- Security Monitoring and Violations

### **Administrative Controls: Data Usage**

- Metadata
- Education
- Secondary Use of Data

## **Procedures**

### **Roles and Responsibilities**

- Decision Support Staff
- Executive Sponsor/Administrative Oversight
- Functional Offices
- Deans, Directors, and Department Heads (DDDH)
- User Responsibilities
- AITs Security
- Office of University Audits

## **Policy Development and Maintenance**

## Philosophy

The value of data as a University resource is increased through its widespread and appropriate use. Its value is diminished through misuse, misinterpretation, or unnecessary restriction to its access. Furthermore, increased data access and use improves data integrity because discrepancies are identified and errors are subsequently corrected.

As an educational institution with a mission to disseminate knowledge, and as a public institution accountable to the public, the University of Illinois values ease of access to information, including administrative data. Permission to view or query Data Warehouse data should be granted to University users for all legitimate institutional purposes. Information specifically protected by law, regulation or University policy must be rigorously protected from inappropriate access. Decision Support's commitment is to balance the appropriate use of data and ease of access with appropriate security protection at all levels.

## Purpose and Scope

This document summarizes security and access policy for the Data Warehouse managed by the Decision Support unit. It applies to multiple environments, databases, applications and users related to the Data Warehouse. It does not cover technical security issues related to data protection, continuity of operations, implementation of security or data integrity.

## Assumptions

- a. Data Warehouse security and access are guided by University of Illinois policy and standards for administrative information.
- b. Data Warehouse security and access is guided by the variety of legal and regulatory directives and standards, such as the Family Educational Rights and Privacy (FERPA) Act, that apply to the University.
- c. Data Warehouse security and access is consistent with Functional Offices' custodianship of subject area data. Decision Support staff work closely with these offices in development of access practices and monitoring of access to the Data Warehouse.
- d. Data Warehouse security and access is consistent with AITS technical infrastructure in which the Data Warehouse is embedded. Decision Support staff work closely with AITS staff on a range of security and technical issues.
- e. Decision Support is responsible for management of security and access for the Data Warehouse and maintaining consistency within these assumptions.
- f. Unit heads are responsible for approving individual's access to Data Warehouse data within their unit. They may delegate this responsibility to a Unit Security Contact (USC). This assumption is consistent with University policy and all other administrative systems.
- g. Access to data is aligned with job responsibilities.
  - Access to data in operational reports is aligned with the individual's responsibility to perform operational tasks. Some individuals performing operational tasks will also have job responsibilities to create reports and queries.

- Access to data to create new queries and reports is also in the job responsibilities of some individuals with no corresponding operational application usage, such as departmental data analysts.
- h. Administrative controls will be balanced by performance and feasibility considerations. In many cases, the more complex the security or access controls, the poorer performance of the data. Where access controls are less than optimal, usage controls, e.g, data education, will be correspondingly increased.

## Relevant University Policies

Access to the Data Warehouse is subject to existing University policies for administrative information and information security. These policies are particularly relevant:

Information Security Policy	2004	<a href="http://www.obfs.uillinois.edu/manual/central_p/sec19-5.htm">http://www.obfs.uillinois.edu/manual/central_p/sec19-5.htm</a>
Social Security Number Policy	2000	<a href="http://www.ssn.uillinois.edu">http://www.ssn.uillinois.edu</a>
University Identification Number (UINs) Policy	2003	<a href="http://www.obfs.uillinois.edu/manual/central_p/sec19-3.html">http://www.obfs.uillinois.edu/manual/central_p/sec19-3.html</a>

## Administrative Controls: Data Access

Access to Data Warehouse data is controlled and monitored. The elements involved in controlling and monitoring this access are described below.

### Data Classification

Not all information resources can be, or must be, equally protected. To ensure that University protection efforts are cost effective, all Data Warehouse resources will be classified based on sensitivity and risk. Access control should be consistent with the classified value of the resources to be protected and the severity of the threat to them.

Data will be classified when it is developed for the Data Warehouse, using categories outlined in the Information Security Policy:

- High Risk - Information assets that would cause severe damage to the University if disclosed or modified. Data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, are in this class. Payroll, personnel, and certain kinds of financial information are also in this class because of privacy requirements.
- Internal - Source code, data, logs, etc. that would not expose University to loss if disclosed, but should be protected to prevent unauthorized disclosure.
- Public - Information that may be freely disseminated.

For the purposes of the Data Warehouse, “Public” is interpreted as freely available within the University community. Data Warehouse data is distributed outside the University only by

those units and individuals authorized to release University data, consistent with University policy and practice.

The design of the Data Warehouse is consistent with the assigned classifications for both detail and summary data. Decision Support is responsible for implementing appropriate protection controls for the data.

Data classification of transformed data is a particular focus. Decision Support transforms data to maximize its usability by the University community. In some cases, transformations are superficial, as in different formats or recoding. In some cases, transformations are substantive, as in creating aggregates, new fields that are combinations of fields or other new data. In the case of superficial transformations, Decision Support will carry forward the data classification of the data from its source. In the case of substantive transformations, a new data classification may be appropriate.

Decision Support staff manage and coordinate this activity with Functional Offices, source system owners and AITS Security. Where there is disagreement on classifications, the appropriate University officer or administrative committee will be consulted.

Decision Support maintains authorization, access, and audit records. These classifications will continue to be maintained throughout Data Warehouse databases.

Decision Support has special responsibilities relative to high risk data. High risk data is private, confidential and protected by law, regulation and University policy. High risk data should only be used for internal record keeping and mandated external reports. Decision Support will collect, maintain and disseminate all high risk data in accordance with University policy, State and Federal laws.

The responsibility to address high risk data issues extends to all venues and formats, including training sessions, education sessions, individual discussions, group discussions, printed materials, electronic materials and Web sites.

Three categories of high risk data warrant additional comment:

**Social Security Number** - Social Security Numbers are represented in the Data Warehouse. Following the University Social Security Number policy, Decision Support will:

- Include the Social Security Number as a data element in the Data Warehouse in a form congruent with that in operational systems
- Source the Social Security Number from the University's system of record, wherever possible
- Not use the Social Security Number as a primary key in its applications
- Identify roles that may and may not view or retrieve Social Security Numbers in the Data Warehouse and seek approval of the University's Social Security Number Oversight Committee for those

**Student Records** - FERPA provides for the confidentiality of student records, requires an educational need to know for access to student records and provides a way for student to opt out of publicly published data. When access to student data is provided through information brokers, such as the Registrar's office or Institutional Research offices, these brokers provide

guidance on appropriate use relative to FERPA. When access to student data is direct, training on FERPA issues is required.

Existence of the Data Warehouse increases the number of University employees directly accessing student data and decreases the opportunities for one-to-one guidance on FERPA issues. Under these circumstances, there is potential for inappropriate use of FERPA protected data. Examples of inappropriate use are: publishing mailing lists that include FERPA protected records on departmental Web sites; failing to include the FERPA confidentiality indicator on reports that list individual student data; leaving paper reports with confidential student data on open desktops, or failing to shred reports with confidential student data after use.

To minimize these risks and be consistent with University policy and practice on FERPA, Decision Support will continue to:

- Include a FERPA confidentiality indicator in the Data Warehouse
- Identify which access roles encompass an educational need to know for student data, relative to FERPA protections
- Coordinate with campus Registrars, the Multi-Campus FERPA Committee and administrative units on policy, procedure and educational issues arising from an increase in student data users
- Limit direct access for one-time or short-term use, instead directing these requestors to the appropriate office where the data needed can be reviewed and prepared. For example, instructional research studies often require short-term use of a complex data set.
- In Decision Support educational programs, include information related to FERPA protections.
- Coordinate with AITS Security and campus Registrars in monitoring FERPA-related security violations

**Other high risk data** - Other examples of high risk data are: University ID Number, racial/ethnic category and disability/veteran status. For these and other data identified as high risk, Decision Support will:

- identify the applicable legal, regulatory and University policies and standards, through consultation with Functional Offices and others
- make stakeholders and users aware of analogous practice for the Data Warehouse
- follow University procedures to resolve any disagreement related to uses of these data elements

## **Authentication**

Access to the Data Warehouse requires authentication of user identity. A unique identifier is used to track access. To the extent possible, identifiers will be consistent with those used in other major University systems.

The identifiers will be secured by passwords. Passwords will follow University guidelines, except where technical considerations, such as software limitations, limit the options.

## **Authorization**

Access to high risk data in the Data Warehouse requires authorization. Authorization is implemented using role-based permissions, rather than assigning permissions to individuals, to provide consistency in access across individuals, data and time.

Authorization will be related to the user's job function and assignments, as determined by the unit (Dean, Director, Department Head or designated Unit Security Contact). It is recognized that the need for analysis and reporting from administrative data will not map as closely to job function as the need for updating operational systems, for example. For example, many support staff are asked by their unit heads to create and run management reports and perform business analyses for the unit. The authorization process for the Data Warehouse therefore must be flexible enough to accommodate a wide range of users while still ensuring appropriate controls.

## **Security Monitoring and Violations**

As defined in the Information Security Policy, a security violation is any event which:

- Fails to comply with data security standards
- Represents an apparent or real effort to undermine, override, or otherwise circumvent security standards or controls.

Decision Support coordinates with AITS Security to monitor security for violations, attempted violations, mistakes, and other breaches to security. Regular reports on security are reviewed by the Executive Director and presented to Functional Office custodians.

Violations will be handled through normal University procedures. Violation of any provision of this policy may result in:

- limitation of an individual's access to some or all University systems;
- initiation of legal action by the University including, but not limited to, criminal prosecution under appropriate State and Federal laws;
- requirement of the violator to provide restitution for any improper use of service; or
- disciplinary sanctions, in accordance with University policy.

## **Administrative Controls: Data Usage**

Usage controls, such as education, are critical for security of Data Warehouse information.

The Data Warehouse is designed to increase the usability of administrative data for multiple purposes throughout the University. Usability can, in some instances, limit the access controls that can be feasibly implemented. For example, performance of the Data Warehouse can be affected by the granularity of authorization mechanisms.

To increase the overall security of Data Warehouse information, Decision Support will continue to balance access controls, usability controls and the usability of the data, except where laws and regulations require otherwise.

## **Metadata**

Decision Support provides users with metadata, that is information on the meaning and appropriate usage of data in the Data Warehouse. Metadata includes information on data source, transformations, model, definition, values, schedules, history tracking, data classification and more. Users informed by metadata are more apt to use data appropriately. Metadata will be provided for all classifications of data. Metadata will be classified and access provided accordingly. For example, there may be some kinds of metadata that are not appropriate for public use, for security reasons.

## **Education**

Decision Support maintains an educational program on meaning and appropriate usage of data in the Data Warehouse to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. Education will include information on these topics:

- appropriate use of high risk data obtained from the Data Warehouse
- appropriate use of data extracted from the Data Warehouse for secondary uses

According to University policy, all users of administrative information share in custodial responsibilities. Custodial responsibility is particularly important in use of a Data Warehouse, where access and active use are encouraged. Active use implies that data moves from person to person throughout the University, whether in paper form, spreadsheets, databases or other forms.

Decision Support will coordinate with those involved in granting access at the unit level (Deans, Directors, Department Heads, Unit Security Contacts) to ensure that they have the information about the Data Warehouse needed to make appropriate assignments. Periodic reminders of these responsibilities and updates will be provided and, where appropriate, coordinated with AITS Security.

Decision Support has a responsibility to assist those involved in educating about data usage, including Institutional Research units, Functional Offices and any staff designated as trainers.

## **Secondary Use of Data**

Secondary use of data is a necessary part of obtaining value from the Data Warehouse. Secondary usage includes, but is not limited to:

- individual use
- local databases
- local applications
- reports, whether electronic or printed
- information distributed to others

Data used for secondary purposes has the same security and access control requirements as those of the Data Warehouse. In particular, sensitivity of data is an attribute of the data itself, and not related to system or location. Those making copies of data for use outside the Data Warehouse are individually responsible for maintaining these requirements at the local site. Department heads, or their designees, are responsible for maintaining these requirements for the department.

Decision Support will provide guidelines for secondary use of data, advise units on specific secondary uses and work with other University units on monitoring of secondary use practices.

Information on responsibilities for local copies of data will be included in Decision Support educational programs.

## **Procedures**

To ensure systematic administrative control, Decision Support will maintain written policies and procedures to govern these procedures.

- Request for access/access change to Data Warehouse
- Request for access/access change to reports in the Business Objects system
- Password change procedures
- New user security procedure
- Maintenance of user lists and profiles
- Procedure changes
- Removing access procedure
- Security monitoring, auditing and reporting

## **Roles and Responsibilities**

All electronic information is the property of the University of Illinois, unless otherwise stated in a contractual agreement. Following is a summary of responsibilities of those units and/or individuals using or supporting Data Warehouse information on University systems.

### **Decision Support staff**

The Executive Director of Decision Support provides oversight of security procedures and controls as applied to Data Warehouse databases and applications. The Executive Director is responsible for assuring users and custodians of operational data that data migrated to the Decision Support environment is secure and managed within University policy, law and regulation. Specific responsibilities are:

- Develop and maintain a Data Warehouse security policy
- Establish and maintain high-level standards and related procedures for access to all levels of Data Warehouse data
- Exercise administrative judgment as to the development, maintenance, operation of, and access to the University data in the Data Warehouse

The Decision Support staff, under guidance of the Executive Director, has these responsibilities:

- Maintain cooperative working relationships with Functional Office Custodians on issues of data classification, data access, data risks and security monitoring

- Provides bimonthly access reports to all functional owners for their review
- Coordinate with AITS Security to select, implement, and administer controls and procedures to manage data access risks
- Ensure that the data design is consistent with data classification
- Identify and evaluate data access risks, such as inactive accounts
- Provide day-to-day administration of access and password requests
- Maintain access and audit records, coordinating where appropriate with AITS staff
- Create, distribute, and follow up on security violation reports
- Communicate appropriate use, and consequences of misuse, to users who access the systems or data
- Promote security awareness to the University community, particularly in the downstream use of Data Warehouse data

### **Executive Sponsor/Administrative Oversight**

The Decision Support Executive Sponsor, in conjunction with appropriate administrative oversight group(s), provides oversight and guidance in development of the Data Warehouse and associated applications and services. Responsibilities are:

- Advise on the administration of security policies
- Review and approve security access policy changes
- Review and approve data classification strategies and outcomes
- Review security monitoring procedures
- Advise when issues should be taken to a broader University context

### **Functional Offices**

Functional Offices are custodians of subject area data. Decision Support staff work closely with these offices in development of access practices and monitoring of access to the Data Warehouse. Responsibilities are:

- Advise on data classification and data risks
- Approve security access plans as new data sets are implemented
- Participate in security data design related to application of University policies, laws and regulations
- Review access and audit records on a regular basis
- Advise on changes and exceptions to access policy
- Promote security awareness to the University community, particularly in the downstream use of Data Warehouse data

### **Deans, Directors, and Department Heads (DDDH) or their designees (USCs)**

According to University policy, Deans, Directors and Department Heads are responsible for ensuring that University security policies are implemented within the unit. These duties may be delegated to a Unit Security Contact (USC). Responsibilities are:

- Ensure that unit employees understand security policies, procedures, and responsibilities related to the Data Warehouse

- Approve appropriate data access for individual staff that allow them to complete job-related assignments
- Review, evaluate, and respond to all security violations reported against staff, and take appropriate action
- Communicate to appropriate campus and University departments when employee departures, arrivals, and changes affect Data Warehouse access
- Ensure security procedures are in place to protect information assets obtained through the Data Warehouse under their control, particularly the secondary use of data in local systems

## **User Responsibilities**

Anyone accessing Data Warehouse data is personally responsible for proper use of the resulting available information. Responsibilities are:

- Comply with University and Decision Support security access standards and procedures in the use, storage, dissemination, and disposal of data
- Protect data from unauthorized access
- Protect data from unauthorized distribution. Specifically, all users are expected to refrain from distributing data to others in any form, unless they know that those others have the appropriate access level. That means that reports developed by person A may not be distributed to person B, unless person B would be permitted to see that data, should s/he request Data Warehouse access.
- Maintain the integrity of user IDs for Data Warehouse data and applications. Specifically user IDs and passwords are not to be shared and users are responsible for maintaining the security of their IDs and all activity occurring under those IDs.
- Report information security violations to their Dean, Director, or Department Head, or to the designated Unit Security Contact (USC)
- Report data integrity errors to Decision Support
- Maintain the accurate presentation of Data Warehouse data, and assume responsibility for the consequences of any intentional misrepresentation of that data

## **AITS Security**

AITS Security is the unit within AITS that is responsible for managing information security standards, procedures, and controls intended to minimize the risk of loss, damage, or misuse of AITS-supported electronic data. Relative to Data Warehouse security, this group's responsibilities are:

- Assist Decision Support staff in identifying and evaluating information security risks
- Coordinate with Decision Support staff on security monitoring, auditing and reporting
- Advise and/or broker Decision Support's contact with the Unit Security Contact (USC) network
- Serve as the AITS focal point for reviewing data security issues that have campus- and University-wide impact

## **Office of University Audits**

Internal auditors are authorized to inquiry-only access to all administrative information and systems, and are responsible for assisting the Decision Support staff in the effective discharge of their duties. Internal auditors responsibilities are:

- Evaluate Decision Support's security policy and procedures compliance, during operational and administrative audits
- Evaluate the effectiveness of security procedures and other internal controls
- Review audit trails provided by staff to determine whether activity is adequately documented
- Assist the Decision Support staff in the investigation of suspected incidents of security breach or improper activity
- Provide advice regarding internal control relevant to new systems being developed or considered for purchase.

## **Policy Development and Maintenance**

### **Administration of Policy**

The Executive Director of Decision Support is responsible for administering this policy with the advice of the Associate Vice President for Planning and Budgeting and appropriate administrative oversight group(s). The Executive Sponsor must approve major policy changes. Policy changes that are potentially incompatible with University security policy for administrative resources must be reviewed and approved by the appropriate University management team. The policy will be reviewed on a biennial basis.

### **Changes to Policy**

All requests to change Data Warehouse policies must be received in writing or via email and contain brief, factual comments describing the problem, recommendations, and benefits of the proposed change.

### **Exceptions to Policy**

If an exception is required, a written/emailed request including a description of and justification for the exception is sent to the Executive Director of Decision Support. All exceptions require the approval of the Executive Director of Decision Support and may be appealed to the Executive Sponsor and/or appropriate administrative oversight group(s). Decision Support retains all such requests for audit purposes.