

ASU Data Warehouse Data Policies and Procedures



How to Get Answers to Questions About the Warehouse

Ware-q@asu.edu Email Support

Send an electronic mail note to the ASU Data Warehouse Consulting user ID, **WARE-Q**. The complete internet address is **WARE-Q@asu.edu**.

WARE-Q is an email distribution list that goes to approximately 20 Warehouse consultants. The consultants cover every aspect of the Data Warehouse and are all approved to access all databases on the Warehouse. The first available consultant with an answer will contact you. When contacting ware-q, feel free to attach a query to your note that you are having a problem with. If you prefer to be contacted by phone, just let us know and we will call. WARE-Q is more efficient than calling individual consultants and you often get good ideas from more than one consultant!

Topics that are handled on ware-q include:

- User ID's and passwords.
- How to get access to the Warehouse or status of access requests.
- Software questions – BrioQuery and Sybase. (We will answer Access questions as we can however a better place to send them is the Access Users Group.)
- Data definitions and use questions – Student, Financial and HR data.
- Error message troubleshooting.
- How To questions of all types.
- Warehouse performance questions. (I.e. why is it slow today?)

Data Administration Web Page

Check out the Data Administration web pages at **http://www.asu.edu/data_admin** for Warehouse information for information on:

- Data Diagrams
- Table Documentation
- Warehouse Users Group (WUG) Handouts
- Brio Query

Data Warehouse Policy Crib Sheet

Data Access Policy

This policy states that data belongs to the University, rather than an individual department. It states that employees shall have access to data without artificial restriction. This policy is responsible for the birth of the ASU Data Warehouse.

Data Usage Policy

This policy states that the University trusts its employees to use data for the purpose of their job not for personal gain or other inappropriate behavior. If you are not using the data for your job... you have no business using it.

File Transfer Guidelines

This policy states that if you obtain data from the Data Warehouse, YOU are responsible for knowing that it is used appropriately even if you transfer it to another person. You cannot assume that persons asking you for data are knowledgeable regarding data policies. You must know that what they need to do with the data constitutes acceptable usage under the various policies. This is especially important with STUDENT data due to FERPA requirements.

Data and Application Control Policy

This policy describes computer related controls that may be necessary for Warehouse users that store data on local hard drives or networks. Once data has been removed from the Warehouse, it must be protected from unauthorized use, hence network and hard drive security become very important. You may want to discuss this policy with your network administrator.

Application User ID Policy

This policy outlines requirements for an application developer to request a special user ID for a computer application to use the Data Warehouse.

Arizona State University - Data Access Policy

Purpose	The University will provide appropriate access to administrative information for its employees without unnecessary difficulties or artificial restriction. The university also intends to protect its data assets through security measures and to assure the proper use of the data when accessed (see the University Information Policy on Security and Responsibilities for Data).
Source	Data Administration Subcommittee of the Administrative Computing Advisory Committee
Applicability	This policy applies to all employees of the university and to all administrative information regardless of the form of storage or presentation. A typical but not exhaustive list of presentation and/or storage means includes: printed matter, microfiche, microcomputer diskettes, computer/terminal screens, mainframe tapes/disks, and computer/communication networks.
Background	University data are institutional assets and are held by the university to support its fundamental instructional, research, and public service missions. Innovative management is largely dependent on data that are freely available. The intent of this policy is to assure that the data are easily accessible for the faculty, staff, and management of the university.
Keywords	Administrative data/information, data trustee, restricted access.
Policy	Open access to administrative information will be provided to employees for the support of university functions. Default access is: <i>Open Access</i> to all employees with <i>Restricted Access</i> to all others (e.g., students, off-campus affiliates, etc.) except for information designated as part of the “public record.” Any request to restrict employee access must be documented to Data Administration by the designated data trustee. Any employee or nonemployee denied access may appeal the denial to Data Administration.
Definitions	<i>Administrative Data/Information</i> —[AKA University Data] is the collection of data elements that is relevant to the operations, plans, or management of more than one ASU unit or are reported on or used in “official” administrative university reports.

Data Trustee—the individual identified by the office responsible for the collection and/or maintenance of the specified data element(s). Data Administration is the Trustee for all data elements not specifically assigned to another trustee.

Open Access—data in this category are available on receipt of an account. No further approvals are required. The cost of connection to the data is still the responsibility of the department or person requesting access.

Restricted Access—a designation applied to certain data elements that limits access because of legal, ethical, or privacy issues. Access to elements so designated can be obtained with the approval of the designated data trustee.

Approved by Information Technology Advisory Committee (ITAC) on 10/2/92
Approved by the Provost Office on 5/18/93

Arizona State University - Data Usage Policy

Purpose	The University will manage its data in a way that provides for confident, open access for the entire university community as support for the performance of their assigned duties. This policy is intended to ensure that the data assets of the university are not misused or abused. Open access to data represents a statement of confidence on the part of the university that its personnel will use the data for the purposes intended and not for personal gain or for other inappropriate behavior.
Source	Data Administration Subcommittee of the Administrative Computing Advisory Committee.
Applicability	Adherence to this policy is mandatory for all university personnel.
Background	University data are institutional assets and are held by the university to support its fundamental instructional, research, and public service missions. Innovative management is largely dependent on data that are freely available and that correctly represent the information intended. This policy is intended to assure that data are used ethically and with due consideration for individual privacy.
Keywords	University data [administrative data/information] data trustee, data integrity, data model, data dictionary (repository, encyclopedia) data element, data value, domain, directory information.
Policy	<p>Use of data falls into the categories of update, read-only, and external dissemination. The cognizant data trustee shall grant authority to update data only to personnel whose job duties specify responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with the university's desire to provide excellent service to our customers and constituents.</p> <p>Read authority is covered in the Arizona State University Data Access Policy.</p> <p>External dissemination of individually identifiable data (whether in summary or specific form) is permitted for official reporting and for "nonofficial" reports when they use only those data elements designated in the data dictionary as <i>Directory Information</i>. Even for these elements, release should be guided by the absolute requirement to respect individual privacy and to protect the integrity of the data. The release of all other data must be approved by the data trustee(s) for the element(s) involved.</p>

Special care must be taken in the creation of “downloaded” files so that both the values and their meanings as defined in the Data Dictionary are not altered.

Definitions

University Data—the collection of data elements that is relevant to the operations, plans, or management of more than one ASU unit or are reported on or used in “official” administrative university reports.

Data Trustee—the individual identified by the office responsible for the collection and/or maintenance of the specified data element(s). The University Data Administrator is the Trustee for all data elements not specifically assigned to another trustee.

Data Integrity—the qualities of validity and reliability conjoined with the accuracy of values.

Data Dictionary—a reference tool (in paper or electronic form) which provides a list of all the data elements and their alias names. A data dictionary usually contains a working definition of each element, the values that are allowed, location information, and additional metadata deemed important for an organization to maintain regarding its data assets.

External Dissemination—the distribution (in any form, including “downloads”) of data to persons or to files that would not otherwise be granted such access. This is intended to apply to individual-specific information and not summary information, especially as contained in government compliance reporting.

Directory Information—data elements identified by the university as being releasable on an individual-specific basis externally unless specifically requested not to do so through the provisions contained within FERPA. Directory elements are so designated with the Data Dictionary and are not limited to student and staff information but may also include financial and research data.

Consequence of Noncompliance

Failure to comply with this policy or any actions deemed “inappropriate conduct” as defined in the following policies and procedures manuals: Academic Affairs Policies and Procedures Manual, number ACD 204-01, page 3, Faculty Code of Ethics, Staff Conduct and Work Rules, and the Student Affairs Policies and Procedures Manual, number 104-01, page 5, Student Code of Conduct, and number 105-01, page 1, Release of Student Information, may result in denial of access.

Approved by ITAC Executive Committee on 1/15/93, Approved by Information Technology Advisory Committee (ITAC) on 4/2/93
Approved by the Provost Office on 5/18/93

Arizona State University - File Transfer Guideline

Purpose	The purpose of this guideline is to assist university staff in dealing with issues related to file transfers of university data. This guideline does not provide technical specifications or other technical information regarding file transfers.
Source	Administrative Computing Advisory Committee.
Scope	This guideline should be followed for file transfers of university data. The university community may also choose to follow the guideline where the file transfer does not involve university data in order to achieve similar benefits.
Background	As the university transitions to and achieves a distributed processing environment, file transfer will become commonplace. This guideline will help practitioners better understand and deal with file transfer issues and thus better protect university data.
Keywords	Data extraction, data trustee, file transfer, data storage, university data.
Guideline	<p>File transfer occurs when a copy of a data file is moved in electronic form from one location to another. Those who choose to perform file transfers should consider the following issues:</p> <p><i>Data Extraction</i></p> <ol style="list-style-type: none">1. Timing—because data files may be updated at any time, the timing of a data extraction should be coordinated with the data trustee for that file. At a minimum, one should consider when in the update cycle to extract the data, and when the data become “official” for reporting or other purposes. In particular, one should consider the difference between data on an active data file, which may be updated many times each day, and data on an historical data file, where data values are generally frozen.2. Definition—extracted data should retain the same definition it had when on the university database to prevent misuse and misunderstandings. <p><i>Data File Transfer:</i></p> <ol style="list-style-type: none">1. Error detection—the data communications software (e.g., FTP Fortenet, IRMA, KERMIT, etc.) used to transfer the data should be capable of managing the data transfer process, detecting data transmission errors, and either correcting the errors or informing the operator that errors have occurred. This will help to ensure the validity and integrity of the data.

2. Standard software—the data communications software should be selected from the list of software offerings officially supported by ASU.
3. Scheduling—the scheduling of the data transfer should consider the quantity of data and what other network activities are taking place. The goal should be to not unduly impact other users of the network by transferring large quantities of data during peak periods of network and system usage.

Data Storage and Usage

1. University data, once transferred, should be stored in a secure location on a secure file device. If the file device is part of a LAN, the LAN should be secure from unauthorized access.
2. The application that processes the transferred data should be documented to show where the data were extracted from, which data were extracted, and how the data are intended to be used.
3. The application documentation should also show how often the data are extracted and transferred so that the user will be aware of its age, condition, and meaning.
4. The application documentation should be on-line.

Definitions

Data Extraction—the process of copying a subset of data from an existing file to create another file.

Data Storage—the storing of data on some electronic device (e.g., hard disk, tape, floppy disk).

Data Trustee—the individual identified by the office responsible for the collection and/or maintenance of the specified data element(s). The University Data Administrator is the trustee for all data elements not specifically assigned to another trustee.

File Transfer—moving copies of data in electronic form from one data storage device to another.

University Data—defined as the collection of data elements that are relevant to the operations, plans, or management of more than one ASU unit or are reported on or used in “official” administrative university reports.

Approved by ITAC Executive Committee on 1/15/93

Approved by Information Technology Advisory Committee (ITAC) on 4/2/93

Approved by the Provost Office on 5/18/93

Arizona State University - Data and Application Control Policy

The purpose of the Data and Application Controls Policy is to make sure that data, which are removed from the ASU Data Warehouse and stored locally in campus units, are appropriately protected to ensure security, integrity and availability. This policy applies to all ASU Data Warehouse users and application developers as well as to managers of units that store Warehouse data locally.

It is a common and necessary practice to query the ASU Data Warehouse and save data locally on departmental computers, disks and networks. Often the data are saved in application software such as BrioQuery, or Microsoft products such as Word, Excel and Access. In some cases, Warehouse data may be imported into a college or department database such as SQL Server, Sybase or Oracle.

This policy is intended to inform Data Warehouse users and their managers about computer-related controls that they should use when maintaining Warehouse data locally. Access Controls are necessary to limit and/or detect access to data or applications, thereby protecting these resources against unauthorized modification, loss, and disclosure. Service continuity controls are designed to prevent and minimize potential damage and interruption, which may make data or applications containing Warehouse data unavailable. Failure to appropriately consider these controls may result in a Data Warehouse user's access being removed.

ACCESS CONTROLS

Access Controls should provide reasonable assurance that data and applications are protected against unauthorized modifications, disclosure, loss or impairment. Such controls include physical controls, such as keeping a computer in a locked room to limit physical access, and logical controls such as security software programs designed to prevent or detect unauthorized access to sensitive files.

Security software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. An operating system such as Microsoft NT can fulfill this function by assigning user IDs with properly maintained passwords and by assigning user ID-based file permissions. Data users must take note of where files are maintained and archived, and understand when and how to delete them. Users are cautioned when storing data and applications on network drives, as they must be accessible to authorized Warehouse users only. Care must be taken to permanently erase all data files on a computer or disk before transfer to another unit, and upon termination, an employee's access must be removed.

SERVICE CONTINUITY CONTROLS

Service continuity controls are designed to prevent and minimize potential damage and interruption which may make data or applications containing Warehouse data unavailable. Locally developed applications may become critical to the mission of campus units. Controls developed to provide service continuity are best planned by management level staff based on the criticality of the data or application to the mission of the unit. These might include:

Appropriately Trained Staff

Data or an application may become unavailable in the event that the only staff member who understands the data resigns. Management must take appropriate steps to ensure adequate staffing for data and applications that are considered necessary to the functioning of the unit.

Back Up of Data and Applications

Backing up a data file on a hard drive can be as simple as copying it to a floppy disk, a network drive, or a zip disk. In situations where large volumes of data are stored and applications that manipulate the data are in use, more traditional back up schemes may be used, e.g., nightly or weekly dual tape backups with one copy being stored remotely. For applications with many transactions, transaction logging may be considered in addition to tape or disk dumps. An effective backup plan will allow recovery of all data and applications with minimal time and effort.

Protection from Viruses

To protect valued data and applications from viruses, virus identification and removal software is critical. Information on virus software for use at ASU is available at <http://www.asu.edu/antivirus/>

Documentation and Training

Developing appropriate documentation regarding stored data and applications is critical so that they are not lost if the staff who developed them leaves the unit or is absent. Documentation should show managers, users, and others, what the system is supposed to do and how it should perform. Documentation should include program flowcharts defining inputs and outputs, data diagrams, commented source programs, report printouts, operating instructions, testing procedures and modification history when applicable. Both application and data policy training must be provided for other staff members who will use the data or application.

Environmental Controls

It may be important to provide appropriate temperature conditions for servers and workstations, protection in case of fire, temporary power supplies for equipment to operate in case of a power failure, and surge protectors to prevent equipment from being damaged by electrical spikes.

Not all of the controls listed above may be necessary for all Warehouse data that is stored locally. Service continuity controls should be appropriate to ensure that critical operations continue without interruption or are promptly resumed in the event of interruption, and that critical and sensitive data are protected. At minimum, Access Controls must be used to prevent unauthorized access to Warehouse data.

Arizona State University - Warehouse Application User ID Policy

An Application User ID is a user ID that is given to a software application rather than to a specific person. The purpose of this Application User ID Requirements document is two fold:

1. To recognize that campus information system applications may be developed which depend on data from the ASU Data Warehouse.
2. To provide a mechanism for those applications to operate with a user ID which is independent of a particular individual whose employment at ASU may change.

With approval from the appropriate Data Trustee, Data Administration will recommend that a Warehouse application ID be approved when the following requirements are met:

Manager's Statement

The manager of the unit in which the application resides, must indicate that the application is critical to the unit's operation and agree to resource the application appropriately to provide Access Control and Service Continuity Controls as described in the ASU Data Warehouse Data and Application Controls Policy. The manager must designate a primary contact person for the application who will be responsible for resolving problems that arise in either the application ID process or the ongoing operation of the application. This person will also be responsible for updating Data Administration with changes to the application that affect the data that is being gathered from the Warehouse or that affect the data's security.

Documentation

In order to plan Warehouse changes and anticipate how they impact applications that use Warehouse data, it is critical that Data Administration, Data Trustees, and Information Technology support staff know what data is being used by the application. To facilitate this, a short description of what the application does must be submitted with copies of the SQL used by the application to obtain data from the Data Warehouse. An explanation of the times of SQL execution should also be included (for example, executes each Monday through Friday at 8 am, or executes upon demand from 8 AM to 5 PM on weekdays).

Training

A training plan for the users of the application must be submitted which includes identification of a local staff member who will be responsible for educating users of the application on Warehouse Data Usage Policies.

Access Control Mechanism

A description of the Access Control methods must be submitted, with at least one regularly employed ASU staff member identified to perform these procedures. A second staff member should be identified as a substitute. These staff will have responsibility for granting individual access to users and deleting their access when no longer employed in the unit. The mechanisms by which the application's user ID will be protected from unauthorized use or detection should be described as well.

Virus Protection and Backup Plan

A description of the virus protection software/procedures and backup procedures for the application must be submitted.

Environmental Controls

A description of any environmental controls that are planned such as temporary power supplies, fire protection, or surge protectors must be submitted.

A campus unit can initiate the process for requesting an application ID by sending a note to ware-q@asu.edu. Data Administration will contact the requesting unit and gather the required materials. This policy is intended to facilitate well-planned and supported applications that use Warehouse data in order to provide maximum benefit to campus units while ensuring that Warehouse data is secure.

Guidelines on the Release of Data To External Agencies

These guidelines refer to all data contained in the ASU Data Warehouse. Please see the ASU Policy on the Release of Student Information for more specific information pertaining to student data. You should use caution when releasing data to any off campus entity or any persons not employed by the university.

1. Requests for summarized or unit record data from **media sources** (i.e. TV, paper, magazine).
 - Refer all media requests to the ASU News Bureau.
2. Requests for summarized or unit record data from **government sources** (i.e. Arizona Board of Regents, State Legislature, Governor's Office).
 - Refer requests to the Provost or President's Office.
3. Requests from **accrediting/licensing agencies** for summarized data.
 - With proper checking of data to ensure accuracy, summarized data can be released. Data should match official publications/reports such as the Enrollment Summary and the Registrar's Report to the Arizona Board of Regents.
4. **Surveys** that require data pertaining to the university as a whole.
 - Refer to Institutional Analysis who is charged with coordinating campus surveys.

ASU Policy on the Release of Student Information

Arizona State University, pursuant to the Family Educational Rights and Privacy Act, 1974 (the Buckley Amendment), has a comprehensive policy to safeguard the confidentiality of student personal and academic information. Complete instructions are furnished in the University Bulletin, "ASU Policy on the Release of Student Information," a copy of which is included in the appendix.

If you have specific questions concerning release of student information, please call Records Information at 5-3124.

Inspection of student records by University officials is permitted for educational purposes only. Two types of educational records are defined:

- 1) Directory Information
- 2) Personally Identifiable Information

Student Directory Information

Directory information may be released to anyone without the consent of the student, unless the student indicates otherwise in which case a Directory Release Flag is added to the student's record in the Student Information System. Directory information includes:

Student Name	Local, Permanent and Email Address
Local Telephone Number	Date and Place of Birth
Citizenship	Degrees and Awards Received
Residency Status	Academic Level
Academic Major	College
Dates of Attendance	Participation in Officially Recognized Activities and Sports
Weight/Height of Members of Athletic Teams	Most Recent Previous Educational Institution Attended

Personally Identifiable Student Information

All information not defined as directory information. It may not be released without the consent of the student. Inspection of student records by **university officials for educational purposes** is permitted.

Guidelines when producing reports with Student data.

The Family Educational Rights and Privacy Act of 1974 remains in effect for Student data that is accessed through the ASU Data Warehouse. The following are guidelines that you should be aware of when producing reports:

1. Always observe student directory release codes.
 - blank - OK to release directory information.
 - 1 - No telephone or address information to be released.
 - 2 - No directory information to be released.
2. Non-university requests for student lists and/or labels
 - Information on applicants that are not yet enrolled must be obtained from the Admissions Office.
 - Information on enrolled students must be obtained through the Registrar's Office.
3. Requests for information from student organizations
 - Must be an officially recognized student organization (verified through Student Life).
 - Must be approved by student organization faculty or staff sponsor.
 - Cannot use non-releasable data elements such as GPA, ethnicity, or gender as a criterion for selection.
4. Questions about use of Student data
 - Can be directed to ware-q@asu.edu or Records Information, 5-3124