

Date	Title	Chapter	Page
7-00	SECURITY	II	A.1

A. TIS On-Line Security System

The TIS On-Line Security System provides security by authorizing staff at two distinct levels: (1) Access to the on-line system and its processing functions and (2) access to the specific populations of data. These levels are described below:

1. TIS Access

Access to the TIS On-line Maintenance System is limited to authorized staff persons only. The determination of who should be authorized is made by each institution, based on what is most appropriate for that institution.

Sign-on Identifier (LOGIN ID):

Each staff person who is authorized to update information using the on-line system is assigned a unique identification code (ID), which is used in the sign-on process to identify the staff person to the computer and to the TIS System. The Login ID consists of the institution's 3 to 5 character abbreviation plus the staff person's 3 character initials.

Password:

A password also is assigned to each staff person with update access, to be used in combination with the Login ID when signing on to the system. The password does not show on the login screen when it is typed, and, in this way, "protects" the Login ID from being used by anyone other than its owner.

It is critical to security that staff persons ensure that their passwords are completely confidential. Passwords should not be written down or shared with anyone, even other staff. Passwords must be at least 5 characters in length. For additional security, passwords should be changed regularly.

A temporary password is assigned when a Login ID is added. During the initial login, the user is required to change the password.

2. TIS Data Access

Once a staff person has been authorized to use the system, access to the TIS data may be authorized at one of the levels described below. These authorizations may vary within each function. For example, a person may be authorized to view and update equivalency information but only be authorized to view course information.

Level 1: View data only

Authorized staff can view course and/or equivalency data for any institution in TIS. Note: View access includes the option to generate reports of the data.

Date	Title	Chapter	Page
7-00	SECURITY	II	A.2

Level 2: View data for any location, and update data for own location (retrieval and maintenance access)

This level will allow authorized individuals to view course and/or equivalency data for any institution in TIS. It also will allow authorized individuals to update data within the authorized function at their institution. Authorized individuals at this level cannot update data for any other institution. Note: View access includes the option to generate reports of the data.

Level 3: View and update data for any location (retrieval and maintenance access)

Authorized System Administration TIS Staff can view and update any data for any of the TIS institutions.

3. Maintaining Authorizations

It is critical to TIS security that access authorizations are kept current and up-to-date, i.e., terminating staff persons are removed from authorization as soon as possible, changes in staff duties that affect authorization are modified as soon as possible, etc.

Authorization Form:

The security authorization form is used to request additions or deletions to system authorizations. It also may be used to request that a password be reset when the password has been forgotten. The institution completes the first block of the form and sends it to the TIS coordinator at UW System Administration, who reviews and approves the request by dating and signing in the second block and forwarding it to the Office of Information Services (OIS) for implementation. The third block on the form is for internal use by OIS security staff. Once the authorization request is received by OIS, the authorization is updated and will be effective the following day. The institution will be notified when the authorization has been processed.

4. Instructions for completing the authorization form.

1st block: to be completed by institution.

- one form is provided (following this page); please make a copy each time you need to submit the form.
- fill in the current date.
- fill in the effective date on the authorization.
- fill in the name of the staff person to be authorized. Also include the phone number and email address on requests for security additions.
- check whether the authorization is to be added or deleted for the staff person or if a password is to be reset.

Date	Title	Chapter	Page
7-00	SECURITY	II	A.3

- circle your Institution Abbreviation.
- fill in the staff person's initials (3 characters).
- sign and date the form. The signature should be of the Campus or District Liaison or Security Administrator for TIS.
- send the form to the TIS Project Coordinator at UWSA.

2nd block: to be completed by TIS staff.

- after reviewing the authorization request and determining its approval, date and sign the form.
- send the form to the UNIX Coordinator at the Office of Information Services.

3rd block: to be completed by the OIS UNIX Coordinator.

- perform the requested authorizations.
- sign and date the form.
- notify the TIS Project Coordinator that the authorization is complete. The TIS Project Coordinator will notify the Campus Security Administrator.

Date	Title	Chapter	Page
7-00	SECURITY	II	A.4

TRANSFER INFORMATION SYSTEM
LOGON SECURITY AUTHORIZATION

DATE: _____

TO: Gail Bergman
1646 Van Hise, 1220 Linden Drive
Madison, WI 53706

Please modify TIS security for the staff person listed below, effective ___/___/___.

Staff name: _____

Phone: (____) _____

Email Address: _____

____ Add TIS access
____ Delete TIS access
____ Reset Password

Institution ID: (circle one)

EAU GBY LAC MSN MIL OSH PKS PLT RVF STO STP SUP WTW EXT SA
BRB BRN FDL FOX MAN MNT MSF MTH RCK RLN SHB WAK WSH UWC
BTC CVTC FVTC GTC LTC MATC4 MATC9 MSTC MPTC NATC NTC NWTC SWTC WCTC
WWTC WITC WTCSB

Staff initials: _ _ _

Campus/District Liaison signature: _____

Phone: (____) _____

DATE: _____

TO: OIS Security Coordinator
780 Regent Street, Room 246

The above security authorization is approved.

Gail Bergman
TIS Project Coordinator

The above security authorization has been updated.

OIS UNIX Coordinator

Date