Application Accounts to the Data Warehouse

Approved by Decision Support Steering Team and UTMT

September 29, 2004

Background

Application logons are defined as logons designated for a computer application or group of applications. Application. They are often needed in units where a scheduled application retrieves data from the Data Warehouse. In many cases, there are multiple technical staff supporting the application. Use of individual logons in these situations involves sharing personal logon, in violation of University policy.

University policy indicates that responsibility for logons is generally assigned to an individual. The policy (http://www.obfs.uillinois.edu/manual/central_p/sec19-5.htm) says:

> Access to the network and servers and systems will be achieved by individual and unique logins, and will require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
>
> …….
>
> As stated in the Appropriate Use Policy (2), users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.
>
> ……
>
> Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.

The purpose of the policy is to maintain information about the person responsible for use of a login, should there be a security/confidentiality violation.

Guideline

Decision Support will provide second logons for use with applications to individuals. The individual is accountable for all use of the application login, just as s/he is for use of a personal logon.

Where there will be multiple individuals supporting an application and using the application logon, each of those individuals must be identified to Decision Support. These individuals must sign a form certifying that they understand the responsibilities associated with use of the application logon.

Below are the responsibilities of the individual with the application logon, the secondary users of the application logon and the unit.

Unit Roles and Responsibilities

- The individual assigned an application logon is expected to ensure that the application is consistent with the unit's security procedures.

  According to the University Information Security Policy http://www.obfs.uillinois.edu/manual/central_p/sec19-5.htm#cc

  > Each unit appoints a person to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

  Applications that access secured data in the Data Warehouse are expected to have a security plan and process to continue appropriate access for secured data as it moves from central database (Data Warehouse) to local use.

- As with personal logons, the individual assigned an application logon is accountable for all use of the application logon. This responsibility includes providing secured data to other individuals via the application and ensuring that the security classification of the data is maintained as it is distributed at the point of contact with the application. (This responsibility is the same as the expectation that individuals distributing data via reports, spreadsheets or other means.)
- Should the individual assigned an application logon leave the university, the logon name may be retained but responsibility must be reassigned to another individual. When the logon is reassigned to a new individual, the password must be changed. If an application logon is not reassigned, it may be suspended or terminated, just as other logons without employees may be, in the course of normal maintenance. Requests for reassignment are done through the Unit Security Contact for the unit.
- Those who are secondary users of another person's application logon, as part of their assigned duties to support the application, have the same responsibilities for ensuring appropriate use of secured data.
- Those who are secondary users of another person's application logon must be designated to Decision Support and sign an agreement indicating that they understand these responsibilities for use of another person's logon. *Agreement similar to that in current use by AITS.*

Central Roles and Responsibilities

- Decision Support is responsible for answering questions on the security status of Data Warehouse data so that a) the unit may take appropriate security measures in the application's security plan and b) those with application logons may ensure appropriate use of the data via the application.
- DS may from time to time audit a unit's procedures for handling application logons that access the Data Warehouse in order to ensure their effectiveness; whether audited or not, units remain responsible for ensuring the effectiveness of their procedures
- DS will approve units having application logins (as defined) based on the general need of the unit; this approval of the need for the service and the general procedures and roles involved in the service normally takes place once, and is not reviewed when the specific individuals change. If a unit changes the number or names of individuals, DS expects that the use and process already approved will not materially change. Review of applications themselves is not within the scope of this policy.
- UTMT and Decision Support will consult on interpretations of the University Information Security Policy as it pertains to application logons for the Data Warehouse.

- In the course of fulfilling its auditing responsibilities for information security, the Office of University Audits may review management's controls over system access and information use, disclosure, modification, or loss.
- Members of UTMT are responsible for procedures for appropriate training to data owners, data custodians, network and system administrators and users; for procedures to implement University Information Security policies and for monitoring compliance.
  http://www.obfs.uillinois.edu/manual/central_p/sec19-5.htm#cc