Application Integration Connection Requirements

Apllication Integration IDs Accessing Restricted Data

Context:

The implementation of value added systems (local data stores) maintained outside of the enterprise data stores introduces additional risks to Cornell data. The focus of this document is on those value added systems that query data from the enterprise data stores and subsequently provide local storage and querying functions for this set of data. Common solutions include FileMaker and local Oracle instances. This definition does not include the work product or the query of data by an individual for the purpose of local reports.
The set of risks these requirements are trying to address include:

- Lack of central logging
- Delegated security
- Minimum visibility of delivered data
- Delegated authentication and authorization
  To address these risks and others the service owner must meet the following requirements.
  Requirements:

Following is a set of technical and process requirements that must be met and maintained if a local data store is developed to use an Application Integration Account (non-person) ID to access restricted data in an Enterprise Data Store.

1. Annual certification acknowledging requirements and responsibilities
2. A description of data use and application purpose must be included in the request for the Application Integration ID. The Central Data Stewards must approve data access as well as specified use of the data prior to the Application Integration account creation.
3. Application Integration IDs must be tied to only one specific service and must never be reused or shared.
4. The Application Integration ID owner must ensure that there are no confidential data stored or delivered through the developed application.
5. If Student data are retrieved, FERPA protection requirements set forth by the University Registrar must be met. Please review FERPA policy and related FAQ documents at (http://www.policy.cornell.edu/vol4_5.cfm)
6. End user authentication must be performed by the application using the Cornell central authentication infrastructure where possible. If integration into the central authentication infrastructure is not possible, local authentication is permissible provided a unique user ID and password are provisioned for each user.
7. Service owners must ensure access is granted to data only which the user is authorized
8. The application or database infrastructure must meet the security requirements specified in University Policy 5.10 Information Security of Institutional Data (http://www.cit.cornell.edu/security/requirements/secreqs-baseline.html)
9. Local audit logs must be retained for six months
10. Audit logs must contain:
    - Date and time of access
    - NetID of end user accessing the database
    - IP address of end user accessing the database
11. The Application Integraion ID Owner must request termination of the ID when use of the ID is no longer needed.
12. If access needs change and additional tables are needed, the ID owner must obtain appropriate Data Steward approval for the new table access.