Data Governance: EIS Internal Policy

ROWAN UNIVERSITY POLICY

Title: Data Governance: EIS Policies & Procedures
Subject: Information Resources and Technology
Policy No: IRT:2014:02
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer:
Adopted: 01/01/2014
Amended:
Last Revision: 12/30/14

I. PURPOSE

This policy is intended to cover any Enterprise Information Services (EIS) for which a separate, approved EIS policy does not exist. All EIS-specific use policies must be consistent with this EIS policy. Additional rules and regulations may be adopted by academic and administrative units to meet specific administrative or academic needs. Such additional requirements must be in compliance with applicable federal and state laws, any contractual agreements with the University and its Vendors, and this policy.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer shall implement this policy and executives and managers throughout the University shall ensure compliance with this policy.

III. APPLICABILITY

1. This policy applies to all members of the Rowan community who seek to acquire, develop, manage, or use services Enterprise Information Services. It also applies to any contractors, vendors, or service providers, who may access, host, receive, transmit, or otherwise use Rowan's EIS data.
2. For the purposes of this policy, EIS is defined as:
    a. Enterprise Information Services is responsible for providing critical enterprise software services, applications and support to enable administrative and academic functions to operate effectively, efficiently and securely..

IV. DEFINITIONS

1. Information Resources and Technology (IRT) – the Rowan University department responsible for the governance of all information and technology.
2. *FERPA* - The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects students' privacy by prohibiting disclosure of education records without adult consent.
3. *Managing Unit* – The Rowan University academic or administrative representative, department or division vested with the day-to-day operations of EIS.

V. POLICY

1. Security of Rowan University's Banner Systems

2. Internal and external auditors routinely examine access to and security of Rowan's Banner ERP system, based upon industry standards and other appropriate means of evaluation. Issues, if any, are identified and recommendations for changes / improvements are presented to the Audit Committee of the Rowan University Board of Trustees (BOT). Upon adoption by the BOT, recommendations become mandates for action. Follow-up reviews are made by the auditors to determine if compliance is achieved and maintained.
3. All mandates issued are complied with or the Audit Committee of the BOT is informed of any such lingering deficiency by the auditors.
4. Oracle and Ellucian product security are in-built to protect data integrity.
5. Audit trails are maintained by Enterprise Information Services staff, and within Banner, for all user accounts created, the privileges granted each account (i.e., what the user can view and / or update), and any changes made to such privileges for an account.
6. Requests for creation of user accounts are routed to the office / functional area which are the steward for the information (e.g., Registrar for student records information; Human Resources for personnel data; Finance / Controller for financial data).
7. EIS security staff may create accounts only upon receipt of requests from the approval-awarding-office and only for the privileges specified. A security audit log is updated daily with all of the transactions that took place that day.
8. If questions should arise about access to a particular system or by a specific user (account) to a specific system, in a given time frame, the Data Base Administrators can run audits and produce access reports.

    a. All EIS staff is FERPA trained and violations of confidentially of data, student or other, is not tolerated. Major disciplinary action is invoked should such occur, including immediate termination of employment. (FERPA training is required of all University personnel; non-compliers or violators are expected to be dealt with appropriately by their supervisors.)
    b. Senior university administrators and Information Resource Technology unit managers – including EIS managers have no "special access" privileges.
    c. Typically the only access accorded such managers is limited to self-service for employees, for access to their personal HR type data. Department heads also have access to their department' s budget data in Finance and when departmental time entry is undertaken, a manager must have Banner INB access to handle time approval. (For example, Jim Henderson and Anne Pinder have Banner HR INB access, for the very limited purpose of reviewing and approving EIS employee timesheets that are entered for Payroll via departmental time entry; as a department head, Henderson also has Finance INB and self-service to view the EIS budget information)

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer