Roger Williams University

Colleague ERP System Access and Security

Purpose

The purpose of this policy is to ensure the security, confidentiality, and appropriate use of all associated data which is processed, stored, maintained, or transmitted in conjunction with the university's enterprise resource planning ("ERP") system known as Colleague. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental.

Scope

The Colleague ERP Access and Security Policy applies to all individuals who have access to campus computer systems and networks, including but not limited to all university employees and student-employees, who are, during the normal course of their employment with RWU, granted access to personal information (examples of personal information include a full name, social security number, driver's license number, email address, date and place of birth, etc.) as defined in the university's Written Information Security Plan (WISP). It applies not only to stored information but also to the use of the various computer systems and programs used to generate or access data, the computers that run those programs including workstations to which the data has been downloaded, and the monitors and printed documents that display data. Users shall keep all such information contained in Colleague confidential except as required to perform authorized job duties.

Access will be limited to that necessary to perform an individual's job functions as specifically authorized by an individual's supervisor, and in the case of undergraduate student-employees, by the divisional Vice President. In addition to the information outlined herein, the confidentiality, use and release of electronic data are further governed by established college/university policies and federal and state laws, including (but not limited to) the following:

- Federal Education Rights and Privacy Act (FERPA)
- Rhode Island Identity Theft Protection Act of 2015
- RWU Student Catalog
- RWU Student Handbook
- RWU Student Code of Conduct
- Information Technology Policies and Procedures, including the Acceptable Use Policy

This policy addresses security and access associated with the Colleague ERP System as defined within this document and does not revise, void, or supersede in any way the duties and obligations of the aforementioned laws, regulations, and policies.

Definitions

Colleague Data: Any data that resides on, is transmitted to, or extracted from any Colleague system, including databases or database tables/views, file systems and directories, and forms.

Colleague Security Administrator: An IT professional position in the Office of Information Technology Services responsible for processing approved requests.

Colleague System: Finance, Financial Aid, Human Resources, Student, and any other interfaces to these systems.

Data Custodians: Data Custodians are responsible for determining who should have access to data within their institutional jurisdiction, and the nature and extent of any authorized access privileges. Responsibilities for implementing security measures may be delegated, though accountability remains with the institutional owner of the data. Additionally, Data Custodians oversee data management functions related to the capture, maintenance, and dissemination of data for a particular operational area.

Areas of Responsibility and corresponding Data Custodians:

Admissions

- Associate Vice President for Enrollment Management
- Director of Graduate Admission
- Assistant Dean of Admission School of Law
- Director of Admissions and Student Enrollment University College

Student System

- University Registrar
- Registrar and Director of Student Finance School of Law

Student Financial Aid

- Director of Financial Aid

Human Resources System

- Assistant Vice President of Human Resources

Accounts Receivable & Cash Receipts

- University Bursar & Registrar and Director of Student Finance School of Law

Finance, Purchasing, Vendors, Payroll

- Vice President for Accounting and Treasury Management

Advancement, Alumni, Development, Major Prospects & Parents

- Vice President for Institutional Advancement

Data Users: Data Users are individuals who access Colleague data in order to perform their assigned duties.

Query access: Access enabling the user to view but not update Colleague data.

Maintenance access: Access enabling the user to both view and update Colleague data. This access is limited to users directly responsible for the collection and maintenance of data.

Data Administration

By law and university policy, certain data is confidential and may not be released without proper authorization. Users must adhere to any applicable federal and state laws as well as university policies and procedures concerning storage, retention, use, release, and destruction of data.

All Colleague data, whether maintained in the central database or captured by other data systems, including personal computers, remains the property of RWU and is covered by all university data policies. Access to and use of data should be approved only for legitimate RWU business and/or academic purposes.

Data Custodians are responsible for ensuring a secure office environment in regard to all Colleague data. Division/department heads will review the Colleague data access needs of their staff as it pertains to their job functions before requesting access via the Colleague Access Request Form.

Colleague data (regardless of how collected or maintained) will only be shared among those employees who have and maintain a demonstrated job-related need to access it.

Any system incident, negligence, abuse, breach of security access, misuse, or compromise of data, or attempt to access any administrative computing system outside of the administrative office's area of supervision for any reason will result in the immediate termination of the employee's access authorization and may result in disciplinary sanction.

Access to Colleague Data

Below are the requirements and limitations for all university divisions/departments to follow in obtaining permission for access to Colleague data.

The Data Custodian must request access authorization for each user (active employees, temporary employees, graduate student employees) under their supervision by completing and submitting a Colleague Access Request Form. Each user is required to sign this request to acknowledge their understanding of, and agreement to comply with, the security and access policies of the university. The appropriate Data Custodian(s) will review the request and either approve or deny it. The Data Custodian and user's supervisor are responsible for assuring that the level of access requested is consistent with each user's job responsibilities and sufficient for the user to effectively perform their duties. Approved requests will be forwarded to the Colleague Security Administrator for processing. Under no circumstances will access be granted without approval of the appropriate Data Custodian(s).

Student Employee Access to Colleague Data

Information Technology policy states that individuals categorized as active undergraduate students of the college are prohibited from direct logon access to the administrative data systems on the administrative portion of the network. Administrative data systems include the Colleague Enterprise Reporting Planning (ERP), RogerCentral (Ellucian's Self-service Application), Safety & Security (T2 System), Student Life/Housing (Adirondack), Student Life/Judicial Affairs (Maxient), Library (OCLC), Dining Services (Cbord), Bookstore(Barnes & Noble), Events (25 Live), Card Access (Safe/QuantumSecure), Outlook/O365, etc. These systems (and any new IT supported system in the future) require greater data security and system security controls and protections.

Active graduate student employees who sign a confidentiality / nondisclosure agreement may obtain access to the Colleague ERP system as long as authorization is granted by the division / department head.

The RWU IT Administrative Services Department establishes logon control measures to implement this policy in accordance with other IT policies, such as the RWU Acceptable Use Policy. Other IT departments design and establish positive application logon access control measures implementing this policy complimenting the multi-layer security posture. Exceptions to this policy are authorized on a case-by-case basis, but must be closely monitored by IT and the Division(s) requesting an exception.

RWU employs students as student-employees in many administrative offices; therefore increasing the demand for access to administrative data systems. In order to permit efficient access and to prevent security breaches, such as an employee using their logon for students, the following procedures are authorized as an Exception to this policy:

- Upon authorization from the relevant divisional Vice President, an RWU Data Custodian who seeks access for the student employee can request an exception of policy from the Information Technology Department by submitting an IT Helpdesk request for each named student employee.
- Exception will only be granted upon a demonstration by the sponsoring requestor that there exists a critical need for access by the student employee, will be limited to those systems for which access is a job-related necessity, and will be granted only for the period of time that the student actually works in the department's office, and cannot exceed the end of academic term. All access will be promptly deleted at end of term, or sooner at the discretion of the university.
- Exceptions cannot be transferred to another office if the student-employee transfers. Exceptions cannot cover more than one office; a second request must be submitted if the student works in two or more administrative offices.
- Summer employment and winter break by RWU students is assumed to be a new academic term for this policy. **Note:** Students from other colleges, schools, or temporary employees working for the summer will be treated as casual employees, not covered under this policy, and therefore ineligible for such exception-based access.
- Undergraduate students will sign the standard Colleague Confidentiality Statement prior to access.

All requests approved for a term, or period of time, will automatically end at close of business on the last day of the academic term, and IT will immediately remove student logon access to all administrative data systems.

Any system incident, negligence, abuse, breach of security access, misuse, or compromise of data, or attempt to access any administrative computing system outside of the administrative office's area of supervision for any reason will result in the immediate termination of the student employee's access authorization and may result in disciplinary action.

To request an exception for student access to administrative systems, please contact the MediaTech Helpdesk at mediatech@rwu.edu or 401-254-6363.

Secured Access to Data

Colleague security classifications are established based upon job function. Specific capabilities will be assigned to each security classification. Each user will be assigned a security classification.

Some users may be assigned several classifications depending on specific needs identified by their division/department head and approved by the Data Custodian(s).

The use of generic accounts is prohibited for any use that could contain protected data.

Each functional area has a clearly defined set of Colleague security classifications that is readily available for review and stored in a location that is available to said area, as well as appropriate systems management staff. Each area reviews the definition of their classes at least annually, and at the time of a system upgrade, to guarantee definitions are still appropriate, and that newly delivered forms are assigned to appropriate classes. Each functional area is required to review and sign off on their Colleague security classes each year.

Twice a year, data custodians will receive from an Information Technology department official a printed report of all users who currently have access to some portion of their data along with the roles assigned. Data Custodians are REQUIRED to review this information, sign off, and return this to the Information Technology department official to keep on file. It is the responsibility of the Data Custodian to verify that each user is still employed and has not changed positions within the university.

Changes are typically fairly limited, as the termination protocol should capture these changes immediately. Failure to return this documentation may result in user account terminations.

Employee supervisors in conjunction with the Data Custodians are responsible for ensuring that each Colleague user is familiar with and understands this policy. User accounts are assigned by the Information Technology department to authorized users after the submission of a complete Colleague access application form. Colleague training is provided by each department as needed and required.

Colleague users will not share their access codes with anyone. If it is found that access codes have been shared, any user involved may be subject to disciplinary action.

All Colleague information must be treated as confidential. Public or “directory” information is subject to restriction on an individual basis. Unless your job involves the release of information and you have been trained in that function, any requests for disclosure of information, especially outside the university, should be referred to the appropriate office.

Colleague System Access and Security
Policy Revised September 2019