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.

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-employee, 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 Coc22c0T0 Tgd nfo (ft)10 (ml)7(sde)13i10 (P)2(t H)f ohno (ftlsde)1o (ftg13 ((nti)
  document and does not revise, void or supersede in any way the duties and obligations of the aforemen
  laws, regulations and policies.

– 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.

– An IT professional position in the Office of Information Technology Services responsible for processing approved requests.

– Finance, Financial Aid, Human Resources, Student, and any other interfaces to these systems.

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

– Access enabling the user to view but not update Colleague data.

– 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.

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

Note: Students of 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.

e. Undergraduate students will sign the standard Colleague Confidentiality Statement prior to access.

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

5. 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 sanction.

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 reviewsal(5 (v)3aff)-4 ((s)2 (av)3.1 (a-4 (in)-4 (i)10 (t)-4 (io)8.1 (n)-4 (o)8(f 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 k (se)-0.9(p)-4 (o)8(n)-4 (f)6 (il4 ((s.)3