Information Security Policy

Introduction

The purpose of the is policy is to protect Rider University information resources from accidental or intentional unauthorized access, modification, or damage and comply with applicable state and federal regulations.

Rider University faculty and staff are expected to be familiar this policy. If you need assistance in understanding or implementing this policy, the Office of Information Technologies staff can assist you. You can request assistance by e-mailing helpdesk@rider.edu or by calling (609) 219-3000.

Policy Statement

Rider University is committed to maintaining appropriate protection of all confidential and sensitive information in our custody. Some information in our custody is protected by state and federal laws or contractual obligations that prohibit its unauthorized use or disclosure.

The exposure of sensitive or protected information to unauthorized individuals could cause irreparable harm to the University or members of our community. An exposure could also subject the University to fines or government sanctions. Additionally, if University information were tampered with or made unavailable, it could adversely impact the University’s ability to do business. Therefore the University requires that all employees diligently protect University information based on its Data Sensitivity Level.

All University employees and contractors are responsible for ensuring that they comply with applicable laws and regulations regarding the protection of confidential information. In addition, beyond strict legal compliance, employees and contractors are also expected to respect confidential and sensitive data and to view and use it only as required by their job.

Administrative department heads are responsible for keeping current with the information security policies and procedures implemented at the University and ensuring their employees understand the Data Sensitivity Level of the information they work with. Information Custodians partnered with OIT will assist departments with achieving and maintaining information security compliance. They are also a good source of information if you have questions regarding the data in their areas of responsibility.

In addition to complying with the policy requirements defined for all employees, contractors, and department heads above, those who manage vendor contracts or on-site computing and network environments that capture, store, process and/or transmit University information are responsible for ensuring that the requirements for confidentiality, integrity, and access are satisfied.
Introduction

The purpose of the is policy is to protect Rider University information resources from accidental or intentional unauthorized access, modification, or damage and comply with applicable state and federal regulations.

Rider University faculty and staff are expected to be familiar this policy. If you need assistance in understanding or implementing this policy, the Office of Information Technologies staff can assist you. You can request assistance by e-mailing helpdesk@rider.edu or by calling (609) 219-3000.

Policy Statement

Rider University is committed to maintaining appropriate protection of all confidential and sensitive information in our custody. Some information in our custody is protected by state and federal laws or contractual obligations that prohibit its unauthorized use or disclosure.

The exposure of sensitive or protected information to unauthorized individuals could cause irreparable harm to the University or members of our community. An exposure could also subject the University to fines or government sanctions. Additionally, if University information were tampered with or made unavailable, it could adversely impact the University’s ability to do business. Therefore the University requires that all employees diligently protect University information based on its Data Sensitivity Level.

All University employees and contractors are responsible for ensuring that they comply with applicable laws and regulations regarding the protection of confidential information. In addition, beyond strict legal compliance, employees and contractors are also expected to respect confidential and sensitive data and to view and use it only as required by their job.

Administrative department heads are responsible for keeping current with the information security policies and procedures implemented at the University and ensuring their employees understand the Data Sensitivity Level of the information they work with. Information Custodians partnered with OIT will assist departments with achieving and maintaining information security compliance. They are also a good source of information if you have questions regarding the data in their areas of responsibility.

In addition to complying with the policy requirements defined for all employees, contractors, and department heads above, those who manage vendor contracts or onsite computing and network environments that capture, store, process and/or transmit University information are responsible for ensuring that the requirements for confidentiality, integrity, and access are satisfied.
Data Sensitivity Levels

Data captured, stored, processed or transmitted by the University is classified into the following three sensitivity levels:

- Legally Protected
- Need to Know
- Public

Legally protected

A variety of state and federal laws impose requirements with respect to the protection of certain types of information. The following laws apply to Rider University:

The New Jersey Identity Theft Law defines “personally identifiable information” or PII as Name in conjunction with any of the following:

- Social Security number
- Bank Account number
- Credit or Debit Card number
- Driver’s License number or other state issued ID number

This law imposes strict requirements for maintaining the confidentiality of personally identifiable information (PII), and triggers significant requirements in the event of a possible breach of personal information.

In addition to the information legally protected by the New Jersey Identify Theft laws, the University also classifies the following information as legally protected:

- Date of birth,
- Place of birth,
- Mother’s maiden name,
- Bank account numbers,
- Income tax records.

This additional information should not be collected, stored or used except in situations where there is legitimate business need and no reasonable alternative.

Managers must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize the risk of loss or theft of this information. Access to such information may only be granted to authorized individuals on a need to know basis by an Information Custodian.
Data Sensitivity Levels

Data captured, stored, processed or transmitted by the University is classified into the following three sensitivity levels:

● Legally Protected
● Need to Know
● Public

Legally protected

A variety of state and federal laws impose requirements with respect to the protection of certain types of information. The following laws apply to Rider University:

The New Jersey Identity Theft Law defines "personally identifiable information" or PII as Name in conjunction with any of the following:

● Social Security number
● Bank Account number
● Credit or Debit Card number
● Driver's License number or other state issued ID number

This law imposes strict requirements for maintaining the confidentiality of personally identifiable information (PII), and triggers significant requirements in the event of a possible breach of personal information.

In addition to the information legally protected by the New Jersey Identify Theft laws, the University also classifies the following information as legally protected:

● Date of birth,
● Place of birth,
● Mother’s maiden name,
● Bank account numbers,
● Income tax records.

This additional information should not be collected, stored or used except in situations where there is legitimate business need and no reasonable alternative.

Managers must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize the risk of loss or theft of this information. Access to such information may only be granted to authorized individuals on a need to know basis by an Information Custodian.
Family Education Rights and Privacy Act of 1974 (FERPA)

FERPA imposes limitations on the use of student educational records, generally restricting disclosure to those faculty and staff with a legitimate need to access it. Education records are defined as records, files, documents, and other materials that contain information directly related to a student and are maintained by Rider or by a person acting for the University. Education records take many forms, including paper and electronic. Examples of educational records include:

- Grades and transcripts
- Student course schedules
- Papers and tests
- Student disciplinary records
- Student financial records
- Personally identifiable information such as social security number, age, parent's name
- Payroll records for employees who are employed as a direct result of the student status (e.g. work study or resident assistant).

Gramm-Leach-Bliley Act of 2000 (GLB)

GLB protects personal financial information that is not public. Examples of financial information in which GLB protections apply include:

- Federal Perkins student loans
- Other student loans where Rider University is the lender
- The federal direct PLUS loan program
- Financial or tax advice to prospective donors

Health Information Portability and Accountability Act of 1996 (HIPAA)

All personal health information of university employees is protected, including insurance policy numbers.

Legally Protected information should only be accessible to, and used by university employees who need it to perform their job responsibilities and who understand the legal constraints on the use of and access to such information.

Need to Know

Need to Know information is information you have access to only because of your employment status and such information must be treated as confidential and should not be discussed or disclosed to others except as required to perform your job duties. Examples of Need to Know information include:

- Employee information: salary data, staff performance data, termination/disability data, non-salary related benefits, biographical information, ethnicity, and grievance/harassment allegations or cases.
FERPA imposes limitations on the use of student educational records, generally restricting disclosure to those faculty and staff with a legitimate need to access it. Education records are defined as records, files, documents, and other materials that contain information directly related to a student and are maintained by Rider or by a person acting for the University. Education records take many forms, including paper and electronic. Examples of educational records include:

- Grades and transcripts
- Student course schedules
- Papers and tests
- Student disciplinary records
- Student financial records
- Personally identifiable information such as social security number, age, parent's name
- Payroll records for employees who are employed as a direct result of the student status (e.g. work study or resident assistant).

**Gramm-Leach-Bliley Act of 2000 (GLB)**

GLB protects personal financial information that is not public. Examples of financial information in which GLB protections apply include:

- Federal Perkins student loans
- Other student loans where Rider University is the lender
- The federal direct PLUS loan program
- Financial or tax advice to prospective donors

**Health Information Portability and Accountability Act of 1996 (HIPAA)**

All personal health information of university employees is protected, including insurance policy numbers.

Legally Protected information should only be accessible to, and used by university employees who need it to perform their job responsibilities and who understand the legal constraints on the use of and access to such information.

**Need to Know**

Need to Know information is information you have access to only because of your employment status and such information must be treated as confidential and should not be discussed or disclosed to others except as required to perform your job duties. Examples of Need to Know information include:

- Employee information: salary data, staff performance data, termination/disability data,
non-salary related benefits, biographical information, ethnicity, and grievance/harassment allegations or cases.
• Faculty Research Data - research projects, whether grant funded or not, often contain confidential and sensitive data, such as personal information about human subject, data subject to confidentiality agreements specific to a particular grant, and financial data regarding use of University research funds.

• Student and applicant data including financial aid data, student accounts receivable data, student grade data, admission application data such as scores, recommendations and personal essays, student athlete evaluations.

• Alumni and Friends data including gift and pledge data, financial data, employment data, biographical data.

• Employee home addresses, home phone numbers, pictures, BroncID (Banner and Campus ID cards).

• Student home and on campus address, phone numbers, pictures, BroncID (Banner and Campus ID cards).

• Nonpublic financial information of the University.

Employees and students have the option of including personal information such as their addresses and phone numbers, contributions to the University or information in campus publications such as alumni magazine, employee or student directories, etc. That voluntarily disclosed data does not constitute Need to Know information, but employees should not disclose such information unless they have confirmed it is publicly available. If in doubt, do not disclose.

Public

Public information may be released to the public without the person’s consent. Examples of public information are:

• Employee directory information: University address, phone number, title, and department.

• Student directory information: Rider University identifies the following as Directory Information under FERPA, except where a student has expressly withheld consent to its release: name, university assigned email address, major, extra-curricular activities, height and weight of members of athletic teams, dates of attendance, degrees, honors and awards, other schools attended.

• Other: press releases, posted college events, college maps, newsletters, newspapers, University Form 990 tax return.

• Data accessible through the Rider University public web site.

Information Custodians

Information Custodians are responsible for managing a set of university information (e.g., medical records, employee benefit data, payroll data, student academic records, alumni information, financial records) wherever it is located, in a manner that is consistent with applicable federal and state laws. Information Custodians are typically the head of a department most closely associated with the information. For example, the Associate Vice President for Human Resources is the Information Custodian for all employee information. The Registrar is the Information Custodian for all student academic information. Information Custodians are responsible for:

• Faculty Research Data - research projects, whether grant funded or not, often contain
confidential and sensitive data, such as personal information about human subject, data subject to confidentiality agreements specific to a particular grant, and financial data regarding use of University research funds.

- Student and applicant data including financial aid data, student accounts receivable data, student grade data, admission application data such as scores, recommendations and personal essays, student athlete evaluations.
- Alumni and Friends data including gift and pledge data, financial data, employment data, biographical data.
- Employee home addresses, home phone numbers, pictures, BroncID (Banner and Campus ID cards).
- Student home and on campus address, phone numbers, pictures, BroncID (Banner and Campus ID cards).
- Nonpublic financial information of the University.

Employees and students have the option of including personal information such as their addresses and phone numbers, contributions to the University or information in campus publications such as alumni magazine, employee or student directories, etc. That voluntarily disclosed data does not constitute Need to Know information, but employees should not disclose such information unless they have confirmed it is publicly available. If in doubt, do not disclose.

Public

Public information may be released to the public without the person's consent. Examples of public information are:

- Employee directory information: University address, phone number, title, and department.

- Student directory information: Rider University identifies the following as Directory Information under FERPA, except where a student has expressly withheld consent to its release: name, university assigned email address, major, extra-curricular activities, height and weight of members of athletic teams, dates of attendance, degrees, honors and awards, other schools attended.

- Other: press releases, posted college events, college maps, newsletters, newspapers, University Form 990 tax return.

- Data accessible through the Rider University public web site.

Information Custodians

Information Custodians are responsible for managing a set of university information
(e.g., medical records, employee benefit data, payroll data, student academic records, alumni information, financial records) wherever it is located, in a manner that is consistent with applicable federal and state laws. Information Custodians are typically the head of a department most closely associated with the information. For example, the Associate Vice President for Human Resources is the Information Custodian for all employee information. The Registrar is the Information Custodian for all student academic information. Information Custodians are responsible for:
● Defining the information sets relevant to this policy.

● Communicating the level of protection that is expected to all employees who are authorized to access the information set.

● Granting access to information by role and name.

● Working with department heads and chairs to determine what job functions are authorized to access the information in a set and in what manner (e.g., who can view only, who can update the information).

● An Information Custodian may designate one or more individuals on his or her staff to perform the above duties however; the Information Custodian retains ultimate responsibility for their actions.

### Information Custodian Contact Information

<table>
<thead>
<tr>
<th>Information Set</th>
<th>Department or Office</th>
<th>Information Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee information, current and job applicants</td>
<td>Human Resources</td>
<td>Rob Stoto</td>
</tr>
<tr>
<td>Payroll information</td>
<td>Disbursements</td>
<td>Debbie Farris</td>
</tr>
<tr>
<td>Admissions applicant information</td>
<td>Enrollment Management</td>
<td>Jen Therien</td>
</tr>
<tr>
<td>Student academic information</td>
<td>Registrar’s Office</td>
<td>Sue Stefanick</td>
</tr>
<tr>
<td>Student biographic/demographic information</td>
<td>Student Affairs</td>
<td>Jan Friedman-Krupnick</td>
</tr>
<tr>
<td>Financial information</td>
<td>Finance Office</td>
<td>Jennifer Potter</td>
</tr>
<tr>
<td>Student loan information</td>
<td>Financial Aid</td>
<td>Drew Aromondo</td>
</tr>
<tr>
<td>Physical building security</td>
<td>Facilities</td>
<td>Mike Reca</td>
</tr>
<tr>
<td>Technology infrastructure and system security</td>
<td>Office of Information</td>
<td>Carol Kondrach</td>
</tr>
<tr>
<td></td>
<td>Technologies</td>
<td></td>
</tr>
<tr>
<td>Alumni information</td>
<td>Advancement</td>
<td>Melissa Anderson</td>
</tr>
<tr>
<td>Legal issues</td>
<td>Vice President for Finance</td>
<td>Julie Kars</td>
</tr>
</tbody>
</table>

### Responsibility of Administrative Department Heads

Each department head is responsible for ensuring the appropriate protection of information within his or her office. These responsibilities include:

● Ensure that everyone in the office is aware of the Data Sensitivity Level of the information they have access to and how that information should be secured.

● Annually review who needs access to what information and only authorize access to information when the job responsibilities require it. Work with Information Custodians to audit and grant access accordingly in administrative information systems (e.g., Banner).

● Maintain an inventory of all confidential information that is collected and maintained by the department, including digital storage, paper storage, and workflows.

● Securely delete or redact all confidential information that is not necessary for the department to collect, maintain, or use and that is not required to be maintained by law.
- Communicating the level of protection that is expected to all employees who are authorized to access the information set.
- Granting access to information by role and name.
- Working with department heads and chairs to determine what job functions are authorized to access the information in a set and in what manner (e.g., who can view only, who can update the information).
- An Information Custodian may designate one or more individuals on his or her staff to perform the above duties however; the Information Custodian retains ultimate responsibility for their actions.

**Information Custodian Contact Information**

**Information Set Department or Office Information Custodian Employee information, current and job applicants**

Human Resources Rob Stoto
Payroll information Disbursements Debbie Farris Admissions applicant information
Enrollment Management Jen Therien Student academic information Registrar’s Office
Sue Stefanick Student biographic/demographic information (including health information)

Student Affairs Jan Friedman-Krupnick

Financial information Finance Office Jennifer Potter Student loan information Financial Aid Drew Aromondo Physical building security Facilities Mike Reca Technology infrastructure and system security

Office of Information Technologies
Carol Kondrach
Alumni information Advancement Melissa Anderson Legal issues Vice President for Finance Julie Karns

**Responsibility of Administrative Department Heads**

Each department head is responsible for ensuring the appropriate protection of information within his or her office. These responsibilities include:
- Ensure that everyone in the office is aware of the Data Sensitivity Level of the information they have access to and how that information should be secured.
- Annually review who needs access to what information and only authorize access to information when the job responsibilities require it. Work with Information Custodians to audit and grant access accordingly in administrative information systems (e.g., Banner).
● Maintain an inventory of all confidential information that is collected and maintained by the department, including digital storage, paper storage, and workflows.

● Securely delete or redact all confidential information that is not necessary for the department to collect, maintain, or use and that is not required to be maintained by law.
• Personally owned computers and devices used to access Legally Protected or Need to Know information are subject to the same rules and security requirements that apply to University-owned computers.

• Do not store Legally Protected or Need to Know information on laptops or portable/mobile storage devices unless they have been encrypted by OIT and there is no other reasonable alternative.

• Determine if Legally Protected or Need to Know information must be on laptops or can be stored exclusively on university approved network and cloud document storage repositories (G:, H:, X:, or Google Drive).

• Have all contracts reviewed and signed by the Vice President for Finance and Treasurer who will ensure that vendors are also compliant with our policies.

• Instruct employees to report possible information breaches, including lost or stolen computing or mobile devices to the department head who in turn will report it to the Associate Vice President for Finance and Controller or the Associate Vice President for Information Technologies.

Responsibility of all Employees

• Ensuring the confidentiality of any information she or he collects or uses, both electronic and on paper.

• Understanding what information is Legally Protected and how such information should be secured.

• Ensuring that no Legally Protected information is on a laptop or other mobile or portable storage device unless it is encrypted. OIT can help determine if such information is present.

• Securely deleting or redacting all confidential information that is not necessary to collect, maintain, use, or archive.

• Reviewing all research projects, whether grant funded or not, to make sure required confidential information is secure. Storing data on university approved network and cloud storage repositories (G:, H:, X:, or Google Drive) when possible.

• Reporting all possible data breaches including lost or stolen computing or mobile devices to supervisor or academic dean who in turn will report it to the Associate Vice President for Finance and Controller or the Associate Vice President for Information Technologies.

• Personally owned computers and devices used to access Legally Protected or Need
to Know information are subject to the same rules and security requirements that apply to University-owned computers.

- Do not store Legally Protected or Need to Know information on laptops or portable/mobile storage devices unless they have been encrypted by OIT and there is no other reasonable alternative.

- Determine if Legally Protected or Need to Know information must be on laptops or can be stored exclusively on university approved network and cloud document storage repositories (G:, H:, X:, or Google Drive).

- Have all contracts reviewed and signed by the Vice President for Finance and Treasurer who will ensure that vendors are also compliant with our policies.

- Instruct employees to report possible information breaches, including lost or stolen computing or mobile devices to the department head who in turn will report it to the Associate Vice President for Finance and Controller or the Associate Vice President for Information Technologies.

Responsibility of all Employees

- Ensuring the confidentiality of any information she or he collects or uses, both electronic and on paper.

- Understanding what information is Legally Protected and how such information should be secured.

- Ensuring that no Legally Protected information is on a laptop or other mobile or portable storage device unless it is encrypted. OIT can help determine if such information is present.

- Securely deleting or redacting all confidential information that is not necessary to collect, maintain, use, or archive.

- Reviewing all research projects, whether grant funded or not, to make sure required confidential information is secure. Storing data on university approved network and cloud storage repositories (G:, H:, X:, or Google Drive) when possible.

- Reporting all possible data breaches including lost or stolen computing or mobile devices to supervisor or academic dean who in turn will report it to the Associate Vice President for Finance and Controller or the Associate Vice President for Information Technologies.