Contents

Section 1: Overview and Purpose of this Policy ................................................................. 2
Section 2: Policy Approval and Review ............................................................................. 4
Section 3: General Acceptable Use Policy ........................................................................ 5
Section 4: Data Management ............................................................................................ 6
Section 5: Access Policies ................................................................................................ 10
Section 6: Electronic Communications ............................................................................. 13
Section 7: Telecommunications ....................................................................................... 18
Section 8: Physical Security .............................................................................................. 20
Section 9: Security Incident Procedures .......................................................................... 22
Section 10: Appeal Process ............................................................................................... 23
Section 11: Data Export Regulations ................................................................................. 23
Section 12: Equipment Disposal ...................................................................................... 23
Appendix A. Definitions .................................................................................................. 24
Section 1: Overview and Purpose of this Policy

1.1 Overview

RHIT supports freedom of expression and an open environment for intellectual and scholarly activity. The contents of the RHIT computer and communications systems must comply with Institute policy and may also be governed by legal, contractual, and financial considerations.

This document is not meant to be a comprehensive list of what is allowed and not allowed, but a guide to ensure that computing resources are used ethically and responsibly within the school community and that the data residing within these resources is secured. Effective security is a team effort involving the participation and support of all RHIT authorized users. It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

This document should be considered a living document. Changes will be made as new questions and situations arise to insure that the document continues to appropriately address its purposes. Those purposes include:

- To protect and ensure the integrity and privacy of Institute information
- To protect the Institute from litigation
- To operate within government guidelines and applicable state and federal laws
- To outline procedures for the flow and access of data
- To define acceptable use of systems and Institute data

The Institute’s Information Security Officer shall be the primary contact to initiate interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it, if the need arises. Any issues concerning law shall be referred to the Institute’s Legal Counsel.

1.2 Other Institute Policies

This document refers to the following independently established RHIT policies and is not intended to supersede them.

Specific references are made to these policies throughout the document. The links may change from time to time.

- Policy for Responsible Use of Rose-Hulman Computing Facilities (primarily for students but applicable to all)
  http://www.rose-hulman.edu/TSC/policies/computer_use
- Annual Computer Use Policy—Acknowledgement Form (for faculty and staff)
- Account Password Policy
  http://www.rose-hulman.edu/HR/Policies/Password_Policy_Final_08312007.pdf
• Mobile Devices Policy
  http://www.rose-hulman.edu/Users/groups/AdminSvcs/html/purchasing/Cell%20Phones.htm

• Equipment Disposal Policy found in the purchasing guide.
  www.rose-hulman.edu/Users/groups/AdminSvcs/html/purchasing/Purchasing%20Guide_FIN
  AL%204012006.doc

• Intellectual Property Policy
  http://www.rose-hulman.edu/HR/Policies/index.html

• Faculty hand book policies
  o Computer utilization policy - section 5.02
    https://www.rose-hulman.edu/Users/groups/AcademicAffairs/facultyhandbook/#Sec_Five_Computer_Utilization
  o Professional Development Activities and Testing - section 5.10
    https://www.rose-hulman.edu/Users/groups/AcademicAffairs/facultyhandbook/#Sec_Five_Prof_Develop_Activities
Section 2: Policy Approval and Review

The initial policy and any subsequent proposed adjustments to the policy shall be submitted to the Enterprise Computing Team (ECT) for review, comments and preliminary approval, with final approval being granted by the President. The policy and any material subsequent adjustments to the policy will be presented for informational purposes to the Audit Committee of the Board of Trustees.
Section 3: General Acceptable Use Policy

3.1 General Policies

RHIT is committed to protecting its stored information from illegal or damaging actions by individuals, either knowingly or unknowingly.

RHIT provided computer systems, including but not limited to: computer equipment, software, storage media, network accounts, e-mail accounts, websites, and smartphones, are the property of Rose-Hulman Institute of Technology. Rose-Hulman is the owner of some of the data on this system and has a responsibility to protect the privacy and security of this data. Except as provided in the Responsible Use document (See Section 1.2), these systems are to be used for institutional purposes in serving the interests of our Institute community.

The Institute strives to maintain an environment free of harassment. The Institute, therefore, prohibits the use of computing and electronic communication equipment in ways that are disruptive or offensive to others.

3.2 Legal Considerations

RHIT is not responsible for any loss or damage to anyone’s personal property including hardware, software or property of a mixed nature as a result of the use of the RHIT computer facilities. RHIT resources are primarily for institutional purposes.

3.3 Unacceptable Use

Please refer to the Policy for Responsible use of Rose-Hulman Computing Facilities referenced in Section 1.2. This policy is primarily directed at students.

3.4 Consequences of Misuse of Computing Resources

Please refer to the “Computer Use Policy” referenced in Section 1.2. All employees are required to review and sign this policy yearly.
Section 4: Data Management

A summary of some common examples of data management situations including ownership, stewardship requirements, and governing policy is given in a Table 4.3 at the end of the section.

4.1 Storage of Copyrighted Material on RHIT Digital Devices

Please refer to the “Computer Use Policy”, noted in the reference table in Section 1.2. All employees are required to review and sign this policy yearly.

4.2 Information Handling

4.2.1 Care and Handling of External Information

External information is defined as any information collected, purchased, or given by a source outside the Institute. Many times this information comes with copyright or confidentiality agreements that dictate how the information is used.

The Institute will adhere to any such agreements accompanying this information.

4.2.2 Care and Handling of Internal Information Internal Information is defined as any information collected and maintained by the Institute. Normally, RHIT is the owner of this information, except as provided by the Intellectual Property Policy in the Faculty Handbook (see Section 1.2). Any data stewards of this information will be designated as needed.

The Banner enterprise resource planning suite is an integrated, inter-departmental suite of applications on a single database where much of the Institute's information is stored. Access to the Banner system, and the information it contains, is authorized by the area Vice President of the maintained data.

4.2.3 Requests for Access to Information

Requests for information (reports, labels, etc.) should be verified with a member of the Administrative Computing Experts (ACE) group responsible for maintaining the information. It is the responsibility of the requesting department responsible for the information to verify it will be used in accordance with FERPA and HIPPA guidelines or any other federal or state guidelines and Institute policies.
4.2.4 Request for Access to Banner Forms and Tables

Requests for access to the Banner Forms or the Oracle tables should be requested from the appropriate member of the Administrative Computing Technical Experts (ACTS) group or designee who is the data steward responsible for the data integrity and security of the information.

4.2.5 Legal Issues

FERPA:
The Family Educational Rights and Privacy Act (FERPA) is a federal law protecting the privacy of student education records. RHIT considers student records private information, belonging to the student. The Institute must have written permission from the eligible student to release any information from a student’s record. Although efforts are made to ensure that the Institute is educated in the FERPA requirements it is the responsibility of the employee to ensure they are following the guidelines set forth by FERPA and should refer any inquiries to the Institute Registrar’s Office.

HIPAA:
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) authorized the development of security and privacy standards to protect healthcare information that is stored electronically. These standards cover processing, storage, and transmission of health information to prevent unauthorized or inadvertent use or disclosure of an individual’s health information. Although efforts are made to ensure that the Institute is educated in the HIPPA requirements it is the responsibility of the employee to ensure they are following the guidelines set forth by HIPPA and should refer any inquiries to the Institute’s Office of Human Resources.

4.3 Data Misuse

Data misuse is defined as using Institute-owned or Institute protected data (either unintentionally or deliberately) in a manner inconsistent with Institute policy, or federal, state, or local laws. Examples of data misuse include:

- Obtaining or attempting to obtain access to data not within the scope of one’s Institute responsibilities or authorized access
- Downloading or exporting centrally held information (limited access, not intended for public) into non-approved databases (as specified by the data steward) or personally owned equipment
- Using Institute data for personal benefit
- Releasing information in an inappropriate manner
- Using information inaccurately, conflicting with published, sanctioned Institute information and/or statistics
4.3 Common examples of data management situations

The table below illustrates some common situations at RHIT involving digital information: where it is kept, who owns it, who is expected to keep it secure and control access, and relevant policy, law, and agreements governing access to the data. The table is not comprehensive, but is intended to give guidance on common situations. Enterprise Information Technology (EIT) has a responsibility for providing secure networks and systems to enable data stewards to control access. However, data stewards, and in many cases, faculty and staff, have specific responsibilities to protect data. These responsibilities are independent of who owns the data. The responsibilities include following account policies such as password policies, ensuring adequate protection for data on mobile devices, and using secure transmission and storage of data. Finally the table is merely a guideline; specific situations may have additional relevant factors.

Table 4.3

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Location</th>
<th>Owner of Data</th>
<th>Stewardship Responsibility</th>
<th>Relevant Policy, Law or Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel Records and Financial records</td>
<td>Banner</td>
<td>RHIT</td>
<td>Designated Employees and data managers</td>
<td>HIPAA and relevant state and federal law.</td>
</tr>
<tr>
<td>Student Records</td>
<td>Banner</td>
<td>RHIT</td>
<td>Registrar, designated employees and data managers</td>
<td>FERPA</td>
</tr>
<tr>
<td>Student Records e.g. grades</td>
<td>Moodle, Faculty computers mobile or fixed</td>
<td>RHIT</td>
<td>Registrar other designated employees</td>
<td>FERPA</td>
</tr>
<tr>
<td>Student Work</td>
<td>Moodle, Faculty computers mobile or fixed</td>
<td>creators</td>
<td>faculty</td>
<td>FERPA</td>
</tr>
<tr>
<td>Externally supplied data</td>
<td>Various secure network locations</td>
<td>usually the external agency</td>
<td>RHIT point of contact with agency and others using the data</td>
<td>Agreement with external agency</td>
</tr>
<tr>
<td>Curriculum materials</td>
<td>Moodle, faculty computer mobile or fixed</td>
<td>Creators</td>
<td>Creators</td>
<td>Intellectual Property Policy</td>
</tr>
<tr>
<td>Scholarly Works, and supporting Data</td>
<td>RHIT servers, faculty laptops</td>
<td>Creators</td>
<td>Creators</td>
<td>Intellectual Property Policy</td>
</tr>
</tbody>
</table>
Table 4.3 continued

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Location</th>
<th>Owner of Data</th>
<th>Stewardship Responsibility</th>
<th>Relevant Policy, Law or Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>RHIT servers, employee desktops and mobile computers and devices</td>
<td>Varies, often the vendor.</td>
<td>RHIT</td>
<td>Vendor license, Responsible Computer Use Policy, Faculty-Staff Annual Computer Use Policy Acknowledgement</td>
</tr>
<tr>
<td>Email</td>
<td>RHIT servers and computers</td>
<td>Varies</td>
<td>Varies</td>
<td>Federal and state law, Policy for Responsible use of Rose-Hulman Computing Facilities</td>
</tr>
<tr>
<td>Personal files not created in the course of an employee’s duties</td>
<td>RHIT servers and computers</td>
<td>Varies</td>
<td>Varies</td>
<td>Federal and state law, Policy for Responsible use of Rose-Hulman Computing Facilities</td>
</tr>
<tr>
<td>Public RHIT websites</td>
<td>RHIT servers</td>
<td>RHIT</td>
<td>Data managers</td>
<td>Federal and state law, Policy for Responsible use of Rose-Hulman Computing Facilities</td>
</tr>
<tr>
<td>Secure RHIT websites</td>
<td>RHIT servers</td>
<td>Usually RHIT</td>
<td>Data managers</td>
<td>Federal and state law, Policy for Responsible use of Rose-Hulman</td>
</tr>
</tbody>
</table>
Section 5: Access Policies

5.1 Username and Password Policies – Refer to EIT website (http://www.rose-hulman.edu/eit) for any questions regarding the Account Password Policy referenced in Section 1.2

5.1.1 Employee and Authorized User Responsibilities:

Authorized Users will be assigned a RHIT or Individual Department account that allows use of certain RHIT computing resources. Accounts will be designated by a username (User ID) and protected by a confidential password known only to the authorized user.

User authorization is granted for students by the Registrar’s office and is granted by Human Resources for all other accounts.

Authorized Users are required to enter their username and password in order to use RHIT computing resources.

Passwords expire every 365 days. Users will be reminded to change their password 14 days in advance. Users will continue to be reminded each day until the password is changed. If users do not change their password by the end of this time, the account will be locked and they will not be able to log in until a password administrator unlocks it.

If a password is entered incorrectly three times in a row, the account will be locked and the user will not be able to log on until the lockout expires, or it is unlocked by a password administrator.

Authorized Users should avoid writing their password where it is not protected. If they must do so, they are responsible for ensuring that no one else has access to the written password. Users shall never write both the username and password together.

Users are responsible for protecting user identification and passwords. If it is believed that someone else knows a user's password, or is using someone else’s account the password should immediately be changed and the Service Desk notified @ x8989.

Users must not share their password with anyone, or log in and allow another user access to their account. If there is need to grant access to an outside user, that user must follow appropriate procedures to apply for access.

5.1.2 Password Changes and Requirements:

If a password is forgotten or needs to be reset, the request to reset the password must be made to the EIT Service Desk. Passwords will not be sent via mail or email, or given to others.
A password is the key to access most systems on campus. All RHIT Authorized Users are expected to keep ALL passwords private. RHIT security policy sets the following rules when creating a password:

- It must have a minimum of eight (8) characters and a maximum of 127
- It must not contain all or part of the user's account name
- It must contain characters from at least three of the following four categories:
  - English Uppercase characters (A through Z)
  - English Lowercase characters (a through z)
  - At least one number (0-9)
  - Non-alphanumeric characters (example: @, $, #, %, ^)

In addition, it is strongly recommended that:

- It should contain both lower and upper case letters (passwords are case-sensitive)
- It should contain at least one special character (@, #, {, }, $, %, etc.)
- Never use a person’s name or any word that could be found in the dictionary. Breaking up words with special characters or numbers is an easy way to avoid this.
- Do not use the same passwords for work as you do for personal use

5.2 Supervisor responsibilities

Managers and supervisors are responsible for notifying Human Resources when (or before) an employee separates from the Institute or transfers to another department so account access can be revoked or updated as appropriate. Separations from the Institute must be reported to Human Resources immediately upon learning of the separation.

Managers and supervisors are responsible to notify the Office of Business and Finance when authorized users with Banner Fund and Organizations security separates from the Institute or transfers to another department so their access can be removed in Banner.

5.3 Human Resources Responsibility

Human Resource is responsible to notify the Service Desk when someone separates from Rose-Hulman so accounts can be deactivated.

5.4 Business and Finance Responsibility

The Office of Business and Finance is responsible for removing privileges to Banner Funds or Organization Codes when notified of a department change or a separation.

5.5 Guest and Special Access

Occasionally it may be necessary to grant access to computing resources to individuals other than
authorized users of the Institute. Examples of such individuals are consultants, review board members, and volunteers. These special users are authorized users and therefore are subject to the same policies as all users.

5.6 Access Audits

The Information Security Officer may routinely audit access to Institute computing resources and reserves the right to temporarily disable questionable access. Department Heads and or Vice Presidents or their appointed designees are responsible for periodically reviewing access to their information and must notify EIT if access should be revoked or levels changed.
Section 6: Electronic Communications

Users should be aware that Institute electronic resources and facilities, including communications such as electronic mail, are not necessarily secure or private.

6.1 Permissible Uses of Electronic Communications Facilities

Electronic communication facilities are intended to be used primarily for official Institute business, including employee and student academic pursuits, and employee administrative, personnel and/or business matters. However, reasonable use of Institute-owned or operated electronic communication facilities for non-commercial personal purposes is permitted if it does not entail any additional cost to the Institute, interfere with the completion of job responsibilities, impede network operations, or violate Institute policies, including, but not limited to this Policy. Should users make use of the electronic communication facilities to transmit personal messages, such messages shall not be treated with a higher standard of privacy than any other electronic communication. The Institute reserves the right to place additional restrictions on the personal use of its electronic communication facilities if necessary to conserve network resources for Institute purposes. Further, those using the Institute’s electronic communication facilities must use such facilities in a responsible and lawful manner. Unlawful use of electronic communication facilities or use of such facilities which violates any Institute policy, including this policy, by any user, as determined by appropriate Institute officials, will be cause for the Institute to deny such user further access to such facilities and may be cause for other Institute disciplinary action, up to and including termination from employment or expulsion. The disciplinary actions shall follow the standard disciplinary procedures.

Consistent with this Policy, users may use the electronic communication facilities to initiate or receive electronic communication. Users should only use their own files, those that have been designated as "public" files, or those that have been made available to them with the knowledge and consent of the owner.

Users shall always keep all copyrighted and trademark notices intact on Institute or third-party materials that are received or disseminated in electronic communication. The Institute Librarian shall be consulted if there is any question about the form of such notice.

6.2 Prohibited Uses of Institute Electronic Communications Facilities

6.2.1 Commercial Purposes

Electronic communication facilities shall not be used for commercial purposes unrelated to the business of the Institute or for any commercial purpose that has not been expressly authorized in writing by the Institute.
6.2.2 Other Prohibited Uses and Restrictions

Electronic communication facilities shall not be used to access or transmit electronic communication which promote or contain unlawful content. This prohibition shall not apply to educational and professional work that requires such access or transmission.

Electronic communication facilities should not be used to transmit, copy, or store confidential information, except as authorized by Institute officials. Further, all users must exercise a great deal of caution in transmitting and storing confidential information due to the ease with which electronic communication may be reproduced, stored and/or redistributed. Users should be particularly cautious in using distribution lists if confidential information is being transmitted.

Electronic communication facilities should not be used in any way that may infringe upon the rights of the holder of any copyright or trademark. Downloading, copying or installing software or other data that is subject to copyright, trademark or other legal protection without appropriate authorization or license is prohibited. Enterprise Information Technology staff will not knowingly provide support for software that a user possesses in violation of the applicable license agreement. EIT staff may ask for proof of ownership before helping users with their software. EIT staff will not knowingly allow infringing copies or otherwise unauthorized copies of software to be installed on electronic communications facilities and will remove any such suspect software loaded onto electronic communication facilities. Employees and students of RHIT are required to observe and abide by copyright and trademark laws. The Institute Librarian should be consulted whenever an employee or student is unsure of relevant restrictions and limitations.

Except as permitted by section 6.1, electronic communication facilities shall not be used in any manner that: is contrary to the Institute's interests; attempts to obscure, withhold or falsify the identity of the sender; impairs the electronic communication facilities in any way; attempts to gain access to the electronic communication of third parties (unless expressly authorized by such third party or by the Institute); interferes with, interrupts or obstructs the ability of others to use such facilities; is not related to the performance of an employee's job responsibilities or a student's academic work; and/or is not otherwise authorized by the Institute.

Electronic communication facilities shall not be used in violation of Institute policies or local, state or federal laws, rules or regulations. Users shall not abuse or vandalize any electronic communication facilities. Users are to immediately report any observed or suspected instances of abuse or vandalizing of electronic communication facilities to Institute officials.
6.2.3 Security/Breach of Security

Although the Institute uses various methods in an effort to secure its electronic communication facilities, the Institute cannot guarantee such security. Electronic communication and electronic communication facilities shall not be used to breach the electronic security of others. A breach of security includes, but is not limited to: any unauthorized attempt to compromise any electronic communication facility, including the use of network privileges, accounts, access codes, identifiers or passwords, or equipment; knowing and unauthorized interception, access, disclosure, disruption, damage, destruction or unauthorized alteration/modification of any electronic information, or electronic communication facilities, including software or hardware; and any unauthorized and intentional disruption or interference with others' use of electronic communication facilities.

Users of electronic communication facilities are responsible for protecting their personal account information and/or password. Any user holding a personal account and its password is, at all times, responsible for its use and all activity originating from that account or using that password. Any unauthorized attempt to determine the passwords or personal account information of others is strictly prohibited.

6.2.4 Privacy

In general, email and other forms of electronic communication are not encrypted in transit, especially once the communication leaves the Institute network and computing facilities. Therefore, the Institute cannot guarantee the privacy of electronic communications, and users should not expect that their use of electronic communication facilities will be private. Users who further encrypt an electronic communication must furnish the encryption key or software to the Institute upon request of the Information Security Officer so that the Institute may fulfill its obligations under federal and state law.

6.3 Monitoring and Disclosure

6.3.1 Overview

The Institute reserves the right to monitor or disclose the content of any electronic communication sent, received or stored using Institute-owned electronic communication facilities. Monitoring, investigation, and examination of electronic content will only be conducted in connection with a specific event, such as the delivery of a warrant for search and seizure or other permissible events as listed in the Policy. Computer Administrators are not permitted to engage in the monitoring, investigation, or examination of electronic communication content without prior specific authorization of the Institute Information Security Officer as specifically permitted under the Policy. Computer Administrators do regularly monitor the performance of the Institute’s computing resources, and the Institute reserves the right to install or update files on any Institute-owned computer to assure the performance or security of the computing environment. Use of the electronic
communication facilities shall be deemed to constitute consent to allow the Institute to exercise its rights outlined in this Policy and agreement to abide by this Policy.
6.3.2 Circumstances

As the owner or operator of electronic communication facilities and a private institution of higher education, the Institute will monitor or disclose the content of the electronic communication of users only under the following circumstances:

- A party to the communication consents; or
- The communication is readily accessible to the public (examples include, but are not limited to, web pages, e-mails sent to a public mailing list, or a newsgroup post); or
- The Institute has an administrative need to access an e-mail, voice mail or other electronic communication or electronic communication facilities (examples include routine maintenance, backup of data, monitoring of usage patterns, troubleshooting or investigation of an excessive use of network resources that adversely affects performance or protection of the Institute’s rights or property); or
- The Institute is furnished with reasonable information causing it to conduct a review or investigation of any electronic communication or the use of electronic communication facilities (examples include reports or evidence of hacking, identity theft, harassment, commercial card fraud). The Institute has sole discretion to conduct such a review or investigation under this Policy; or
- The monitoring or disclosure occurs as a result of the Institute's obligations under local, state and/or federal laws, rules or regulations.

Note: The Institute maintains extensive logs of system activity, user activity, etc. These logs may be used for diagnostics or forensics when authorized by the Information Security Officer.
Section 7: Telecommunications

The purpose of this section is to ensure a secure method of connectivity between RHIT and all users with access to RHIT systems and information using mobile and remote computing devices. This applies to any mobile and remote computing device connected to RHIT’s system or used to conduct Institute business (laptops, smartphones, etc.).

7.1 Land-line Phone Usage

Authorized Users of RHIT may be provided land-line phones. Users of Institute land-line phones should remember that phone conversations can be recorded, monitored and retrieved, if required, as allowed by law.

7.2 Mobile and Remote Computing

Authorized Users of RHIT may be provided cell phones and/or cellular enabled devices or given a stipend for their personal devices in conjunction with conducting Institute business, both on and off campus. Users of these devices should remember that business information and data is often stored, retrieved and transmitted via airwaves, and without appropriate securities (encryption and passwords) in place, may be susceptible to unauthorized use by others outside the campus community.

Authorized Users are required to follow the same Information Technology Security Policies and Procedures as outlined in this document for all wireless or portable devices.

Smartphones and other mobile devices are not considered secure computing devices. One of these devices in the wrong hands can do considerable damage to the RHIT network if the data is not protected. Any mobile device that syncs with a RHIT computer or system contains information that could be used to compromise our network. It is highly likely that a mobile device contains confidential RHIT information in the form of email correspondence, documents, or other files. It is the responsibility of the user to ensure that information stored on a mobile device is protected as required by applicable state and federal laws such as FERPA and HIPAA. Users must provide proof of the following security provisions before the device will be synchronized with RHIT systems.

These devices can receive and transmit emails, documents, files, addresses/phone numbers, pictures and directory information. All Users of these devices must comply with the Institute’s Mobile Device Policy.

Users are encouraged to adopt the following habits for an enhanced security posture:

- Store highly sensitive information on the Institute network storage systems rather than on local storage devices. Additionally, sensitive information should be encrypted.

- Exercise extreme caution when using mobile devices in environments which are not secure when off-campus.
• “Remote wipe” capabilities are available for lost or stolen Institute provided cellular enabled device.

• Under no circumstances should PINs or RHIT passwords be stored unencrypted on a Smartphone or other mobile device. Power-on passwords for accessing information stored on the mobile device must be enabled.

7.3 Responsibility to Protect Data:

Users must be aware that RHIT has a responsibility to protect the security and privacy of certain types of information being synchronized from the RHIT network. This responsibility is independent of who owns the data. This information includes, but is not limited to: email correspondence, documents, spreadsheets, PowerPoint presentations, as well as institute owned data such as student, personnel and financial records. Confidential and highly sensitive information should never be stored on a mobile device.
Section 8: Physical Security

8.1 Purpose

The purpose of this section is to outline the minimum physical security expected for computing facilities and all computing equipment and digital devices.

8.2 Classes of Data

In order to understand how physical security procedures may vary according to the data being protected it is useful to classify data by physical location and sensitivity. See also Table 4.3 for different security situations.

By Location

Network Data
Stored only on a secure network in various data archives
- Banner database
- Moodle database (student grades, and submitted work)
- Applicant data (People Admin)
- Departmental data bases (applicant data, personnel records, corporate data)
- Committee records (e.g. Dept. Heads SharePoint archive)

RHIIT Internet data (www. rose-hulman.edu and other Institute owned domains)
- Committee records e.g. Curriculum Committee

Mobile data
- Laptop drives
- Smartphones
- USB drives
- CDROMs and DVDs
- External Hard Drives

By sensitivity

- Sensitive: Including but not limited to medical, personnel and official student records, budget and accounting data, applicant data, committee/departmental records (such as minutes, ABET data) of a confidential, corporate nature. Some curriculum materials such as exams.
- Not sensitive: certain curriculum materials, public websites.

8.3 Office/Workstation/Laptop/Tablet Security

All users shall be responsible for maintaining the security of their assigned workstation. Required security provisions include locking or logging off when not in use, and preventing
unauthorized physical access to unattended systems.

Users are encouraged to adopt the following habits for an enhanced security posture:

- Automatic screen saver and screen lock.
- Lock offices/rooms containing computers or mobile devices when not occupied for extended periods of time.
- Ensure all virus protection software is enabled and up-to-date.
- Ensure all Windows updates are installed.
- Store sensitive information on the Institute network storage systems rather than on local or mobile storage devices.
- Alternatively, sensitive information on mobile devices can be encrypted.
Section 9: Security Incident Procedures

9.1 Security Incident Definition

A security incident is defined as any act that violates an explicit security policy as Institute policies referenced from this document. Violations may include events having actual or potential adverse effects which compromise an aspect of computer, network or user resources, including but not limited to: loss of confidentiality of information; a compromise of the integrity of information; misuse of service, systems or information; damage to systems and damage or loss of property or information.

9.2 Security Incidents

- “Data Exposure” – Lost laptop, Institute issued cell phone, stipend reimbursed personal device, thumb drive, smartphone, or any other device containing confidential information.
- Files containing confidential information exposed to the internet or other persons not privy to Institute information.

9.3 Employee/Student Response

NOTE: For all instances when confidential information is or “may be” compromised the Information Security Officer and the CIO is to be notified immediately.

Service Desk and/or Public Safety (in the case of lost or stolen equipment) should be notified immediately with the following information:

- Date and time of incident
- Type of incident and any other pertinent details that would assist in verifying incident (i.e. confidential data exposed, password exposed, etc.)
- A statement describing the impact on users, department or the network including the number of users/departments affected.
- Contact information of submitter
Section 10: Appeal Process

Refer to the Faculty, Staff and Student Handbook Appeals Processes. Area Vice Presidents should guide the appeals process.

Section 11: Data Export Regulations

Refer to the Policy as outlined on the Government Website: http://www.export.gov/regulation/index.asp

Section 12: Equipment Disposal

The purpose of this policy is intended to ensure accountability and to remain in compliance with licensing agreements for proper disposal of any equipment that contains Rose-Hulman licensed software or Institute data.

Refer to the Equipment Disposal Policy listed in Section 1.2

- All licensed software must be removed from the equipment prior to the disposal of the equipment. Licenses are only valid for equipment while being used for Rose-Hulman purposes. This will be done by EIT. Contact the Service Desk @ X8989 to make these arrangements.

- All Institutional data must be removed from the equipment prior to disposal. This will be done by EIT. Contact the Service Desk @ X8989 to make these arrangements.

- Disposal of equipment includes donations, purchases and any other method where the equipment will not be owned, leased or provided for by Rose-Hulman.

- This equipment includes phones, laptop computers, desktop computers, USB drives, smartphones, tablets or any other device that contains any Rose-Hulman licensed software or Institute data.

- Recommend wiping of hard drives
Appendix A. Definitions

A.1 Indiana Code Definition of Personal Information

Under Indiana Code 24-4.9, "Personal Information" is defined as follows:

- a Social Security number that is not encrypted or redacted; or
- an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:
  - A driver's license number.
  - A state identification card number.

Source: House Enrolled Act No. 1101

A.2 Dictionary

ACE- Administrative Computing Experts- ace@rose-hulman.edu

This is a group consisting of Banner users throughout the Institute community whose responsibilities include:

- Include ACTS members and other key campus end-users
- Intended to be a comprehensive user group that will discuss upcoming initiatives
- Provide feedback on Banner/administrative computing
- Disseminate information to their respective departments
- Form task forces to address interdepartmental issues.

ACTS- Administrative Computing Technical Support – AdministrativeComputingTechnicalSupport@rose-hulman.edu

This is a group consisting of individuals selected by the Cabinet whose responsibilities include:

- Project prioritization and implementation
- Data stewardship
- Business process analysis
- Quality assurance and software testing
- Training support
**Authorized User:** a RHIT employee, student, or other individual affiliated with the school that has been granted authorization to use a specific electronic resource.

**Backup:** To create a copy of critical files to minimize the loss of data in the event of a system failure.

**Chief Information Officer (CIO):** Chief Information Officer – the Head of the Information Technology Department. At Rose-Hulman it is the Vice-President of Information Technology is also the CIO.

**Computer Administrators:** A Computer Administrator is a user who manages and maintains a computer. The computer administrator makes system-wide changes to the computer, including installing programs and accessing all files on the computer, allocating disk storage space, adding and configuring new workstations, and can create, change and delete the accounts of other users. The computer administrator may also perform systems programmer activities.

**Confidential Information:** See “Personal Information”

**Electronic Communications:** Electronic communications include, but are not limited to, the World Wide Web, Internet-based discussion groups, electronic bulletin board and forum systems, electronic mail, telephony services (wired and wireless telephone, voice mail, and facsimile services) or any other type of wireless transmission. Users must adhere to this Policy when using (a) the Institute's Internet connection, (b) the Institute’s internal networks, (c) the Institute’s connection to the public telephone system, and (d) Institute-owned equipment. Electronic communications include any and all information, graphics, audio, video, multimedia, or data stored, transmitted, or received by electronic systems.

**Electronic Resource:** Material in digital format which requires a digital device for use.

**Email:** Electronic Mail. Electronic messages sent from one person to another via electronic communication systems.

**Employee:** A person hired by RHIT, who receives wages or salary.

**Encryption:** A security method used to transform data from its original form into a difficult to interpret format, in order to prevent any but the intended recipient from reading the data.

**Firewall:** An access control device that acts as a barrier between two or more segments of a computer network, used to protect internal networks from unauthorized users or processes of other networks.

**Service Desk:** Central point of contact within IAIT to which customers of Rose-Hulman computing and telephone services may report issues, problems, suggestions and concerns for resolution.

**EIT:** The Institute department responsible for the purchasing, management, and support of all
computer, network, and telecommunications systems that are the property of RHIT.

**Information Security Officer (ISO):** Employee of Rose-Hulman assigned to interpret, enforce and monitor this policy and to resolve problems concerning it.

**Internet:** Global system of interconnected computers and computer networks. The computers and networks are owned and maintained separately by a host of organizations, government agencies, companies, and colleges and exist outside the USF network.

**Intranet:** A private network for communication and information that is only accessible to authorized users within the Institute.

**Institutional Purposes:** Broadly defined as legitimate items directly related to the mission of the Institute.

**Logon:** see “Username”

**Mobile Devices:** A mobile device (also known as cell phone devices, handheld device, handheld computer, "Palmtop" or simply handheld) is a pocket-sized computing device, typically having a display screen with touch input or a miniature keyboard.

**Non-Approved Databases:** Any form in which data is stored that does not meet the security requirements outlined in this policy. This could be a spreadsheet, Access database of information stored on an unsecured server.

**Password:** A string of characters known only to the user that serves as authentication of a person’s identity. Passwords may be used to grant, or deny, access to information or resources. Access to systems or information is usually granted by a combination of Username and Password.

**Personal Information:** Information related to a person’s private life or concerns, recorded in any form, by which individuals can be identified. Personal information can include: name, address, telephone number, race, ethnic origin, religious or political beliefs, bank account numbers, or social security numbers *(Refer to A.1 of this Appendix)*

**Personal Files:** Any type of record, document, or file that is of a personal nature and does not relate to the Institute or Institute business.

**Privileged Information:** Information confined to an exclusive or chosen group of users. Privileged information is not considered common knowledge, or has not been cleared for release to others outside the group.

**Reasonable Efforts:** Efforts based on known statements, events, or conditions. Reasonable efforts are defined as being within common sense, known best practices, or logical actions.
Remote Access: The ability to obtain access to an IT resource or the RHIT network from a location other than the physical campus of the Institute located at 5500 Wabash Ave. Terre Haute, IN.

RHIT: Rose-Hulman Institute of Technology

Security: Measures taken as to ensure a reliable computing platform free from the risk of loss.

Server: A system or computer program that provides information or services to other programs or devices.

Smart Phone: A mobile phone offering advanced capabilities, often with PC-like functionality

Spam: Unauthorized and/or unsolicited mass electronic mailings.

Student: Person who is enrolled for study, as their primary role, at RHIT

System Administrator: An individual responsible for maintaining a multi-user computer system, including a local-area network (LAN). Typical duties include:

- Adding and configuring new workstations
- Setting up user accounts
- Installing system-wide software
- Performing procedures to prevent the spread of viruses
- Allocating mass storage space

The system administrator is sometimes called sysadmin or the systems administrator. Small organizations may have just one system administrator, whereas larger enterprises usually have a team of system administrators.

User: Any individual who uses, logs in, attempts to use, or attempts to log into a system, whether by direct connection (modem or network) or across one or more networks.

User ID: see “Username”

Username: Also referred to as “logon” or “User ID”. A unique string of characters used to identify a specific user in a multi-user environment. Access to systems or information is usually granted by a combination of Username and Password.

Virtual Private Network (VPN): a private data network established within or across a public network that utilizes various security methods to transfer information

Wireless Network: A network utilizing radio waves to transmit data, as opposed to physical wired connection.