Information Security Policy – vol. 1.0
BR 9/10
Location: Employee Handbook, Policy Manual, WASC CPR document

Information Security Policy and Guidelines

Policy
Rudolf Steiner College (College) is committed to information security. Information security is defined as protection of data, applications, networks, and computer systems from unauthorized access, alteration, or destruction. This information security policy establishes the framework for the information security program that has been authorized by the President and Executive Committee of the College. This Policy applies to all personnel who use the College's systems of data gathering and retention. All personnel who use any aspect of the College's data system are expected to follow the guidelines of this policy. All users of the College's IT resources are responsible for adhering to all legal and ethical requirements in accordance with the policies of the College and applicable law.

Calendar of the Policy

The Policy will be regularly updated as needed and disseminated to all who are affected by changes in the policy. As the College grows and adds more offsite (off main campus) activities, this policy could be subject to change. Changes could affect one or more sites and as such, each site could have guidelines unique to that site. The Controller/CFO is charged with oversight of personnel charged with identifying and developing information security policies for all College activities.

Purpose of the Policy The purposes of the information security program and this information security policy
are:

- To establish a College-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of College data and computer systems.
- To define mechanisms that protect the reputation and integrity of the College and allow the College to satisfy its legal and ethical responsibilities with regard to its computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this Policy.

This Policy contains elements that intersect with other policies of the College. Should there be questions as to which policy should be followed; clarifications should be addressed to the Executive Committee.

Personnel Charged with <u>Assuring</u> Compliance with Policy as charged with Supervision or functional oversight of personnel listed in the Management Map of the College.

- Controller/CFO
- Executive Committee Members
- Admissions Officer
- Program Directors

Information Security Policy – vol. 1.0
BR 9/10
Location: Employee Handbook, Policy Manual, WASC CPR document

TABLE OF CONTENTS

DATA CLASSIFICATION AND SECURITY RISK ASSESSMENT

College data (student information, employee information, financial information) **must be classified according to use, sensitivity, and importance** into one of three classification **l**evels. The level of protection should be consistent when the data is replicated and as it flows through the College or to outside sources.

The three data classification levels established by RSC are as follows:

1. **Restricted** - Information for which there are legal requirements preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA or HIPAA, are in this class. Payroll and personnel information are also in this class because of privacy requirements. This Policy recognizes that other data may need to be treated as restricted because it would cause severe damage to the College if disclosed or modified.

2. **Confidential** - Data that would not expose the College to loss or penalty if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure**.**

3. **Public -** Information that may be disseminated freely**.**

RSC data must be protected according to its data classification regardless of the form (i.e., hardcopy such as a printed document, softcopy such as an excel spreadsheet) it is in.

Information security risk assessments will be undertaken to determine areas of vulnerability, classify data, and to identify any remediation necessary to mitigate or reduce the occurrence of any such vulnerability. All data resource users are expected to cooperate fully with any information security risk assessment conducted**,** and are expected to participate in development of any remediation plan. The College must be provided with written assurances from any entity that it enters into an IT business relationship with (consultant, vendor, service) that appropriate levels of information security exist.

ACCESS SECURITY

This Policy recognizes the balance between protecting data and permitting access to those who need to use the data for authorized purposes. Access controls must allow for sufficient levels to enable the appropriate authorized access.

All RSC systems and applications must have an "owner" identified. The "owner" is generally the Director or Dean charged with the responsibility of data associated with his/her job responsibility. The "owner" (herein referred to as data owner) will work to define the appropriate levels of access and will be the sign off on requests for access to the system and/or application. Changes in access or unusual to normal usage must be reported to the Controller/CFO.
All College applications and systems are required to have user accounts with strong passwords that are changed regularly. This includes all vendor-supplied default accounts and administrator accounts; generic accounts should be disabled wherever possible.

The College does not allow the coding of user accounts and passwords into programs or queries.

Authorized resource users must not share user accounts and/or passwords.

Access for terminated data resource users must be disabled immediately upon Termination. Authorization for termination is issued by the Controller/CFO upon notification of supervisor of local data user or group.

Access, for inter-departmental or campus-transferred data resource users, must be reviewed by the supervisors, of their old and new positions, jointly to determine adjustments that need to be made. Increased access is requested of and authorized by the Controller/CFO upon notification of new supervisor.

The Controller/CFO is responsible for informing all those affected of changes in data users permissions.

Supervisors, working with the Controller/CFO are responsible for terminating access to data of all terminated data users.

User access reviews must be periodically conducted by supervisors to ensure that access is on a need to know basis.

Unless authorized or required to do so by law, policy, or regulation, College resource users may not access, copy, print, alter, transmit or destroy anyone else's electronic files without prior express written permission. Simply being able to access a file or other information does not necessarily imply permission to do so.

ACCEPTABLE USE, TRANSMISSION AND COMMUNICATION

All College resource users must abide by the "Acceptable use of computing resources" policy kept by each campus.

Use of the College**'**s network, computer system, application and data resource requires express permission of the data owner, except in situations that require vendor assistance and/or IT personnel to resolve a problem; then the Controller/CFO and/or the local supervisor must provide the appropriate authorization while notifying the data owner.

Automated mechanisms/tools implemented to protect College data and resources must not be disabled.

• Servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with a licensed anti-virus software product that is updated according to the vendor's recommendations. Wherever feasible, the ability to disable the virus scanning mechanism will be removed. Anti-virus software should include malware protection, wherever possible.

• Incoming and outgoing communication, including electronic mail, must be scanned for viruses. Where feasible, system or network administrators should inform users when a virus has been detected.

• Systems connected to the Internet must be current with security patches.

• Connections to the College computer services that contain confidential or restricted data should go through properly-secured channels and data should not be downloaded from a controlled environment (i.e., the "S" Series system) without first undertaking an information security risk assessment to identify and implement any measures that must be undertaken to secure the downloaded data.

The College provides mechanisms, including tools, for communication. The College cannot guarantee security, privacy or confidentiality of email. Nevertheless, the College provides the tools for this communication. The tools for communication are subject to all College policies, including the following:
• Confidential or restricted College data must not be sent via email.
• Restricted and/or confidential data must not be included in public blogs or any other public online forum.
• College's trademarks, logos and any other intellectual property may not be used in

connection with any public blogging activity.

• Data or resource users may not circumvent user authentication mechanisms or security of any application, system or account.

• Data or resource users may not use any program/script/command, or send messages of any kind, with the intent to interfere with, deny service to, or disable a user's terminal session, via any means. The willful introduction of computer viruses or disruptive/destructive programs into**,** or originating from**,** the College environment is prohibited.

• Data or resource users may not disable protection mechanisms (such as workstation passwords) established to protect electronic data.

• Data or resource users may not run or otherwise configure software or hardware to intentionally allow themselves or other individuals to circumvent account privileges and security mechanisms. This includes, but is not limited to**,** intercepting, accessing, printing, transmitting, copying, or decoding passwords or similar access control information, whether by means of using any computer program or device or by deception or observation of other users; and accessing abilities used during a previous position at RSC by using knowledge of a special password, loopholes in computer security systems, another authorized user's password, or any other means.

• Data resource users should avoid working on public workstations when dealing with restricted and/or confidential data (e.g., social security numbers, exams, etc.).

INTELLECTUAL PROPERTY
The College IT resource users are required to abide by all intellectual property, copyright or similar laws or regulations. Plagiarism, in any form, is not acceptable at the College.

The College IT resource users:
• Must follow the established purchasing procedures for ordering and installing software on equipment at their local site. Installing or distributing "pirated" or other software products that are not appropriately licensed for use by the College or authorized by the Controller/CFO for use in actuation of College activities is not acceptable.

• May not copy copyrighted material [in excess of the amount allowed under fair use]. For example, College IT and data resource users may not digitize or distribute images from magazines, books or other copyrighted sources, including copyrighted music, without ensuring that the College or the end user has an active license to make such copies [or that such copies fall within the fair use guidelines. The fair use guidelines call for a weighing of four factors**:** the amount of the work copied, the type of work copied, the purpose of the use, and the impact on the market value of the work. While these guidelines favor non-profit educational use, not all such uses are permitted under the guidelines.]

The College IT and data resource users are responsible for recognizing, attributing and acquiring appropriate permission to use the Intellectual Property of others and for not violating any Intellectual Property Rights, and are prohibited from using, accessing, copying, printing, and storing copyrighted computer programs and other protected or proprietary material, in violation of another's Intellectual Property rights.

• The College IT and data resource users may not export software, technical information, encryption software or technology that violates international or regional export control laws.

Location: Employee Handbook, Policy Manual, WASC CPR document

PORTABLE DEVICES AND REMOTE ACCESS

Portable devices (e.g., flash drives, laptops, CDs, DVDs) may not be used to store restricted or confidential data specifically in an unencrypted state. Exceptions: authorized use of such devices by the Controller/CFO.

Remote access to non-library resources needs to be facilitated in a secure manner consistent with best practice and in accordance with control measures identified during the Information Security Risk Assessment process.

AUDIT TRAILS AND BACKUPS
Audit trails on all devices must be enabled wherever possible**,** and logs should be retained in separate secure locations wherever possible.

• Activities performed as application or system administrator or "superuser" must be logged where it is feasible to do so**,** or documented where they cannot be logged.

• Intrusion tools should be installed where appropriate and intruder detection monitoring must be implemented on all devices containing data classified as confidential and/or restricted.

All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

• Backups of data must be handled with the same security precautions as the data itself.

RETENTION AND DESTRUCTION OF INFORMATION ASSETS
All RSC IT resource users must abide by all laws associated with the retention and destruction of Information Assets.

• Each campus\department must develop and document retention and destruction schedules, and all data resource users should follow the policies set forth by their respective supervised areas for record retention and destruction.

• Printouts containing restricted and/or confidential data (e.g., social security numbers, payroll data, and student grades) are required to be shredded when discarded.

• When systems and/or physical media are disposed of, or repurposed (e.g., transferred to other areas for reuse, donated, resold, etc.), the physical media used to store data that is classified as restricted or confidential should be wiped clean, according to industry standard for the media used, before the media is physically discarded or reused.

SECURITY BREACHES
All suspected computer breaches must be recorded and reported. All College IT resource users are required to cooperate with investigations into suspected computer breaches or security incidents, including those involving law enforcement authorities, when required.
A suspected computer breach or security incident represents the attempted or successful unauthorized access, use, modification, or destruction of information systems or data. If unauthorized access occurs, computer systems could potentially fail, and restricted and/or confidential information could be compromised; thus, it is the College's policy that all suspicious activity must be reported.

Each employee is responsible for reporting a suspected computer breach or security incident to:
• Faculty should report to their local campus Academic Dean and Program Director **and** a copy of the report must be given to the Controller/CFO.

• Non Faculty should report to their Supervisor Manager **and** a copy of the report must be given to the Controller/CFO.
• All College IT resource users are required to inform their immediate supervisor of any security loopholes discovered, and to cooperate in implementing security procedures.
• College IT resource users should not execute any form of network scanning (e.g., port, security).

The Controller/CFO will coordinate with College Counsel and the Executive Committee in reporting computer breaches to law enforcement authorities.

PHYSICAL ACCESS
Unauthorized physical access to RSC computer equipment is prohibited. Therefore:
• College resource users should not undermine physical premises security controls implemented to protect property owned by the College.
• Unauthorized access to the data center or computer labs should not be permitted.
• Data center or lab visitors must sign in, and visitors must be escorted whenever they are given access to the data center or computer labs**.**
• College data and resource users must either carry campus-issued ID while on RSC premises or be identified by an immediate supervisor or faculty member as authorized to be on campus and using equipment.
• College data and resource users must report suspicious activity to the Controller/CFO and Executive Committee.

• College data and resource users must obtain proper authorization from the Executive committee to remove any RSC-owned equipment from the College premises, and present such authorization to authorized personnel of the Executive Committee when it is requested.

WARNING NOTICE
RSC, reserves the right to have members of the Executive Committee and those designated by that group access e-mail, files, history, and other utilization, audit trail, usage and user data or information in order to monitor equipment, systems and network traffic at any time to ensure compliance with this Policy and applicable laws.
Any employee found to have violated this Policy may be subject to disciplinary action, according to their respective faculty, staff or administrative handbooks.

EXCEPTIONS TO POLICY
No exceptions to this Policy will be granted. Individual requests for deviations from this Policy must be made in writing to the Controller/CFO who will consult with the Executive Committee, and, if granted will be granted in writing.