# ROSEDALE TECHNICAL COLLEGE
# Information Security Program

May 15, 2023

## 1. Scope & Objectives

The objectives of this comprehensive written Information Security Program ("ISP") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards Rosedale Technical College has selected to protect the personal information it collects, receives, uses, and maintains. All employees, staff, contractors, and guests of the following locations are expected to comply with this ISP:

Rosedale Technical College, 215 Beecham Drive, Pittsburgh PA 15205
Rosedale Technical College, 170 Bilmar Drive, Pittsburgh, PA 15205

All locations shall protect customer information by adopting and implementing, at a minimum, the security standards, policies, and procedures outlined in this ISP. This ISP outlines the minimum standards for the protection of personal information and each location is encouraged to adopt standards that exceed the requirements outlined in this ISP. This ISP has been developed in accordance with the requirements of all applicable state and federal laws, including, but not limited to, the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (16 C.F.R. §§ 314.l to 314.5). If this ISP conflicts with any legal obligation or other Rosedale Technical College policy or procedure, the provisions of this ISP shall govern. The purpose of this ISP is to:

1. Ensure the security, confidentiality, integrity, and availability of personal information Rosedale Technical College collects, receives, uses, and maintains.

2. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.

3. Protect against unauthorized access to or use of Rosedale Technical College maintained personal information that could result in substantial harm or inconvenience to any customer or employee. Fulfill Rosedale Technical College's obligation to comply with all state and federal regulations, policies, and standards associated with safeguarding customer information.

4. Define an information security program that is appropriate to Rosedale Technical College's size, scope, and business, its available resources, and the amount of personal information that Rosedale Technical College owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

This ISP applies to all employees, contractors, officers, and directors of Rosedale Technical College. It applies to any records that contain personal information in any format and on any media, whether in electronic or paper form.

For purposes of this ISP, "personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer:

1. Identifiers such as a real name, alias, postal address, online identifiers such as Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

2. Customer records, including but not limited to, digital and electronic signatures, telephone numbers, insurance policy numbers, credit and debit card numbers, financial and credit-related information, physical characteristics and descriptions (e.g., government identification), bank account numbers, and medical and health insurance information (in the context of employment).

3. Characteristics of protected classifications under state or federal law.

4. Commercial information, including records of personal property, products or services purchased, obtained,

or considered, or other purchasing or consuming histories or tendencies.

5. Biometric information.
6. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
7. Geolocation data.
8. Audio, electronic, visual, thermal, olfactory, or similar information.
9. Professional or employment-related information.
10. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g, 34 C.F.R. Part 99).
11. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
12. Persistent identifiers that can be used to recognize a consumer or a device that is linked to a consumer, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address, cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

"Personal information" does not include publicly available information, aggregate consumer information, or consumer information that is de-identified. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records.

### 2. Program Coordinator

This ISP and the safeguards it contemplates are implemented and maintained by a single qualified employee or service provider ("Program Coordinator") designated by Rosedale Technical College. The Program Coordinator is responsible for the design, implementation, and maintenance of information safeguards and other responsibilities as outlined in this ISP. The Program Coordinator may delegate or outsource the performance of any function under the ISP as he or she deems necessary from time to time. Rosedale Technical College has designated the following individual as the Program Coordinator:

Rosedale Technical College’s Chief Financial Officer

The Program Coordinator shall be responsible for the following:

- Implementation and maintenance of this ISP, including, but not limited to:
  - Assessing internal and external risks to personal information and maintaining related documentation, including risk assessment reports and remediation steps;
  - Coordinating the development, distribution, and maintenance of information security policies and procedures;
  - Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal information;
  - Ensuring that the safeguards are implemented and maintained to protect personal information throughout Rosedale Technical College where applicable;
  - Overseeing service providers, processors, and third parties that access or maintain personal information on behalf of Rosedale Technical College;
  - Monitoring and testing the ISP's implementation and effectiveness on an ongoing basis through documented risk assessments and other mechanisms;

- Defining and managing incident response procedures; and
- Establishing and managing enforcement policies and procedures for this ISP, in collaboration with Rosedale Technical College legal counsel, human resources department, and upper management.

- Employee, staff, and contractor information security training, including:
  - Providing periodic security awareness and related training regarding this ISP, Rosedale Technical College safeguards, and relevant information security policies and procedures for all employees, staff, and contractors;
  - Ensuring that those employees, staff, and contractors who have been enrolled in training courses have completed and passed the course in a timely manner; and
  - Retaining training completion records.

- Reviewing this ISP at least annually, or whenever there is a material change in Rosedale Technical College business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information.
- Annually reporting to Rosedale Technical College management regarding the status of the information security program and Rosedale Technical College's safeguards to protect personal information.

## 3. Implementation Cycle

Rosedale Technical College utilizes a methodology that establishes information security policies based on periodic and updated risk assessments. Once initial risks are identified and assessed, mitigation controls are documented by the Program Coordinator or his/her designees. Employees are then trained and made aware of their responsibilities for following the proper information safeguards outlined in this document. Each Rosedale Technical College location will then be monitored and tested for its effectiveness at complying with the safeguards by performing updated risk assessments, performed at least annually. The process continues as periodic audits and risk assessments are conducted to identify and evaluate residual risk.

## 4. Risk Assessments

As a part of developing and implementing this ISP, Rosedale Technical College for each location, will conduct and document periodic risk assessments, at least annually, or whenever there is a material change in Rosedale Technical College's business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal information.

The risk assessment shall evaluate:

1. Reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal information;

2. The likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal information; and

3. The sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

   a. Employee, staff, and contractor training and management;
   b. Employee, staff, contractor, service provider, process, and third-party compliance with this ISP and related policies and procedures;
   c. Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and
   d. Rosedale Technical College's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

Following each risk assessment, Rosedale Technical College will:

1. Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;
2. Make available the results of the risk assessment to upper management for review;
3. Reasonably and appropriately mitigate any identified risks or violations of this ISP and document such mitigation in the risk assessment; and
4. Regularly monitor the effectiveness of Rosedale Technical College's safeguards, as specified in this ISP.

## 5. Safeguard Principals

Rosedale Technical College will develop, implement, and maintain reasonable administrative, electronic, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal information that Rosedale Technical College owns, accesses, or maintains on behalf of others. In doing so, Rosedale Technical College will adhere to the following principles:

1. Safeguards shall be appropriate to Rosedale Technical College’s size, scope, and business, its available resources, and the amount of personal information that Rosedale Technical College owns or maintains on behalf of others, while recognizing the need to protect both customer and employee personal information.
2. Rosedale Technical College shall document its administrative, electronic, technical, and physical safeguards (see Section 6 of this ISP).
3. Rosedale Technical College's administrative safeguards shall include, at a minimum:
    a. Designating one or more employees to coordinate the information security program (see Section 2 of this ISP);
    b. Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 3 and 4 of this ISP);
    c. Training employees in security program practices and procedures (with management oversight);
    d. Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7 of this ISP); and
    e. Adjusting the information security program in light of business changes or new circumstances.
4. Rosedale Technical College's electronic and technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, support:
    a. Secure user authentication protocols, including:
        i. Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;
        ii. Restricting access to active users and active user accounts only and preventing terminated employees or contractors from accessing systems or records; and
        iii. Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.
    b. Secure access control measures, including:
        i. Restricting access to records and files containing personal information to those with a need-to- know to perform their duties; and
        ii. Assigning to each individual with computer or network access unique identifiers and passwords (or other

authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.

c. Encryption of all personal information traveling wirelessly or across public networks;

d. Encryption of all personal information stored on laptops or other portable or mobile devices, and to the extent technically feasible, personal information stored on any other device or media (data-at-rest);

e. Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal information or other attacks or system failures;

f. Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal information

g. Current system security software (or a version that can still be supported with reasonably current patches and malicious software ("malware") definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

5. Rosedale Technical College's physical safeguards shall, at a minimum, provide for:

a. Defining and implementing reasonable physical security measures to protect areas where personal information may be accessed, including reasonably restricting physical access and storing records containing personal information in locked facilities, areas, or containers;

b. Preventing, detecting, and responding to intrusions or unauthorized access to personal information, including during or after data collection, transportation, or disposal; and

c. Secure disposal or destruction of personal information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

## 6. Information Security Policies, Procedures & Safeguards

The following policies, procedures, and safeguards reflect Rosedale Technical College's objectives for managing operations and controlling activities related to information security. Additionally, the policies and procedures within this document represent Rosedale Technical College's ongoing efforts in achieving and maintaining internal control over customer information security as well as compliance with state and federal requirements. This section of the ISP outlines minimum requirements and is not meant to be a comprehensive or all-inclusive list. The Program Coordinator shall implement, test, monitor, and enforce all of the policies and procedures covered below:

1. GENERAL SAFEGUARDS

a. Documents with personal information shall not be left unattended on the desk or workspace of any employee. At a minimum, employees shall place any documents containing customer information in a drawer or enclosed container.

b. Customer personal information that is no longer part of an ongoing transaction (e.g., "dead" or "lost" deal documentation) should generally not be retained unless required by law or Rosedale Technical College policy, or unless it is securely stored, such as in a locked drawer or file cabinet.

c. When away from their office, desk, or workspace, employees, staff, and contractors shall either (1) lock their office doors, or (2) utilize lockable storage for any customer personal information. If keys and/or locks are not available, then the workspace shall be cleared of all customer personal information, with no customer personal information left visibly unattended.

d. Files and documents containing personal information that do not need to be retained by state, federal, or internal Rosedale Technical College rules shall be securely destroyed and never placed into a regular trash or recycling bin. This includes mistakenly printed documents (including duplicates), as well as handwritten notes with customer personal information such as names, addresses, emails, and telephone numbers.

e. Printers, fax machines, copiers, and other office equipment shall be located in secure areas that are well monitored. At a minimum, documents should be immediately retrieved when faxed or printed from a remotely located machine.

Under no circumstances should a document be left unattended at an unsecured machine location. Trash bins near copiers, printers, and other office equipment should be inspected for documents containing personal information.

f. Personal information should never be placed in a manner that exposes customer information to unintended individuals. When with a customer, only that customer 's personal information should be visible near the employee's desk or workspace.

g. Credit application interviews, as well any other verbally communicated information involving the collection or disclosure of personal information, shall be conducted in areas secure from eavesdropping. Employees shall not use speakerphones in open areas susceptible to eavesdropping.

h. All new employees should be trained on the basics of customer information security policies, procedures and safeguards outlined in this ISP. This should be conducted during, and incorporated into, the new employee onboarding process. Training shall recur, at a minimum, annually for each employee.

i. All employees shall be granted access to customer information (both physical and electronic) on a need-to-know and least-access basis.

j. Rosedale Technical College shall conduct an inventory of all categories of personal information collected, map to which departments it is shared, the business purposes for which it is shared or disclosed, the categories of third parties and service providers to whom it is shared or disclosed, and the categories of sources from whom it is collected.

## 2. PHYSICAL & ADMINISTRATIVE SAFEGUARDS

a. Rosedale Technical College recognizes that best practices relating to information security are constantly evolving and therefore adopts many of the physical and administrative safeguards outlined in guidance and enforcement actions from the Federal Trade Commission. Accordingly, Rosedale Technical College shall do each of the following:

- Limit Access to Customer Files to Individuals with a Need-to-Know
- Protect File Storage Areas with Locking or Continuous Monitoring
- Ensure Copiers and Office Equipment Are Kept Clear of Personal Information
- Protect File Storage Areas from Destruction and Damage
- Ensure Unattended Computers Are Not Left Unlocked
- Ensure Proper Disposal of Customer Information
- Provide Mechanisms for Secure Disposal of Personal Information
- Ensure Unattended Workspaces Are Kept Clear of Personal Information & Security Credentials
- Keep Safety Standards in Place when Data is Enroute
- Require locking unattended offices and cabinets containing customer information

## 3. ELECTRONIC & TECHNICAL SAFEGUARDS

a. Rosedale Technical College recognizes that best practices relating to information security are constantly evolving and therefore adopts many of the technical safeguards outlined in guidance and enforcement actions from the Federal Trade Commission. Accordingly, Rosedale Technical College shall do each of the following:

- Hold on to Information Only as Long as You Have a Legitimate Business Need
- Use Only Fake or Test Data for Training and Testing Purposes
- Restrict Electronic Access to Sensitive Data to Individuals with a Business Need
- Limit Administrative Access to a Neutral Department or Person
- Require Complex and Unique Passwords
- Ensure User Credentials Are Not Stored in Vulnerable Formats
- Enable MFA for All Systems Containing Non-public Personal Information
- Disable User Accounts After Multiple Unsuccessful Login Attempts
- Encrypt Data at Rest and in Transit

- Use Firewalls to Segment Networks
- Use or Enable Intrusion Detection and Monitoring Tools
- Require Remote Network Access Be Done Through VPN and MFA
- Place Limits on Third-Party Access to Networks and Applications
- Update and Patch Third-Party Software
- Encrypt Data Sent Over Point-of-Sale Devices
- Restrict Downloading of Unauthorized Software
- Encrypt Information Sent Over Wireless Networks
- Ensure Digital Copiers Have Encryption or Overwriting Enabled

**4.** ADOPTION OF SAFEGUARDS UNDER THE CIS CONTROLS FRAMEWORK

a. Rosedale Technical College also adopts the physical, administrative, and technical safeguards outlined in version 8 of the Center for Internet Security (CIS) Controls. Accordingly, Rosedale Technical College shall do each of the following:

- Establish and Maintain Detailed Enterprise Asset Inventory
- Address Unauthorized Assets
- Establish and Maintain a Software Inventory
- Ensure Authorized Software is Currently Supported
- Address Unauthorized Software
- Establish and Maintain a Data Management Process
- Establish and Maintain a Data Inventory
- Configure Data Access Control Lists
- Enforce Data Retention
- Securely Dispose of Data
- Encrypt Data on End-User Devices
- Establish and Maintain a Secure Configuration Process
- Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Configure Automatic Session Locking on Enterprise Assets
- Implement and Manage a Firewall on Servers
- Implement and Manage a Firewall on End-User Devices
- Securely Manage Enterprise Assets and Software
- Manage Default Accounts on Enterprise Assets and Software
- Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
- Establish and Maintain an Inventory of Accounts
- Use Unique Passwords
- Disable Dormant Accounts
- Restrict Administrator Privileges to Dedicated Administrator Accounts
- Establish an Access Granting Process
- Establish an Access Revoking Process
- Require MFA for Externally Exposed Applications
- Require MFA for Remote Network Access
- Require MFA for Administrative Access
- Establish and Maintain a Vulnerability Management Process
- Establish and Maintain a Remediation Process
- Perform Automated Operating System Patch Management

- Perform Automated Application Patch Management
- Establish and Maintain an Audit Log Management Process
- Collect Audit Logs
- Ensure Adequate Audit Log Storage
- Ensure Use of Only Fully Supported Browsers and Email Clients
- Use DNS Filtering Services
- Deploy and Maintain Anti-Malware Software
- Configure Automatic Anti-Malware Signature Updates
- Disable Auto run and Auto play for Removable Media
- Establish and Maintain a Data Recovery Process
- Perform Automated Backups
- Protect Recovery Data
- Establish and Maintain an Isolated Instance of Recovery Data
- Ensure Network Infrastructure is Up to Date
- Establish and Maintain a Security Awareness Program
- Train Workforce Members to Recognize Social Engineering Attacks
- Train Workforce Members on Authentication Best Practices
- Train Workforce on Data Handling Best Practices
- Train Workforce Members on Causes of Unintentional Data Exposure
- Train Workforce Members on Recognizing and Reporting Security Incidents
- Train Workforce on How to Identify and Report if Their Enterprise Assets Are Missing Security Updates
- Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
- Establish and Maintain an Inventory of Service Providers
- Designate Personnel to Manage Incident Handling
- Establish and Maintain Contact Information for Reporting Security Incidents

**5.** RECORD REQUEST & INFORMATION DISCLOSURE POLICIES

a. Only authorized employees shall disclose, share, send, or provide customer personal information to third parties.

b. In general, customer records containing personal information should not be mailed, emailed, texted, faxed, or otherwise transmitted electronically. Whenever possible, employees authorized to provide customer records containing personal information shall require the customer to pick up the records in-person after being required to present a valid government-issued photo identification. If the person cannot reasonably be expected to visit the school, the person's identity must be verified using both of the following methods:

    i. Requesting they fax a copy of a valid government-issued photo identification;

        1. In the event a customer prefers to email or text their license, employees have an obligation to inform the customer that Rosedale Technical College DOES NOT endorse, recommend or request sensitive information be sent via email. Furthermore, employees are prohibited from accepting such information in the form of a text, whether on a company or personal phone. A customer who insists on sending information via email should be informed of the risks of sending information over an unencrypted network and that faxing or providing in-person are safer alternatives.

    ii. Requesting the person's full name and at least two other identifiers such as date of birth, address, phone

number, last four digits of Social Security Number, or email address.

c. Rosedale Technical College personnel handling record requests have an obligation to securely destroy and shred customer information obtained in the process of verifying a customer's identity (e.g. shredding a faxed government-issued photo ID).

d. In no event may documents containing sensitive customer information (e.g., financial information, Social Security Number, credit information, and identification cards) be mailed or electronically transmitted. Customers must retrieve such documents from the school in-person after presenting a valid government- issued photo identification.

e. In general, customer records containing personal information should not be provided to unaffiliated third parties (e.g., vendors, manufacturers, and financial institutions) unless doing so is (1) required by law, (2) required to process a transaction initiated or requested by the consumer or (3) pursuant to a valid subpoena.

f. Special rules under state and federal laws govern the disclosure of information related to victims or potential victims of identity theft. Employees should contact competent legal counsel regarding requests related to identity theft.

## 7. Service Provider Oversight

Rosedale Technical College will oversee each of its service providers and processors that may have access to or otherwise create, collect, use, or maintain personal information on its behalf by:

1. Evaluating the service provider's or processor's ability to implement and maintain appropriate security measures, consistent with this ISP and all applicable laws and Rosedale Technical College's obligations. This may include having the service provider or processor complete a vendor risk assessment questionnaire.

2. Requiring the service provider or processor by contract to implement and maintain reasonable security measures, consistent with this ISP and all applicable laws and Rosedale Technical College's obligations. This may include having the service provider or processor complete and sign an applicable Data Processor Agreement.

3. Monitoring and auditing the service provider's or processor's performance to verify compliance with this ISP and all applicable laws and Rosedale Technical College's obligations.

## 8. IT Change Management Policy

Changes to Rosedale Technical College infrastructure introduces a heightened risk of cybersecurity incidents. Accordingly, this section governs the addition, removal, or modification of the elements of Rosedale Technical College IT infrastructure as follows:

1. Adding and removing end-user devices. The Program Coordinator or designated IT personnel must be involved in adding end-user devices. Adding end-user devices, such as desktops, laptops, phones, or tablets requires that the devices be securely configured in accordance with the technical and electronic safeguards outlined in this policy. This includes, but is not limited to, automatic session locking after a defined period of inactivity, strong password requirements, and device lockouts after a specified number of failed authentication attempts. If possible, portable devices should be set up to support remote wiping of all company data upon suspected theft, loss, or employee termination.

2. Adding third-party software & applications. Prior to adding any third-party software or applications (whether hosted on premises or cloud-based), the vendor must be assessed for the adequacy of their technical and physical information safeguards. This includes, at a minimum, completing an electronic vendor risk assessment questionnaire for the service provider.

3. Additions or modifications to web browsers. Cybercriminals can exploit web browsers in multiple ways. If they have

access to exploits of vulnerable browsers, they can craft malicious webpages that can exploit those vulnerabilities when browsed with an insecure, or unpatched, browser. Alternatively, they can try to target any number of common web browser third-party plugins that may allow them to hook into the browser or even directly into the operating system or application. Accordingly, before allowing any browser to execute on the network, the following must be ensured:

- Browser plugins are limited to trusted sources or otherwise disabled. Many plugins come from untrusted sources, and some are even written to be malicious. Therefore, it is best to prevent users from intentionally or unintentionally installing untrusted plugins that might contain ma/ware or critical security vulnerabilities.
- Automatic updates and patches for the browser and plugins have been properly configured.
- Content filters for phishing and ma/ware sites have been enabled.
- Pop-up blockers have been enabled. Pop-ups can host embedded malware directly or lure users into clicking links using social engineering tricks.

4. Major additions or modifications to servers, operating systems, or network elements. Any major modification, addition, or removal of servers, operating systems, or network elements (e.g., routers, switches, and firewalls) must be accompanied by the following:

   - A full internal penetration test.
   - A full internal and external vulnerability assessment.

Consider conducting a technical risk assessment that is designed to assess the safeguards outlined in this Program, as appropriate based on the changes made.

## **9.** Data Retention Plan

The information of Rosedale Technical College is important to how it conducts business, protects customer data, and manages employees. Federal and state law require Rosedale Technical College to retain certain customer records, usually for a specific amount of time. Rosedale Technical College must retain certain records because they contain information that (1) serves as Rosedale Technical College's corporate memory, (2) have enduring business value, or (3) must be kept to satisfy legal, accounting, or regulatory requirements. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences for Rosedale Technical College and/or its employees:

- Fines and penalties. Loss of rights.
- Obstruction of justice charges.
- Inference of spoliation of evidence and spoliation tort claims.
- Contempt of court charges.
- Serious disadvantages in litigation.

This policy is part of a company-wide system for the review, retention, and destruction of records that Rosedale Technical College creates or receives in connection with the business it conducts. Any type of information created, received, or transmitted in the transaction of Rosedale Technical College's business, regardless of physical format (collectively "record" or "records" hereinafter) are covered by this policy. Examples of where the various types of information are located include:

- Appointment books and calendars.
- Audio and video recordings.
- Computer programs and online applications.
- Contracts.

- Electronic files.
- Emails.
- Handwritten notes.
- Hard drives.
- Invoices.
- Letters and other correspondence.
- Memory in cell phones and mobile devices.
- Online postings, such as on Facebook, Twitter, Instagram, Snapchat, Slack, Reedit, and other social media platforms and websites.
- Repair files.
- Voicemails.

Rosedale Technical College prohibits the inappropriate destruction of any records, files, documents, samples, and other forms of information. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Rosedale Technical College and retained primarily for reference purposes.
- Spam and junk mail.

How and When to Destroy Records:

Rosedale Technical College's Program Coordinator is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. Regarding customer information, if no record retention period is specified, the secure disposal of customer information in any format must occur no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes. The destruction of confidential, financial, customer and personnel-related records must be conducted by shredding. The destruction of electronic records must be coordinated with the Program Coordinator. The destruction of records must stop immediately upon notification from legal counsel that a litigation hold is to begin because Rosedale Technical College may be involved in a lawsuit or an official investigation (see below). Destruction may begin again once legal counsel lifts the relevant litigation hold.

Litigation Holds and other Special Situations:

Rosedale Technical College requires all employees to comply fully with its published procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or legal counsel informs you, that Rosedale Technical College records are relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails, until legal counsel determines those records are no longer needed. This exception is referred to as a litigation hold or legal hold and replaces any previously or subsequently established destruction schedule for those records. If you believe this exception may apply, or have any questions regarding whether it may apply, please contact legal counsel. In addition, you may be asked to suspend any routine document disposal procedures in connection with certain other types of events, such as the merger of Rosedale Technical College with another organization or the replacement of Rosedale Technical College's information technology systems.

Periodic Review & Other Responsibilities:

The Program Coordinator shall periodically review this policy and its procedures with legal counsel and/or Rosedale Technical College certified public accountant to ensure Rosedale Technical College is minimizing the unnecessary retention of data to the extent possible and is in full compliance with relevant new or amended regulations. The Program Coordinator (or a more qualified individual as determined by the Program Coordinator) is responsible for identifying the documents that Rosedale Technical College must or should retain, and determining, in collaboration with legal counsel, the proper period of retention. The Program Coordinator also arranges for the proper storage and retrieval of records, coordinating with outside vendors where appropriate. Additionally, the Program Coordinator is responsible for the destruction of records whose retention period has expired.

Record Retention Schedule:

Occasionally, Rosedale Technical College establishes retention or destruction schedules or procedures for specific categories of records. This is done to ensure legal compliance and accomplish other objectives, such as protecting intellectual property and controlling costs. Avoid retaining a record if there is no business reason for doing so and consult with the Program Coordinator or legal counsel if unsure.

## 10. Enforcement

Violations of this ISP may result in disciplinary action, up to and including termination, in accordance with Rosedale Technical College's human resources policies.

## 11. Program Review

Rosedale Technical College will review this ISP and the security measures defined herein at least annually, or whenever there is a material change in Rosedale Technical College's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information. Rosedale Technical College shall retain documentation regarding any such program review, including risk assessment, mitigation steps, disciplinary actions, and remedial actions.

## 12. Incident Response Plan

Purpose & Goals

The purpose of this Incident Response Plan (IRP) is to outline the responsibilities of the Program Coordinator for responding to "information security incidents". "Information security incident" means an actual or reasonably suspected event that has one or more of the following consequences:

1. loss or theft of personal information;
2. unauthorized use, disclosure, acquisition of or access to, or other unauthorized processing of personal information that may reasonably compromise the privacy or confidentiality, integrity, or availability of personal information; or
3. unauthorized access to or use of, inability to access, loss or theft of, or malicious infection of Rosedale Technical College’s IT systems or third-party systems that reasonably may compromise the privacy or confidentiality, integrity, or availability of personal information or Rosedale Technical College's operating environment or services.

Specifically, Rosedale Technical College's goals for this IRP include to:

- Define Rosedale Technical College's cyber incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.
- Assist Rosedale Technical College and any applicable third parties in quickly and efficiently responding to and

recovering from different levels of information security incidents.

- Mitigate or minimize the effects of any information security incident on Rosedale Technical College, its customers and employees.
- Help Rosedale Technical College consistently document the actions it takes in response to information security incidents.
- Reduce overall risk exposure for Rosedale Technical College.
- Engage stakeholders and drive appropriate participation in resolving information security incidents while fostering continuous improvement in Rosedale Technical College's information security program and incident response process.

Accountability:

Rosedale Technical College has designated the Program Coordinator to implement and maintain this IRP. Additionally, the Program Coordinator is responsible for coordinating each of the internal processes for responding to information security incidents, as defined in more detail below.

Internal Processes for Responding to Information Security Incidents:

Rosedale Technical College may, from time to time, approve and make available more specific procedures for certain types of information security incidents. Those additional procedures and checklists are extensions to this IRP. The Program Coordinator may assign the duties of responding to an information security incident to other employees, departments (e.g., Human Resources, Legal, Information Technology) and external individuals, including vendors, service providers, or other resources, to participate in this IRP.

Upon identification of an information security incident, the Program Coordinator shall move quickly to perform the following steps, as applicable:

1. Secure the school’s operations. The Program Coordinator, in conjunction with qualified IT personnel, shall be responsible for performing each of the following:
    1. Secure systems and fix vulnerabilities that may have caused the breach.
    2. Secure physical areas potentially related to the breach. Lock them and change access codes, if needed.
    3. Ask a forensics expert or law enforcement when it is reasonable to resume regular operations, if applicable.
    4. Mobilize a breach response team to prevent additional data loss. The exact steps to take depend on the nature of the breach, but should normally include Rosedale Technical College 's forensics, legal, information security, information technology, operations, human resources, communications, investor relations, and executive management.
    5. Consider hiring independent forensic investigators to help determine the source and scope of the breach. They will capture forensic images of affected systems, collect and analyze evidence, and outline remediation steps.
    6. Consult with legal counsel and consider hiring outside legal counsel with privacy and data security expertise to advise on federal and state laws that may be implicated by a breach.
    7. Stop additional data loss by taking all affected equipment offline immediately, but don't turn any machines off until forensic experts arrive.
    8. Closely monitor all entry and exit points, especially those involved in the breach.
    9. If possible, put clean machines online in place of affected ones.
    10. Update credentials and passwords of authorized users. If a hacker steals credentials, systems will remain

vulnerable until those credentials are changed, even if the hacker 's tools have been removed.

11. Remove improperly posted information from the web. If the incident involved personal information improperly posted on your website, immediately remove it. Be aware that internet search engines store, or "cache," information for a period of time. Contact the search engines to ensure that they don't archive personal information posted in error.

12. Search online for exposed data to make sure that no other websites have saved a copy. If you find any, contact those sites and ask them to remove it.

13. Interview employees who discovered the breach. Also, talk with anyone else who may know about it.

14. Do not destroy evidence. Don't destroy any forensic evidence during your investigation and remediation.

2. Remediate weaknesses and fix vulnerabilities. The Program Coordinator, in conjunction with qualified IT personnel, shall be responsible for performing each of the following:

    1. If service providers, contractors, processors, or other third parties were involved in the information security incident, examine what personal information they can access and decide if their access privileges need to change. Also, ensure they are taking the necessary steps to prevent another breach from occurring. If your service providers say they have remedied vulnerabilities, verify that they really fixed things.

    2. Work with forensics experts to analyze whether any network segmentation plan was effective in containing the breach and make changes as necessary.

    3. Find out if measures such as encryption were enabled when the breach happened.

    4. Analyze backup or preserved data.

    5. Review logs to determine who had access to the data at the time of the breach and analyze who currently has access. Then determine whether that access is needed and restrict access if it is not.

    6. Once all identified weaknesses have been remediated, perform the following:

        1. A full internal penetration test.

        2. A full internal and external vulnerability assessment.

        3. Consider conducting a technical risk assessment that is designed to assess the safeguards outlined in this Program, as appropriate based on the information security incident.

3. Develop a comprehensive communications plan. The Program Coordinator, in conjunction with competent legal counsel and executive management, shall perform each of the following:

    1. Verify the types of information compromised, the number of people affected, and whether contact information is available for those people.

    2. Develop a comprehensive communications plan that reaches all affected audiences - employees, customers, investors, business partners, and other stakeholders. Don't make misleading statements about the breach and don't withhold key details that might help consumers protect themselves and their information. Ensure that there is no information disclosed in the communications that might put consumers at further risk.

    2. Anticipate questions that people will ask. Consider putting together a list of frequently asked questions (FAQs)

that can be displayed on your website or provided to customer-facing employees who might be asked about the incident. Make sure to use plain-language answers since good communication up front can limit customers' concerns and frustration, saving Rosedale Technical College time and resources later.

3. Notify appropriate parties. The Program Coordinator, in conjunction with competent legal counsel and executive management, shall perform each of the following:

    1. Work with legal counsel to determine applicable breach notification laws. All states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. Depending on the circumstances and types of information involved in the incident, there may be several laws or regulations that apply, or none at all.

    2. Work with legal counsel to discuss notifying your local police department if there is a potential risk for identity theft. The sooner law enforcement learns about the incident, the more effective they can be. If local police aren't familiar with investigating information compromises, contact the local office of the Federal Bureau of Investigation or the U.S. Secret Service. For incidents involving mail theft, consider contacting the U.S. Postal Inspection Service.

    3. Work with legal counsel to discuss notifying affected businesses. For example, if credit card or bank account numbers have been stolen, but Rosedale Technical College does not maintain the accounts, notify the institution so that it can monitor the accounts for fraudulent activity. If the information compromised is collected or stored on behalf of other businesses, notify them of the incident.

    4. If Social Security Numbers have been stolen, work with legal counsel to discuss contacting the major credit bureaus and whether it is recommended that people request fraud alerts and credit freezes for their files.

    5. Work with legal counsel to discuss notifying individuals affected by the incident.

        1. Consult with law enforcement about the timing and content of the notification so it doesn't impede any active investigation.

        2. Designate a point person for releasing information.

        3. Consider offering at least a year of free credit monitoring or other support such as identity theft protection of identity restoration services, particularly if financial information or Social Security Numbers were exposed. When such information is exposed, thieves may use it to open new accounts. Depending on the circumstances, this may be required by law.

        4. Consider using the sample data breach notification letter below, which incorporates guidance from state and federal agencies, and consider creating a designated email or toll-free numbers to communicate with people whose information may have been compromised. If the contact information for all of the affected individuals is not available, consider building a press release or other news media notification. As part of any notification plan, consider enclosing with the letter a copy of "Identity Theft: A Recovery Plan," which is a comprehensive guide from the FTC to help people address identity theft. The guide can be ordered in bulk for free at bulkorder.ftc.gov. The guide will be particularly helpful to people with limited or no internet access.

5. Evaluate need for modifying incident response plan. Following any information security incident, the Program Coordinator shall determine whether changes to this incident response plan are necessary and shall make such changes, as necessary, to improve the future handling of information security incidents. The Program Coordinator shall consider Rosedale Technical College's effectiveness in detecting and responding to the incident and identify any gaps or opportunities for improvement. The Program Coordinator shall also seek to identify one or more root causes for the incident and, according to risk, shall recommend appropriate actions to minimize the risks of recurrence.

Sample Data Breach Notification Letter

[Insert Name of Company/Logo]. Date: [Insert Date]

NOTICE OF DATA BREACH

Dear [Insert Name]:

We are contacting you about a data breach that has occurred at [insert Company Name].

What Happened?

[Describe how the data breach happened, the date of the breach, and how the stolen information has been misused (if you know)].

What Information Was Involved?

This incident involved your [describe the type of personal information that may have been exposed due to the breach].

What We Are Doing

[Describe how you are responding to the data breach, including: what actions you 've taken to remedy the situation; what steps you are taking to protect individuals whose information has been breached; and what services you are offering (like credit monitoring or identity theft restoration services)].

What You Can Do

[Insert the following language if the information compromised poses a high risk of identity theft or social security numbers were compromised].

The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: Equifax .com/personal/credit-report-services or 1-800-685-1111 Experian:

experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

[Insert the following language if you choose to provide a copy of the FTC's identity theft guide].

We have attached information from the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information ex posed in this breach.

Other Important Information

[Insert other important information here]

For More Information

Call [telephone number] or go to [Internet website]. [State how additional information or updates will be shared/or where they will be posted].

[Insert Closing] [Your

Name]

13. Effective Date

This ISP is effective as of May 15, 2023