Title: Privacy Compliance Program	
Department: Information Security Office	**Owner/Contact:** Adam Ratcliff
Approval Date: 08/20/2021	**Last Review Date:** 1/17/2024 **Review Period:** Annual
Applicability: All employees, contractors, and vendors of Navigate360 and its affiliated entities who access or use Navigate360 technology.	
Authority: The Compliance Program is enacted at Navigate360 under the direction of its Board of Directors.	

Document History			
Version	**Date**	**Revised by**	**Description of Change**
1.0	07/01/2021	Adam Ratcliff	Original Draft
1.1	8/20/2021	Adam Ratcliff	Added Information Retention
1.2	03/22/2022	Adam Ratcliff	Changed Customer Data Retention from 60 to 30 days
1.3	11/10/2022	Adam Ratcliff	Annual review for 2022, updated language around state privacy
1.4	1/30/2023	Nick Zoglman	Legal Review
1.5	1/17/2024	Adam Ratcliff	Annual Review, no changes noted

Privacy Compliance Program

This Privacy Compliance Program (Program) applies to all officers, employees, contractors, and agents of Navigate360 (collectively "Associates"). This Program is overseen by the Board of Directors. The Board has appointed its Director of Information Security (DIS) to perform periodic risk assessments in order to update and monitor this Program. The VP of Engineering (VPE) oversees all aspects of regulatory compliance, including, without limitation, intellectual property laws, privacy laws and regulations, labor and employment, and corporate governance.

Table of Contents

I. Overview

Administration of this Program

Navigate360 ("**Company**") expressly reserves the right to change, modify, or delete the provisions of this Program and the subsequent Policies that are a component of this Program. If you have any questions regarding this Program, please contact the DIS or VPE.

Purpose of this Program

This Program is established to detect noncompliance and prevent misconduct regarding Company policies to ensure Company activities are conducted in accordance with applicable criminal and civil laws, regulations, and rules. This Program is a component of our culture and the foundation for our solid reputation. Our reputation allows us to have better relationships with investors, employees, clients, prospects, regulators, and rating agencies. This Program also assists when employees are unsure of the appropriate course of action by considering whether their situation or contemplated course of action is against the law or Company policy.

Scope

Privacy Compliance is an obligation that is the responsibility of every Associate. The Company is responsible for communicating standards of conduct and for developing policies, procedures, and systems to assist Associates in understanding the laws and meeting Company's Code of Conduct. Each Associate is expected to comply with all laws and Company's Code of Conduct.

What is included in the Privacy Compliance Program?

1. **Policies**. These are designed to provide Associates with:
    - Awareness of the laws, regulations, and policies impacting Company and its vendors to be incorporated as part of the Vendor Management Program;
    - Opportunities and instructions to ask questions or report suspected violations of laws, regulations, or policies without fear of retaliation;
    - Accountability for violations of policies, legal or regulatory obligations (including supervisors who condone or unreasonably fail to prevent improper conduct), and;
    - Requirements to align departmental procedures and practices with Company's compliance policies and this Program.

2. **Assignments.** The Program defines roles and responsibilities for carrying out Company's compliance obligations. All Associates are responsible for the promotion and enforcement of compliance through established policy and procedural requirements.

3. **Periodic risk assessments.** Management designated the person referenced above as responsible for conducting periodic risk assessments that focus on compliance with laws and regulations, including a process to design, evaluate, modify, and implement changes to the Program based on issues identified through the risk assessment. The risk assessments shall consider: (i) the country and industry sector, (ii) potential business partners and related compliance obligations (iii) oversight over the potential business partners relationship, (iv) government regulation and oversight, and (iv) exposure to import/export control laws and international laws in conducting international business.

4. **Training.** Training of Associates regarding compliance-related topics is an important component of this Program. All new employees and contractors are required to complete compliance orientation training within 30 days of hire or commencement of the contractual relationship with the Company. This includes an acknowledgement that the employee understands and agrees to abide by the Code of Conduct. All Associates must also complete annual compliance refresher training. Whenever possible, training will incorporate the use of practical, real-world scenarios which encourage employees to make choices as to a potential course of action and then discuss how actions affect the integrity and credibility of the employees and Company.

5. **Detection.** Company has defined control frameworks to meet its objectives, including its compliance objectives. This Program along with Policies are designed to control and detect the particular types of misconduct and noncompliance most likely to occur.

6. **Instructions for Investigations.** The Program includes instructions and guidance for the HR Department and Executive Leadership Team to promptly investigate all credible reports of violations of laws, rules, and regulations.

7. **Merger and Acquisition Due Diligence.** Pre-merger and acquisition due diligence enables Company, as the acquiring company, to evaluate costs of any violations of law or misconduct which occurred prior to purchase and may be borne by Company as a result of the acquisition. This Program includes guidance for conducting merger and acquisition integration of a newly acquired company including post-acquisition training and controls to reduce post-acquisition exposure.

Designing and Maintaining the Compliance Program

The Company's DIS manages the daily activities of the Compliance Program and reports concerns directly to the VPE. DIS job description includes the requirements to:

- Continuously monitor legal and regulatory changes as well as product and service offering changes and update this Program and the risk assessment accordingly.
- Prepare an annual compliance plan for approval by the Executive Leadership Team.
- Present the Executive Leadership Team with periodic reports on progress in meeting the plan, including reports of any independent assessments and/or audit results.

Associate's Responsibility

It is the obligation of all Associates to join in the Company's compliance commitment. Associates are expected to:

- Read and understand the Code of Conduct.
- Apply the Code every day in the course of your job.
- Use good judgment and abide by both the letter and the spirit of the Code.
- Know the laws that apply to your job. Our Code of Conduct and Program does not require you to be a legal expert. However, you are expected to be familiar with the basic laws that apply to your specific job and level of responsibility.
- Pay close attention to all training information and policies. Do not be afraid to ask questions. You should offer suggestions to improve policies and procedures or make them easier to understand and use.
- Cooperate with Company representatives on audits and internal investigations. If you believe there is a potential violation of law or policy or if you have doubts about the legal or policy implications of a situation, bring the matter to the attention of your supervisor or the HR department. Compliance questions and concerns can also be reported anonymously through the anonymous hotline.

Supervisor's Responsibility

Each supervisor and manager is expected to:

- Ensure Associates are properly trained and understand their obligations under the Code of Conduct and the Compliance Program.
- Know where policies and procedures are located and promote departmental compliance with regulatory standards. Consider whether it is easy for Associates to comply with the law and hard to circumvent policy and procedural requirements. If you come to believe that they are not, voice your concerns to the Executive Leadership team.
- Maintain an open-door policy. As a supervisor and manager, you are to make it clear you are open to questions or concerns about compliance-related issues from your direct reports or other Associates who may bring concerns to you.
- Take prompt and appropriate action when a suspected violation of law or policy is brought to their attention. No one who reports a suspected violation of law or policy in good faith is subject to any retaliation.

II. Privacy Policy

Purpose of Policy

This Policy is to provide an understanding of privacy risks the activities and priorities established by Executive Leadership to collect, process, use, maintain, and dispose of Personal Information and the appropriate safeguards.

Scope

This Privacy Policy applies to both Student Information (see the Student Privacy Policy) as well as any other Personal Information (as that term is used below) made available by customers.

Associates' Privacy Obligations

All Associates shall manage data, especially Personal Information, consistent with Company's privacy risk strategy to protect the data of individuals and entities which we collect. Data protection occurs at all stages and decision points including when data is collected, processed, used, maintained and disposed (herein collectively referred to as "processed" or "processing"). Company's privacy risk strategy requires Associates to:

- Conduct all data processing practices in accordance with reasonable information security practices (as outlined with Company's Information Security Policy).
- Notify Executive Leadership immediately upon identifying any actual or suspected data breach incident.

Responsibility

Company has assigned the DIS/VPE to provide ownership, leadership, and coordination to privacy compliance and the day-to-day implementation of this Policy.

What are Privacy Laws?

Laws that apply to the processing of an individual's Personal Information or might otherwise affect an individual's privacy rights.

- Key US Federal Privacy Laws
    - **Federal Trade Commission Act:** prohibit unfair or deceptive practices in the collection, use, processing, protection, and disclosure of personal information. This means that privacy notices and statements must be accurate and personal information must be safeguarded against unauthorized access, use, and disclosure.
    - **The Family Educational Rights and Privacy Act (FERPA)** is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
        - Although FERPA applies to schools, and not companies, Navigate360 is designated as a 'School Official' and as such, we are compliant with FERPA and are committed to protecting the privacy of students' information, which is entrusted to us by educational institutions who purchase our products and services. The educational institutions are in control of all student data and we proceed under their direction. Under FERPA, parents or eligible students have the right to access, inspect, review and rectify student records and Navigate360 complies with these rights when we get a verified written request from an educational institution.
        - ***Please note that Navigate360 has no direct contact with students or parents through use of our products and services.***

- **Children's Online Privacy Protection Act (COPPA):** imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.
    - We meet the following COPPA guidelines and agree to:
        - **NOT** collect online contact information without the consent of either a parent or qualified educator or educational institution.
        - **NOT** collect personally identifiable offline contact information.
        - **NOT** distribute to third parties any personally identifiable information without prior parental consent.
        - **NOT** entice divulging personal information by the prospect of a special game, prize, or other activity or to entice divulging more information than is needed to participate in the game, prize, or other activity.
        - **NOT** use or disclose student information for behavioral targeting of advertisements to students.
        - **NOT** build a personal profile of a student other than for supporting authorized educational/school purposes.

- Key US State Laws:

    - **Breach Notification Laws:** all 50 states and the District of Columbia, Guam, and the US Virgin Islands have enacted laws requiring notification of security breaches involving personal information.
    - **The California Consumer Privacy Act of 2018 (CCPA) and California Privacy Rights Act of 2020 (CPRA)** provide California residents certain rights regarding the personal information we collect about them. For more information on the CCPA/CPRA and how it relates to your data, contact us at legal@navigate360.com or refer to our Privacy Notice located here.
    - **The Colorado Privacy Act (CPA)** provides Colorado residents with the right to opt out of targeted advertising, the sale of their personal data, and certain types of profiling.
    - **New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act")** requires any person or business owning or licensing computerized data that includes the private information of a resident **of New York** ("covered business") to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information.
    - **The Virginia Consumer Data Privacy Act (VCDPA)** gives consumers the right to access their data and request that their personal information be deleted by businesses.

Company's Privacy Notice

Navigate 360 maintains an online Privacy Notice that describes the nature of our data standards and practices. If a customer seeks any information regarding our data practices or standards Associates should refer them the online Privacy Notice. The Navigate360 Privacy Notice can be viewed here for more information.

What is Personal Information?

For purposes of this Policy, Company has defined Personal Information as any information that identifies, relates to, describes, or is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular person or household.

Your Privacy Rights

When you engage Navigate360, you have the following privacy rights in relation to your personal data:

- **Right to know and access:** You have the right to request what, where from, and why we collect your personal information, as well as who we have disclosed, shared, or you're your personal information to, in the last 12 months. You have a right to request a copy of such personal data information at any time.

- **Right to correct:** You have the right to request the correction of any inaccurate personal information about you we may maintain.
- **Right to delete & data erasure**: You have the right to request Navigate360 to delete/erase your personal information at any time.
- **Right to withdraw consent:** If you have declared your consent for any personal information processing activities as described in this Privacy Policy, you have the right to withdraw this consent at any time with future effect. Such a withdrawal will not affect the lawfulness of the processing prior to the withdrawal. Please note that withdrawal of certain contents may limit functions of the website or online services.
- **Right to lodge a complaint:** In case you have a complaint about the processing of your personal information, you have the **right to lodge a complaint** with a competent supervisory authority.
- **Right to not be discriminated or retaliated against:** You will not receive any discriminatory treatment if you choose to exercise any of your rights. We will not deny goods or services to you, charge different prices or rates, provide a different level or quality of goods or services, or suggest that you will receive a different price or rate or a different level or quality of good or services. Providing your personal is optional. Refusal to provide your personal information will not have any impact on using our website. If requested under any data protection laws, we will collect your prior consent before proceeding to processing your personal information for these purposes.
- **Right to limit use and disclose of sensitive personal information:** We only use sensitive personal information for that which is necessary to perform the services or provide the goods reasonably expected by a consumer who requests the services or goods.
- **Right to restrict processing:** You have the right to request that Navigate360 restricts the processing of your personal information, under certain conditions.
- **Right to object to processing:** You have the right to object to Navigate360's processing of your personal information, under certain conditions.
- **Right to object to use:** You have the right to object to the use of your information at any time.
- **Right to information portability:** You have the right to request that Navigate360 transfers the personal information that we have collected to another organization, or directly to you, under certain conditions.
- **How we share information**: We may disclose your personal information with our affiliated brands or any business that we may acquire in the future.

III. Student Privacy Policy

Purpose of Policy

This Policy is to provide a general understanding of student data privacy laws, compliance risks, and the procedures and priorities established by Executive Leadership when Company collects, processes, uses, maintains, and disposes of Student Information (term defined below) and the appropriate security safeguards.

Scope

This Student Privacy Policy applies to Student Information obtained through an organization's use of any Company products or services. Student Information, as that term is used in this policy, refers to directory information or personally identifiable information contained in any educational record that is disclosed to the Company. Directory information refers to information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Personally identifiable information refers to personal or indirect identifiers and information linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Educational Records refers to records maintained by educational agencies or institutions or by parties acting on behalf of educational agencies or institutions.

Applicable Law

Company's collection, processing, use, maintenance, and disposal of Student Information is guided largely by federal law and regulations. In many cases it is additionally guided by individual state law and regulations. In some cases, these laws place specific obligations only on educational institutions, such as allowing parents to exercise certain rights. In other cases, obligations are placed on organizations who provide products or services to educational institutions, such as restrictions on using Student Information for targeting advertising. In the case of the former, Company will work with the educational institution to help them maintain compliance with such laws or regulations. In the case of the latter, Company will maintain policies and procedures to ensure compliance with the laws and regulations.

- Key US Federal Student Data Privacy Laws
    - Family Educational Rights and Privacy Act (FERPA)
    - Children's Online Privacy Protection Rule (COPPA)
    - Protection of Pupil Rights Amendment (PPRA)
    - Individuals with Disabilities Education Act (IDEA)

- Key US State Student Data Privacy Laws
    - Florida law related to Student and Parental Rights and Educational Choices (Ch. 1002.22)
    - Georgia Student Data Privacy, Accessibility, and Transparency Act
    - Illinois' Student Online Personal Protection Act (SOPPA)
    - Kentucky Family Educational Rights and Privacy Act
    - Maine's Student Information Privacy Act
    - Massachusetts law related to Student Records (603 CMR 23.00)
    - Nevada law related to Privacy of Data Concerning Pupils (NRS 388.281-388.296)
    - New Hampshire law related to Student Online Personal Information (Rev Stat § 189:68-a)
    - New York law related to Unauthorized Release of Personally Identifiable Information (Section 2-D) and Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information (Part 121)
    - Rhode Island's Educational Records Bill of Rights Act
    - Utah law related to Student Privacy and Data Protection (53E-9-309)
    - Virginia law related to Pupil Records (Code of Virginia § 22.1-289.01-22.1-287.02)
    - West Virginia law related to Procedures for the Collection, Maintenance, and Disclosure of Student Data (Series 126-094)

Policy Application

This Policy describes Company standards in relation to:

- Defining the types of Student Information approved to be collected in designing Company products and services.
- Determining the controls and processes for transferring Student Information from an educational institution to Company, including any service providers Company works with to provide its products and services.
- Ensuring Student Information is used solely for the purpose for which Company's products and services are created, and in compliance with the terms of any contract between Company and an organization.
- Designing Company's Information Security Program and Software Development Life Cycle program to ensure Student Information is safeguarded against unauthorized access, use, and disclosure.
- Outlining when and how Student Information will be destroyed and/or transferred back to an organization taking in consideration legal, contractual, and practical risks to Company.

In consideration of educational institution due diligence obligations and Company's alignment with security best practices, Company maintains the following lists of standards as they relate to collection, processing, use, maintenance, and retention of Student Information. (See FTC Guidance and PTAC Guidance)

1. **Collection**
   - Data field inventories that list the types of Student Information that can be collected by each Company product and service.
   - Clear, unambiguous, and accurate contract terms describing the use of Student Information for each Company product or service.

2. **Processing**
   - Effective and efficient methods, defined by written procedures, to authenticate an educator and assist in requests, as appropriate, to provide educators with data access to honor requests from the government, regulatory agencies, and students/parents—*State contracts often prescribe the turnaround time as being within 5 business days*. (See US Dept. of Education Guidance.)
   - Employment of the principle of least privilege to limiting internal access to Student Information to only those Associates who have a legitimate business interest.

3. **Use**
   - Vendor management program that prohibits vendors from using Student Information for any purpose other than those necessary to fulfill the obligations of Company in supporting the products and services purchased by educational institutions.
   - Clear, unambiguous, and accurate contract terms describing disclosure of Student Information for each Company product or service.

4. **Maintenance**
   - An up to date Company Information Security Program ("CISP") that defines security controls and the evaluation of those controls to meet Company's data security strategic objectives.
   - Data risk assessments that are designed to detect and report data security vulnerabilities to Executive Leadership and key stakeholders to ensure resources are available to remediate those vulnerabilities as appropriate. (See PTAC Guidance.)
   - Data back-up procedures that align with Data Processing Agreement ("DPA") and service level commitments – *standard DPA is to perform daily back-up*.
   - Contract prohibitions with vendors and internal policy/procedures that prohibit the transmission of Student Data outside of the United States.
   - A Data Breach Policy and related procedures to alert the appropriate authorities and/or educational institutions in the event Student Information held by Company, or on behalf of Company, is accessed without authorization. (See PTAC Guidance.)

5. **Retention**
   - Defining and implementing data retention standards and destroying Student Information when it is no longer needed—*within 60 days when the contract is terminated or a school notifies Company that Student Information is no longer needed.*
   - Data destruction practices that are consistent with Industry Best Practices. (NIST 800-88). (See PTAC Guidance.)

Associate Responsibilities

All Associates shall manage Student Information consistent with this Policy which is aligned with Company's privacy risk strategy--*to protect Student Information and to only display and capture data when necessary for the intended use of Company products and services*. To accomplish, each Associate shall coordinate and adopt procedures to accomplish the following:

Associate Training

- Company maintains the following data security training requirements: (See PTAC Guidance.)
  - A role-based data security training program that is reflective upon the role's responsibility, considering the volume and sensitivity of the data the role has access to, in defining, managing, and maintaining data security controls
  - Participation of all Associates who have access to Student Information are trained to protect data confidentiality and to preserve data security.
  - Sufficient communication to maintain a culture of security throughout the organization.
  - Training encompasses all areas of potential material threats and vulnerabilities identified by the Company's risk assessment.

IV. Data Breach Policy

Purpose of Policy

A data breach can be extremely damaging to Company, data subjects, and Company's clients. All fifty states, including the District of Columbia, have adopted data breach notification statutes. This Policy serves as a checklist to ensure Company's response to unauthorized access, use, or disclosure of Personally Identifiable Information ("**PII**") (such access use, or disclosure is hereafter referred to as a "**Data Breach**") is aligned with our legal obligations.

Scope

This Data Breach Policy applies to any Data Breach that occurs to PII:

- Owned or licensed by Company (even if the Data Breach occurs when PII is in possession of another party).
- Owned by the customer and stored by Company.

A Data Breach may be effectuated by various means and methods of acquiring or accessing PII without authorization. These include, but are not limited to:

- Insider attacks
- Social engineering
- Exploitation of a hardware/software vulnerability
- Exploitation from malware
- Extortion

Authority

The Executive Leadership team has delegated responsibility for Company's cybersecurity risk evaluation and incident response plans to the Incidence Response Team member(s) named in the Incident Response Plan. These individual(s) are to:

- Develop, maintain, and routinely evaluate processes to detect a data breach incident.
- Update and modify this policy to appropriately respond to a data breach incident.
- Include within the Incident Response Plan a process to (i) identify and respond to any lessons learned from an actual event, (ii) report such lessons learned and actions taken to Company's Executive Leadership team, and (iii) whenever necessary, work with Company's law enforcement liaison to ensure all evidence of the event are collected and reported in accordance with statutory and contractual obligations.

Data Breach Response

Any actual or reasonable belief that a Data Breach of PII has occurred will activate the Data Breach Response steps listed within this policy.

Step 1: Contain the Data Breach: The Incidence Response Team shall follow the Incidence Response Plan and make every effort to limit further data loss or intrusion which may include isolating the affected systems, changing passwords, and terminating access points.

Step 2: Risk of Harm: The Incident Response Team, in consultation with Company's Executive Leadership Team and Legal Counsel, shall commence an investigation to determine the number of records subject to the Data Breach, whether data misuse is likely, and the effect of encryption or means of making the information unusable to the person(s) who has unauthorized access to PII.

Step 3: Internal Communication: Once the Incident Response Team has contained the incident and coordinated internal resources to investigate the risk of harm (See Steps 1 and 2), the Team shall also begin the process of enacting internal communication plans that are designed to promote limited "need to know" information similar to that which will be provided to the public.

Step 4: Identify the Statutory and Contractual Requirements: Statutes often dictate when information is deemed PII for Data Breach notices, the content and format of Data Breach notices, the recipients of Data Breach notices, and timelines for delivery of Data Breach notices. Contracts (which includes data processing agreements ("DPA") and non-disclosure agreements ("NDA")) also commonly define Data Breach obligations and those obligations should be honored unless Legal Counsel has advised otherwise due to another compelling risk or obligation. Some federal statutes also require notification to regulatory agencies.

- See PTAC Data Breach Response Checklist.

Step 5: Notices: The Incidence Response Team, upon approval of the Executive Leadership Team, shall deliver the Data Breach notices to the appropriate customer contact. Please see Appendix A for standard notification language.

- In the event that a customer is affected with Ransomware, an internal investigation will determine the cause of the breach. On a case-by-case basis, if it is determined that Navigate360 systems were the cause of the breach Cyber Liability Insurance is in place to assist with remediation of the system.

Step 6: Lessons Learned and Remediation: The Incident Response Team will meet following all incidents to determine how the incident occurred, and produce a Lessons Learned document for advisement to the DIS/VPE. Once reviewed, updates to both internal processes and logical controls will be implemented to ensure no repeat offenses occur in the future.

Notice to State Government Entities and Consumer Reporting Agencies

In accordance with Steps 4 and 5 above, Company shall notify, as required by state law, the state's attorney general office or other state government agency and, when appropriate, the three major credit reporting agencies. See State Law Charts.

V. Information Retention Policy

Purpose of Policy

Information owned or processed by Company (whether internally or through a third party) is a vital Company asset. This Policy is to provide Associates with:

- Instructions about retaining data owned or processed by Company.
- Defined retention standards that are aligned with Company's strategic objective which is to destroy or erase information (including deidentified data or metadata) when there is no continuing value or need to retain it.

Scope

This Information Retention Policy applies to all data owned or processed by Company through the use of Company's services or products. This includes, but is not limited to, Personal Information, Student Information, and PII, as those terms are used throughout this Program.

Authority

Company has assigned DIS/VPE to:

- Routinely solicit feedback from leaders from information technology, finance, legal, data security, and product development within the Company to confirm appropriateness of this Policy;
- Document and update, as needed, this policy, and;
- Oversee the data life cycle's destruction process to ensure timeliness and adherence to Company required destruction practices.

What is considered Information?

The term Information as used in this policy refers to all data, whether contained in tangible or electronic format, created or processed by Company, or processed by a third party on behalf of Company.

Retention

Company's information retention timeline has considered the following needs and responsibilities in setting forth its retention schedule:

1. **When Information has Value**
   Information has value when it is used to meet Company needs and responsibilities. Information is valuable when:
   - It provides evidence to support any intellectual property rights or applications filed or to be filed.
   - Held in back-up systems and needed to recover from a disaster.
   - It is general business information used to:
     - Inform investors and stakeholder of Company's performance,
     - Support employee performance and communication,
     - Support products and/or services, or
     - To facilitate sales and future product offerings.

2. **Information is Needed**
   Information is needed by the Company when:
   - Information is subject to a Legal Hold (see Legal Hold Policy).
   - Required to retain by contract.
   - There is a federal, state, or local law that requires retention.

3. **Duplicates and Informal Communication**
   The following is a list of information that has no value at time of creation and may be immediately discarded or deleted at the discretion of the Associate once it has served its temporary purpose:
   - Drafts of letters, worksheets, memorandum, notes, and duplicates of originals that have no significant steps or decisions notated.
   - Spam or junk mail.
   - Training binders and manuals, or other similar information, retained only for reference purposes and obtained from sources outside of Company.

Destruction Methods

Company's Information must be disposed of in accordance with the Corporate Information Security Program ("CISP").

Retention Schedule

At times, Company establishes a retention schedule for specific types of Information. This is done to ensure legal compliance, to protect intellectual property, and to control storage costs. The following Record Retention Schedule is to be adhered to and subject to any Legal Hold.

Record Type	Retention Period	Person(s) Responsible
Employment records	Termination + 7 years	HR
Employment applications	5 years	HR
Employment Benefit Plan records	7 years	HR
Workers' Compensation	Permanent	HR
Payroll records	4 years	HR
Corporate records	Permanent	HR
Contracts	6 years after termination	Products
Customer Production Data	30 days following end of contract (sooner based on customer request)	Products
Financial statements	7 years	Finance
Annual audit reports	Permanent	Finance
Invoices	7 years	Finance
Tax records and filings	7 years	Finance
Insurance contracts / claims / applications	Permanent	Legal
Patents / patent applications	Permanent	Legal
Trademark registration / evidence of use	Permanent	Legal

Appendix A: Data Breach Notification Template

[COMPANY LETTERHEAD]

[INDIVIDUAL NAME/District/etc]

[STREET ADDRESS]

[CITY, STATE AND POSTAL CODE]

[DATE]

Dear [INDIVIDUAL NAME]:

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to inform you about a data security incident that [may involve/involves] [your/your institution's] personal information. [[Between/On] [IDENTIFY TIME PERIOD OF BREACH], [SUMMARIZE BREACH INCIDENT]]. The data accessed [may have included/included] personal information such as [IDENTIFY TYPES OF PII AT ISSUE]. To our knowledge, the data accessed did not include any [IDENTIFY TYPES OF PII NOT INVOLVED].

[COMPANY NAME] values your privacy and deeply regrets that this incident occurred. [COMPANY NAME] is conducting a thorough review of the potentially affected [records/computer system/IDENTIFY OTHER], and will notify you if there are any significant developments. [COMPANY NAME] has implemented additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of [COMPANY NAME]'s valued [customers/employees/IDENTIFY GROUP OF AFFECTED INDIVIDUALS].

The company also is working closely with [major credit card suppliers and] law enforcement to ensure the incident is properly addressed.

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information[, and how to receive free credit monitoring for one year].

For further information and assistance, please contact [NAME OF COMPANY REPRESENTATIVE/ COMPANY] at [TELEPHONE NUMBER/TOLL-FREE NUMBER] between [TIME] a.m.- [TIME] p.m. [EST] daily[, or visit [WEBSITE]].

Sincerely,

[NAME] [TITLE]