The following is a template designed to assist in the policy development governing the identification and proper handling of company-sensitive information. As with all templates, this document provides a basic framework for the broad topics for consideration and the related drafting necessary to properly account for the risks associated with such device use. Where applicable, footnotes have been provided to prompt for other considerations and discussions. For more information, contact Ron Raether at (949) 622-2722 or ron.raether@troutman.com, or Mark Mao at (415) 477-5717 or mark.mao@troutman.com.

SENSITIVE INFORMATION HANDLING POLICY

Template

Title: Sensitive Information Handling Policy	**Doc. No.** Insert
Issued by: (*e.g.*, Corporate Compliance)	**Original Effective Date:** Insert Month/Year
Approved by: (*e.g.*, Board of Directors)	**Last Review/Approval Date:** Insert Month/Year
Replaces: Insert	**Effective Date:** Insert Month/Year
Cross-referenced Policies: Insert	

APPLICABILITY

The purpose of this policy is to define the types of sensitive information stored by us or available to Insert Company Name ("Company," "we," "our," or "us") users, and to set forth guidelines for handling Company Sensitive Information and Personally Identifiable Information ("PII")[1] while in transmission, storage (at rest), or in use/creation.

APPLICABILITY

This policy applies to all employees, administrative consultants, contractors, temporary personnel, third parties, and the like who receive, create, store, handle and transmit Company Sensitive Information or PII in hard copy or electronically. Additional controls are further addressed by the Insert Company Policy Name(s)[2], and other access controls.

POLICY

This policy establishes the guidelines for safeguarding PII and Company Sensitive Information during transmission or while in storage (at rest), or when being initially received, developed, or processed. This policy also covers the hard copy of this information from initial collection or printout.

1. Labeling and Identification

[1] Such terms should be formally defined to ensure proper handling throughout an organization. Attention should be given to regulatory terms, as well, to ensure any policy lines up with the regulation's use of such terms (*i.e.*, "PHI" for HIPAA compliance). Questions should be directed to legal counsel.

[2] In conjunction with the note above, terms should be consistently defined and used in all policies in which protected information is governed. Furthermore, all policies should be reviewed and approved by Human Resource and legal counsel to ensure compliance with other laws or requirements.

a. Public information does not require any special labeling.

b. Company Sensitive Information may or may not require labeling. The author, project manager, or supervisor should provide specific guidance on appropriate labeling. If in doubt, label the information "Confidential" until instructed otherwise.

c. PII should not be labeled so as to bring attention to it. A cover sheet can be placed on it and marked as "Confidential."

d. Labels should be used both on printed/hard copies and electronic formats.

2. Safeguarding During Transmission

a. All transmittal of Company Sensitive Information and PII on public networks or wireless systems will be done using encryption technology. For instance, email encryption, PGP, VPN, secure file transfer, WPA2, and SSL can be used.

b. When faxing Company Sensitive Information or PII, the sender should ensure that the recipient is available to receive the fax and validate the number of pages received or that the receiving fax requires a PIN or other form of identification (*i.e.*, RFID card) to receive the information.

c. If transmittal is via mail, some form of certified mail or a service which provides a chain of custody (*i.e.*, UPS or FedEx, or certified mail with delivery confirmation) should be used.

3. Safeguarding During Storage (at Rest)

a. When Company Sensitive Information and PII is stored on company information computing assets, it should be protected appropriately using available user authentication and file privileges, such as encryption when required.

b. Encryption meeting our standards will be used when storing Company Sensitive Information or PII on laptops and PCs.

c. Encryption meeting our standards will be used when technically possible on mobile computing devices storing Company Sensitive Information or PII.

d. Storage of personal information should be avoided on unencrypted USBs, jump drives, CDs, or DVDs.

e. The retention period of each class of information should be determined according to the Company retention policy.[3]

4. Safeguarding During Creation/Development/Processing

a. When initially receiving Company Sensitive Information and PII, the information may be handwritten, perhaps on a form. If this is the case, the same care must be taken to protect this

3 Consult with legal counsel on applicable legal requirements relating to document retention.

initial piece of paper as you would the formal hardcopy or printout of this information. At a minimum, this information should be secured in a locked office or desk.

b. Company Sensitive Information or PII placed in a document or spreadsheet should be labeled "Confidential" prior to saving.

c. A file or folder containing Company Sensitive Information or PII should not be shared with anyone who is not authorized to access this information.

5. Disposal of Company Sensitive Information and PII

a. Written notes or hardcopy/printout and faxes when no longer needed must be disposed of in an appropriate shred/burn bin or shredded using a cross-cut shredder.

b. Whenever possible, ensure that your screen is not visible to others.

c. Discarded computer equipment (including printer/fax machines) must be decommissioned and the hard drive destroyed using a program that permanently eliminates any PII or Company Sensitive Information.[4]

d. Any computer equipment being sold or transferred to other organizations must be properly sanitized (securely cleared of all information) by the Information Technology Department ("Information Technology").

6. Access and Sharing of Sensitive Information

a. We take the security and safeguarding of our information and employee information seriously. Employee access to our information computing resources is not provided until a background check is completed. If an individual does not pass the background check, including drug testing, the offer to hire is not made or rescinded, and the applicant notified.[5]

b. Prior to being provided access to Company Sensitive Information or PII, users must acknowledge the safeguarding requirements outlined in the Information Security Program.

c. The release of Company Sensitive Information or PII, whether written, oral, or electronic, to persons outside Company is prohibited unless authorized by Information Technology and the General Counsel.

d. In such cases, a signed nondisclosure agreement should be entered into between the recipient of Company Sensitive Information or PII and Company.

e. Company Sensitive Information may be released to the U.S. government if the material is exempt from disclosure under the Freedom of Information Act, and it is marked in accordance with this policy.

[4] Certain regulations may have specific standards for the secure destruction of such hardware prior to disposal, to include federal and state laws, depending on the industry in which your company operates.

[5] Any policy on the use of background checks and drug testing should be coordinated and approved through Human Resources and legal counsel.

f. Information may be disclosed if it is required by legal process or court order as determined by the General Counsel.

7. Termination

a. Individuals having access to Company Sensitive Information or PII who are terminating their employment/relationship with us will have their user ID disabled, access control ID card revoked, and will be advised as to their responsibilities with respect to Company Sensitive Information and PII.

b. The terminating employee will be alerted to the legal consequences of using, retaining, or disclosing Company Sensitive Information or PII for any purpose not expressly authorized by us in writing.

COMPLIANCE

1. Accountability: All users, past and present, are responsible for using the guidance provided by this policy. Any person having knowledge of any unauthorized disclosure or removal of Company Sensitive Information or PII shall report this information to their supervisor, the Human Resources Department or Information Security.

2. Non-Compliance: Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. We reserve the right to advise appropriate authorities of any violation of law.

3. Exceptions: Any exception to this policy must be approved by the General Counsel.

4. Compliance Measurement: Internal Audit will verify compliance to this policy through various methods, including, for example, business tool reports and audits.