

# MITIGATION & PRIVACY POLICY FOR SAGAMORE HILL BROADCASTING

Sagamore Hill Broadcasting adopts this policy to help mitigate damages related to loss or misuse of sensitive information. Following this policy helps protect employees, customers, vendors and the company from damages related to loss or misuse of private, non-public and sensitive information.

The policy applies to any party, person or business possessing or handling sensitive and non-public information belonging to customers/clients, employees, temporaries, vendors, consultants or any others affiliated with Sagamore Hill Broadcasting.

## **SENSITIVE & NON-PUBLIC INFORMATION:**

**The following information will be secured and not shared internally or outside the company unless otherwise noted.**

- **Credit and debit card** numbers (in part or in whole), cardholder name, address, card expiration date and pin number, etc. whether on paper or stored in the computer.
- **Checks** from individuals or businesses
- **Employee and business identifying information** including but not limited to: Social Security numbers, employee identification numbers and Business Identification numbers.
- **Employee pay information**, including, among other information: paychecks, pay stubs and pay rates. Employee pay information and proof of employment with Sagamore Hill Broadcasting will not be released to anyone inquiring without written consent of that employee.

As part of this mitigation and privacy policy for Sagamore Hill Broadcasting employees are required not to discuss pay rates, pay increases, bonuses or commissions with other employees.

- **Medical Information** for any employee or customer including but not limited to: Doctors' names, insurance information, employee medical card numbers, claims, prescriptions or any related personal medical information.
- **Other Personal Information** belonging to employees, customers, contractors, etc. including but not limited to: name or identity of any employee, address, phone numbers, maiden name, personal family information, daily work schedule or work hours. Verifying the employment status of any employee will be done only by Sagamore Hill Broadcasting's Human Resources Manager, Elizabeth Callum and related calls should be directed to her.

**Employees are encouraged not to retain or store any unnecessary papers, documents, computer files, etc. containing sensitive and non-public information and purge such documents periodically.**

## **CORPORATE SENSITIVE AND NON-PUBLIC INFORMATION:**

**This Corporate confidential information for Sagamore Hill Broadcasting will be kept private, secured and not shared internally or outside the company unless otherwise noted.**

- The company's internal policies and procedures
- Customer, vendor and other business relationships and utilization information
- Marketing and advertising information, as well, as other company strategies.
- Sales and retention information
- Personal computer codes, screens, forms, etc.
- Personal information about or received from Sagamore Hill Broadcasting's current, former and prospective customers/clients including but not limited to: names, addresses, phone numbers, sales information, relationship and status with the company, etc.
- Names, identities and information about sales associates, suppliers, vendors and specifics of the relationships between them and Sagamore Hill Broadcasting.
- Any papers or documents marked "Non-Public, "Confidential," "Sensitive," "Proprietary," etc.

## **QUESTIONS ABOUT NON-PUBLIC AND SENSITIVE INFORMATION:**

**The employees of Sagamore Hill Broadcasting are encouraged to exercise common sense judgment when handling, processing and securing Sensitive and Non-Public information. When an employee is unsure of how to handle certain information that employee should consult with his/her direct supervisor. If that supervisor has security questions he/she should consult with the Privacy & Security Manager, LISA BROWN.**

## **HANDLING, STORING AND SECURING HARD COPIES (Paper or data printout, CDs, floppy disks, zip drives, tapes and backups containing personally identifiable information):**

**All employees and contractors will comply with the following policies while doing work for Sagamore Hill Broadcasting.**

- File cabinets, desk drawers, overhead bins, storage cabinets, vaults and all other areas containing personally identifiable information will be locked except when an authorized employee is working on the file. Only authorized personnel will have access to these storage areas.
- Storage rooms containing retained records and data with personally identifiable information will be locked at the end of each workday. Only authorized personnel will have access to these storage rooms.
- Employee's desks, workstations and work areas will be cleared of any documents or papers containing sensitive information when in the company of guests, clients, vendors or other unauthorized people, when the employee is away from his/her desk or work area and at the end of each day.
- Whiteboards, dry-erase boards, writing pads, etc. should not be in view or accessible to unauthorized clients, customers, guests, etc. and will be erased, removed or shredded when not in use.
- Papers containing private, sensitive and personally identifiable information should be immediately removed from printers and fax machines.
- All documents and papers containing sensitive and non-public information will be shredded using a mechanical cross cut or Department of Defense approved shredding device or in a locked shred bin.

Employees are asked to never leave purses, backpacks, briefcases, wallets, etc. containing non-public and private information such as credit & debit cards, driver's licenses, social security cards, checks, etc. or containing money unattended at any time.

#### **INTERNET SECURITY AND POLICY:**

Access to the Internet and Network is provided to staff for the benefit of the organization and its customers. Every employee has the responsibility to maintain and enhance Sagamore Hill Broadcasting's public image and to use the Internet and Network in a productive manner. Please use the following guidelines.

- **Acceptable use of the Internet:** Use of the Internet representing Sagamore Hill Broadcasting for professional reasons using an effective, ethical and lawful manner. Chat channels may only be used to conduct official business or to gain technical or analytical advice.
- **Unacceptable use of the Internet or Network:** The Internet or Network may not be used for personal gain or advancement of individual views, no solicitation of non-company business and no use for personal gain.
- **Communications:** Employees are responsible for the content of all text, audio or images they place or send over the Internet or Network. Fraudulent, harassing or obscene pictures and messages are prohibited. All messages must have the employee's name attached and will not be transmitted under an assumed name. Users may not attempt to obscure the origin of any message. Information published on the Internet or Network should not violate or infringe upon the rights of others. No abusive, profane or offensive language should be transmitted. Employees who wish to express personal opinions on the Internet or Network must use some other Internet or Network systems.
- **Software:** All software downloads will be done only through the station engineer. All data and software on the Network is the property of Sagamore Hill Broadcasting and deleting or changing any data and software is strictly prohibited without prior approval by an authorized Company representative.
- **Copyright Issues:** Employees may not transmit copyrighted materials belonging to entities other than Sagamore Hill Broadcasting. Users may not copy, transfer, rename, add or delete information on programs belonging to other users unless given permission to do so. Employees are not to download or unload music/video on the Internet or Network. Failure to observe copyright or license agreements may result in disciplinary action by the Company or legal action by copyright owners.
- **Security:** All messages created, sent or retrieved over the Internet or Network are the property of Sagamore Hill Broadcasting and should be considered public information. The company reserves the right to access and monitor all messages and fields on the computer system as deemed necessary and appropriate. Internet messages are public communication and are not private.
- **Harassment:** Harassment of any kind is prohibited. No messages with derogatory remarks about an individual or group's race, religion, national origin, physical attributes or sexual preference should be transmitted.
- **Violations:** Violations of any of these guidelines may result in disciplinary action up to and including termination and if necessary Sagamore Hill Broadcasting will advise appropriate officials of any illegal activity.

**EMAIL POLICY:** This is Sagamore Hill Broadcasting policy with regard to access and use of electronic mail messages created, sent or received by Company employees using the Company's mail system.

- The email system is provided by the Company to assist in conducting business within the Company or with clients.
- The email system hardware is the property of Sagamore Hill Broadcasting. All messages composed, sent or received on the company email system are the sole property of Sagamore Hill Broadcasting.
- Use of electronic mail system is made available only to conduct business at the Company and may not be used for personal business.
- Email may not be used to solicit for personal gain, religious or political cause, outside organizations or other non-job-related solicitations.
- The email system will not be sent or received containing offensive messages among which are sexual implications, racial slurs or any other comments that regarding someone's age, gender, sexual orientation, religious or political beliefs, national origin or disability.
- The email system will not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information or similar materials without prior authorization.
- Sagamore Hill Broadcasting reserves and will exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose. Contents of electronic mail properly obtained for legitimate business purposes may be disclosed within the Company without the permission of the employee.
- Confidentiality of any message should not be assumed.
- Erased messages may still be retrieve and read. Passwords do not guarantee confidentiality. All passwords must be disclosed to management or they are invalid and cannot be used.
- Employees of Sagamore Hill Broadcasting may not retrieve or read any email messages that are not sent to them unless given prior approval by management.
- Employees will not use a code, access a file or retrieve any stored information unless authorized to do so. Employees should not attempt to gain access to another employee's messages without the latter's permission. No pass code may be used that is unknown to the Company.
- Any employee discovering a violation of the policy must notify their manager.
- Any employee violating this policy may be subject to disciplinary measures or termination.

**ELECTRONIC SECURITY OF NON-PUBLIC INFORMATION:**

**All employees and contractors conducting work on computers belonging to Sagamore Hill Broadcasting will comply with the following policies:**

- Identify the computers or servers where sensitive personal information is stored.
- Identify all connections to the computers where you store sensitive information including the Internet, electronic cash registers, and computers at branch offices or other locations, computers used by service providers to support your network.
- Do not store sensitive consumer or employee data on any computer with an Internet connection unless it is essential for conducting your business.

- The company engineer for Sagamore Hill Broadcasting will make sure all computers are properly secured and protected from viruses, hacking and Identity Theft and will run up-to-date anti-virus and anti-spy ware programs on company computers and on servers.
- Any personal, non-public or sensitive information sent by email over the Internet should be encrypted and password protected.
- Employees with computers storing private, non-public and sensitive information will not share computer passwords, user names, etc. with other employees and will not post them near workstations. No employee is authorized to give out a password, pass code or user name under any circumstances. Contact the company engineer if you encounter any problems.
- Employees with company or personal laptops containing private, non-public information are required to store laptops in a secure place.
- Employees will log off your computers at the end of each day.
- Discarded CDs, floppy disks, zip drives, tapes, etc. containing personally identifying and non-public information should be properly destroyed or pulverized. Sagamore Hill Broadcasting will contain a statement such as "This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

#### **ROLES AND RESPONSIBILITIES:**

**Management of Sagamore Hill Broadcasting will have the responsibility to enforce this policy and ensure that it is followed by employees and contractors.**

#### **ENFORCEMENT:**

**Any employee of Sagamore Hill Broadcasting found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any employee found stealing any private, non-public or personally identifying information from Sagamore Hill Broadcasting will be criminally prosecuted.**