

**MASSACHUSETTS 201 CMR 17:00 ELECTRONIC SECURITY PLAN****Table of Contents**

<b>Section 1</b>	<b>Provisions and Requirements</b>	
1.1	Provisions of MGL 93H CMR 17:00 .....	2
1.2	Required Elements of the WISP.....	3
1.3	Designation of a Compliance Security Officer.....	4
1.4	Program Development and Implementation .....	5
1.5	Training.....	5
1.6	Definitions.....	6
1.7	Consumer Privacy Policy .....	7
1.8	Third Party Service Providers .....	8
1.9	Safeguarding Confidential Information .....	9
<b>Section 2</b>	<b>Electronic Security System</b>	
2.1	Computer System General Requirements .....	10
2.2	E-mail Policy & Procedures .....	10
2.3	Network & Internet Policy .....	11
2.4	Electronic Access .....	13
2.5	Prohibited Activities .....	13
2.6	Authorized Use of Software .....	15
2.7	Administrative Access Control .....	15
2.8	Firewall Procedures .....	16
2.9	Data Center Security.....	16
2.10	Incident Response & Preparedness.....	16
2.11	Document Destruction .....	17
2.12	Breach of Security.....	18
2.13	Monitoring.....	18

## Section 1 Provisions and Requirements of the Law

### 1.1 Provision of M.G.L. 93H 201 CMR 17.00

Massachusetts General Law 93H 201 CMR 17.00 is a regulation to promulgate standards for entities that own, store, or license personal identifying information of citizens of the Commonwealth. This regulation establishes requirements to safeguard and protect the confidentiality of this information consistent with industry standards. The purpose of this new regulation is to protect confidential information from unauthorized access or use by third parties as well as to protect against security or integrity threats that could harm or inconvenience the customer. All required businesses must have a Written Information Security Plan (WISP) in place by March 1, 2010.

Sample Client has developed the foregoing written Information Security Plan in accordance with M.G.L. 93H 201 CMR 17.00. The foregoing policy has been developed to reflect the size, structure, and business model of the company. The written Information Security Plan has been developed with the consent and approval of the company's Managers, Officers, and Compliance Managers.

The written Information Security Plan outlines the company's overall corporate-wide program to detect, prevent, and mitigate electronic information security breaches. Elements of the program apply to all company employees, contractors, affiliates, third party service providers, secondary market investors, insurers and agencies. Every entity that owns, licenses, stores, or maintains personal identifying information is responsible for ensuring compliance to the plan.

Sample Client has a duty to protect the information of a Massachusetts resident that has been received by the company in connection with employment, the provision of goods or services including the origination, processing, approval, funding, settlement or servicing of a consumer's mortgage. The duty includes the requirement have a written program (WISP) to safeguard such information. If personal information of a consumer is electronically stored or transmitted, the security program must cover computers and portable and/or wireless devices. The WISP must be appropriate to the size, scope and type of business, available resources, the amount of stored data and the need for security and confidentiality of consumer and employee information.

## 1.2 Required Elements of the WISP

The Written Information Security Program (WISP) must provide administrative, technical and physical safeguards for personal information under 201 CMR 17.00. It must address a wide range of matters that include, but are not limited to:

1. Analysis of the reasonably foreseeable risks to the security, confidentiality and integrity of records, in any form, that contain personal information, of the effectiveness of any current safeguards for limiting those risks, and of the need to develop improved safeguards;
2. Policies and procedures relating to employee training on the importance of the WISP, its specific requirements, the consequences of failure to comply with those requirements, and prevention of access by former employees;
3. For paper records, provisions for secure storage of materials containing personal information, including restrictions on physical access to such records and, for electronic records, control measures that restrict access and include secure user authentication protocols;
4. Encryption of personal information that is stored on computers, laptops or other portable devices or is transmitted across public networks or transmitted wirelessly;
5. Provisions to ensure that any electronic records system that is connected to the internet includes firewall protection and operating system security patches, that security software includes malware protections and virus definitions, and that all these programs are reasonably current as of March 1, 2010 and will be updated on a regular basis thereafter;
6. Oversight of third-party service providers who have access to personal information, including a process to select and retain service providers that are able to maintain appropriate security measures consistent with 201 CMR 17.00
7. Regular monitoring to ensure that the WISP operates effectively to protect both paper and electronic records, to detect any unauthorized use of or access to personal information, and to identify any areas where upgraded safeguards are needed;

8. Review of the WISP's scope at least annually, and whenever there is a material change in business practices that may reasonably implicate the protection of personal information; and
9. Documentation of responses to any breach of security and of any actions taken thereafter to change practices relating to the protection of personal information.

### 1.3

#### Designation of a Compliance or Security Compliance Officer

Sample Client has designated a responsible person to serve as a Security Compliance Officer. The officer shall be responsible for the development and implementation of the plan, dissemination of materials, and staff training. Members of senior management are responsible for ensuring the role of the Compliance or Security Compliance Officer is carried out adequately and that a second-in-command person be trained to serve in the absence of the security officer. Every employee is required to sign an acknowledgement that he/she has read and understands all components of the plan.

On at least a quarterly basis the Security Compliance Officer is to make a written report to the Managers and Officers regarding the status of the company's compliance activities. Listed are the general areas of responsibility of the Security Compliance Officer.

1. Development and updating of the WISP
2. Overall administering of the plan
3. Development and delivery of employee training
4. Creating the list of security procedures
5. Assigning the level of risk to security procedure
6. Development of forms and recordkeeping materials
7. Coordination of audit functions
8. Report results of audits to senior management
9. Ensuring related policy and procedures ensure compliance with the program, including:
  - *Consumer privacy policy*
  - *Information security policy*
  - *Vendor management*

## 1.4 Program Development and Implementation

On an annual basis, Sample Client's Managers and Officers shall review the plan, audit reports and assess the merits of the plan. Changes and recommendations shall be discussed and approved. As appropriate and in accordance with the Sample Client's growth as well as changes to the company's business model, service delivery platforms, and expanded market areas, the foregoing plan shall be amended by the Security Compliance Officer. Revisions shall be submitted and approved by senior management. Applicable training and dissemination of updated materials shall be provided to all employees, affiliates, and service providers.

The company's Managers and Officers are responsible for ensuring the overall effectiveness of the plan and providing assistance to Security Compliance Officer. Listed are the key responsibilities of the managers and officers:

1. Reviewing and approving the company's Written Information Security Plan and recommending updates or changes
2. Monitor changes to federal and Massachusetts laws and mandates to ensure the company has the tools and resources to remain compliant
3. Providing guidance and assistance to the Security Compliance Officer charged with administering the program
4. Review audit reports and results of regulatory examinations
5. Review the company's response to incidents
6. Assess overall effectiveness on a periodic basis

## 1.5 Employee Training

Sample Client requires training for all employees about identify theft and electronic security measures. Training shall be completed annually and include updated information and requirements for the mortgage industry. All new hires must receive identity theft and electronic security training within 30 days of hire. This policy manual must be included as part of the training program. All staff shall be trained to detect electronic security breaches with regard to new applications as well as the refinancing of borrowers whose prior confidential information is retained by the company. All staff should also be trained to mitigate security breaches, whether or not it is the employee's responsibility to complete the detection and mitigation steps.

## 1.6 Definitions

1. **Breach of Security:** Unauthorized use of or access to encrypted or unencrypted personal identifying information and the process by which the security or integrity of the information is compromised. Also, an entity or person who creates a substantial risk of identity theft or misuse of personal identifying information against a citizen of the Commonwealth. An unauthorized but good faith acquisition for lawful purposes of personal information by a person, agency, employee, or agent is not a security breach unless the information is further disclosed or at risk of further disclosure or is used in an unauthorized manner.
2. **Electronic:** Technology having electronic, wireless, magnetic, digital, electromagnetic, or similar capabilities.
3. **Encrypted:** Data which is transformed whereby meaning is not assigned without a confidential process or key.
4. **Owns or Licenses:** An entity that stores, maintains, receives, processes, or has access to personal identifying information used to provide goods or services or in relation to employment.
5. **Person:** A natural person, corporation, entity, agency, partnership, association, or the like other than an agency or office of the Commonwealth or any political subdivision.
6. **Personal Information:** A resident of the Commonwealth's first name and last name or first initial and last name in combination with one or more of the following:
  1. Social Security Number
  2. Driver's License Number or State-Issued Identification Card Number (or)
  3. Financial Account Number, Credit or Debit Card Number, with or without any security code or PIN.

Personal information does not include any information lawfully obtained from publicly available information or government records.
7. **Record or Records:** Material where written, spoken, drawn, visual, or electromagnetic information is recorded or preserved.
8. **Service Providers:** A person, who receives, stores, transmits, processes, or has authorized access to personal information in connection with providing services or goods directly to a resident of the Commonwealth.

- 9. Address Discrepancies:** Notices sent to lenders by credit agencies informing the company of a substantial difference between the information provided on the request order form with the agency's database. Mandatory response steps include cross-checking data, verifying directly with the consumer, and submitting a confirmation to the credit agency.
- 10. Identity Theft:** A fraud committed or attempted using the identifying information of another person without authority.
- 11. Identify Theft Report:** A report filed by a consumer to an appropriate local, state or federal law enforcement agency that alleges an identity theft or suspicious activity.
- 12. Incident Response:** A report filed by the company to authorities that describes an information security breach or suspicious activity.
- 13. Risk Assessment:** An evaluation of the risk to the company regarding any exposure of identity theft to the consumer.
- 14. Response:** Action that the company takes to mitigate exposure to confidential consumer information.
- 15. Suspicious Activity Report (SAR):** A federal form submitted to a law enforcement agency that describes the suspicious activity and identifies all known parties.

## 1.7

### Consumer Privacy Policy

Sample Mortgage Client requires all employees, affiliates and service providers to comply with the Gramm-Leach-Bliley Consumer Privacy Act (GLB) regarding the disclosure of their privacy policies and practices. Disclosures must contain language with respect to information sharing with third parties on financial products for personal, family and household purposes. The disclosure applies to all consumers who apply for a financial product, regardless of whether the credit is extended by the company.

Sample client's policy pertains to web-based, telephone or written mortgage applications. The company's employees, affiliates and third party providers are required to comply with the GLB act for information sharing with any of the following:

- Credit Agencies
- Appraisers
- Designated Underwriters
- Mortgage Insurance Companies
- Mortgage Investors
- Document Preparation Companies
- Closing Agents
- Electronic Business to Business Portals
- Outsource Quality Control Firms

The Privacy Notice must contain language to inform the borrower that personal information will not be shared with third parties and must be given to the borrower when the loan application is taken. Borrowers who inquire company to review existing documents for the purpose of refinance eligibility must be given the notice with or without completing an application.

## 1.8 Third Party Service Providers

Sample Client will select and oversee third party service providers in order to safeguard personal identifying information. The company shall take all reasonable steps necessary to use third party service providers that use proper security safeguards and measures that are consistent with the foregoing policy. Gramm-Leach-Bliley (GLB) requires that privacy agreements are executed between business entities and its affiliates to ensure that the information received by the business is not disclosed to any third party, sold to marketing companies or list distributors or engage in any act that is in violation of the Gramm-Leach-Bliley Consumer Privacy Act.

Sample Client shall require third party service providers to disclose and detail their electronic security measures and may require such measures to be detailed in the service providers' contracts with the company. Privacy agreements shall be executed between the company and all third party service organization hired to conduct credit investigations, background checks, certain asset or income verifying procedures and post-funding quality control reviews on behalf of the company.

The agreement shall require the third party to maintain the confidentiality of the information to at least the same extent that the company must maintain confidentiality under the 201 CMR 17:00 and the Gramm-Leach-Bliley Act. Third party service providers are prohibited from disclosing or using the information other than to carry out the purposes for which the third party is contracted in the ordinary course of business. Included in the privacy agreement shall be a provision for the proper destruction of documents.

## 1.9

### Safeguarding of Confidential Information

Employees may have access to confidential information contained in the company's customer data base. All loan originators, processors, and other staff-members referencing file documents from former customers for the purposes of evaluation and processing and application shall adhere to the policies set forth regarding use and re-use of consumer information and information-sharing. For direct marketing to prior customers, the consumer may be unaware of what information, and the extent of information, that has been made available to the company representative, who may be a different loan originator. In these cases, caution must be exercised to assure the borrower that access to their information was duly authorized and in compliance with privacy regulations. For purposes of this policy, confidential information includes, but is not limited to:

- *Information regarding personnel who are currently or formerly employed by the company*
- *Procedures for computer access and passwords of employees and system users.*
- *Any information pertaining to mortgage borrowers who have closed loans with the company*
- *Any information regarding mortgage applicants whose loans were closed for incompleteness, withdrawn, denied or counter-offer not accepted.*
- *Prospect information concerning potential customers of the company*
- *Any other information relating to the company's research, marketing, operations, investors, warehouse lenders and secondary marketing agencies.*

## Section 2

### Electronic Security System

#### 2.1 Computer System General Requirements

Sample Mortgage Bank has established and maintains a security system that covers its computers and wireless system in order to protect against unauthorized access to personal identifying information. At a minimum, this security system implements:

1. Secure user authentication protocols
2. Secure access control methods, including passwords and identification procedures
3. Encryption of transmitted records and files
4. Encryption of any personal identifying information transmitted over a public or wireless network and stored on laptops or other portable devices
5. Up to date firewall protection and security patches
6. Up to date security software including malware and virus protection with security patches
7. Reasonable monitoring for detection of unauthorized access to information
8. Education and training of employees in the best practices for information security

#### 2.2 E-Mail Policy

Sample Client's e-mail system is designed to improve service to customers, enhance internal communications, and reduce paperwork. Employees using the company's e-mail system must adhere to the following policies and procedures:

1. The company's e-mail system, network, and Internet/Intranet access are intended for business-use only. Employees may access e-mail and the Internet for personal use only during non-working hours, and strictly in compliance with the terms of this policy.
2. All information created, sent, or received via the company's e-mail system, network, Internet, or Intranet, including all e-mail messages and electronic files, is the property of the company.

3. The company reserves the right, at its discretion, to access, read, review, monitor, and copy all messages and files on its computer system at any time and without notice. When deemed necessary, the company reserves the right to disclose text or images to law enforcement agencies or other third parties without the employee's consent.
4. Any message or file sent via e-mail that contains borrower information of any type must have the employee's name attached.
5. Information transmittals must utilize extreme caution to ensure that the correct e-mail address is used for the intended recipient(s).
6. Any mortgage documents, including closing packages, and/or confidential customer information sent to service providers must be properly protected by a firewall or other appropriate security device(s) and/or software and transmitted through SSL systems.
7. All borrower confidential information cannot be sent via e-mail unless encrypted by company approved encryption software and according to established company procedure in effect at the time of transmittal. This includes, but is not limited to, the transmission of customer financial account numbers, Social Security numbers, and other non-public consumer information.
8. Any mortgage documents, including closing packages, and/or confidential customer information sent to service providers must be properly protected by a firewall or other appropriate security device(s) and/or software and transmitted through SSL systems.
9. Employees must provide the System Administrator and/or Information Security Compliance Officer with all passwords. Passwords may not be changed without permission.
10. Only authorized management personnel are permitted to access another person's e-mail without consent and access shall be limited for the business related purposes except for unforeseen circumstances requiring access for other purposes.
11. All messages archived in the company's server, network and workgroup computers shall be deemed company property. Employees must archive messages to prevent them from being automatically deleted. Employees are responsible for knowing the company's e-mail retention policies.

12. Misuse and/or abuse of electronic access, including but not limited to, personal use during working hours, copying or downloading copyrighted materials, unprofessional content searches or messages will result in disciplinary action, up to and including termination.

### 2.3 Network and Internet Policy

Network configurations enable loan processors, originators, closing coordinators, and administrative staff to access certain files. All rules and policies with respect to consumer information apply to files accessed among network users. Safeguarding confidential information involves local area network (LAN) and wide area network (WAN) configurations. The company requires all users having access to networked information comply with the safeguarding of confidential information, as follows:

1. Sample Client reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the network and the Internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received, or stored in connection with this usage.
2. Use of network and Internet access extends throughout an employee's term of employment, providing the employee does not violate the company's policies regarding network, Internet or Intranet use.
3. By accepting an account password, related information, and accessing the company's network or Internet system, an employee agrees to adhere to company policies regarding their use. Employees agree to report any misuse or policy violation(s) to the Security Compliance Officer.
4. Sample Client reserves the right to suspend access at any time, without notice, for technical reasons, possible policy violations, security or other concerns.
4. Sample Client, at its sole discretion, will determine what materials, files, information, software, communications, and other content and/or activity will be permitted or prohibited. All such information, content, and file are the property of the company.

5. Network administrators may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring employees are using the system consistently with this policy.

## 2.4 Electronic Access

Sample Client provides every employee with electronic access to all employees that handle loan origination, closing and post-closing information. Personnel are assigned an e-mail address, a network connection, and Internet access. This policy governs all use of the company's network, Internet access, and e-mails system at all company locations and offices. This policy includes, but is not limited to, electronic mail, chat rooms, the Internet, news groups, electronic bulletin boards, the company's VPM / Intranet, and all other company electronic messaging systems. This policy governs the information security for all documentation utilized by the company and its affiliates, whether the communication is made by telephone, mail, facsimile, courier, or any electronic system.

## 2.5 Prohibited Activities

Sample Client's employees and contractors are prohibited from using the company's e-mail system, network, or Internet/Intranet access for the following activities:

1. Downloading software without the prior written approval of the Security Compliance Officer.
2. Printing or distributing copyrighted materials. This includes, but is not limited to, software, articles and graphics protected by copyright.
3. Using software that is not licensed by the manufacturer or approved by the company.
4. Sending, printing, or otherwise disseminating the company's proprietary data or any other information deemed confidential.
5. Operating a business or otherwise engaging in commercial activity outside the scope of employment.

6. Sending or forwarding messages containing borrower consumer credit or confidential information or account numbers.
7. Sending or forwarding a message that discloses personal information without authorization. This shall also include accessing, transmitting, receiving, or seeking confidential information about borrowers or mortgage transactions without authorization.
8. Using another employee's password or impersonating another person while communicating or accessing the network or Internet.

## 2.6 Authorized Use of Software

Sample Client purchases, leases, or maintains site licenses for computer software applications from a variety of commercial manufacturers. To ensure compliance with software license agreements, the company's security policy, and to prevent identity theft resulting from shared, copied, or unauthorized downloading of software programs, applications, and data, all employees must adhere to the following:

1. Software must be used in accordance with the manufacturer's license agreements. Employees acknowledge they do not own the Loan Origination System (LOS), Desktop Originator, Loan Prospector, or other mortgage pre-qualification programs used in connection with an adjunct to the firm's LOS system that are supplied by the company.
2. Employees may not make additional copies of any software, unless expressly authorized by the company and software publisher.
3. Any employee who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to the company, or who places or uses unauthorized software on the company premises or equipment shall be subject to disciplinary action or termination.
4. Employees must obtain permission from the Security Compliance Officer prior to installing personal software onto the company's computer system. Employees are not permitted to copy software from the company's computer system for installation on home or other computers without prior authorization.

5. In cases that require an employee to use software at home, the company will purchase an additional copy or license. Employee acknowledges that any additional copies or licenses purchased for home use are the property of the company. Employees who are required to use software at home should consult with the Security Compliance Officer to determine if appropriate licenses allow for home use.
6. Employees who suspect or become aware of software misuse by any employee are required to notify the Security Compliance Officer in confidence.

## 2.7 Administrative Access Control

The Security Compliance Officer shall maintain confidential passwords and access codes for technology on a corporate-wide level. The company President, and key personnel shall have copies of access code information. Changes in personnel, termination, extended leave, etc. shall warrant changes in passwords or other access code. All changes must be documented by memorandum and placed as an addendum to this policy manual.

## 2.8 Firewall Procedures

This policy guide includes a systemized plan for design and maintenance of firewalls in the company's computer systems. The firewall policy serves as a variable component of the company's overall security policy, depending on the extent of internet access by the company's employees. The firewall policy and implementation must cover each of the following elements:

- *Ensure the system is able to examine information content*
- *Ensure that logging functionality is consistent with access controls*
- *Support advanced user authentication*
- *Detect intrusions*
- *Respond to intrusions*
- *Cover domain name, HTTP, SMTP, DNS and IP traffic*
- *Website spoofing*
- *Cover all levels of firewall protection, such as:*
  - ✓ *Packet filtering*
  - ✓ *Proxy services*
  - ✓ *Application-level firewalls*
  - ✓ *Phishing*
  - ✓ *Pharming*
  - ✓ *Spyware*

## 2.9 Firewall Procedures

The site for maintaining the information systems components must have the least amount of exposure from internal and external sources. The site should be checked for exposure from fire, flood, and environmental hazards. Windows and doors must be secure and the location should not be identified by signage. Detection devices should be used where applicable to prevent theft and safeguard equipment.

Sample Client must ensure that outside services providers such as cleaning personnel who are not required to sign the Services Provider Agreement, may unwittingly access confidential information of borrowers while cleaning carpets, emptying trash, etc. It is imperative that desks, conference tables, photocopying centers, are cleared of confidential documents to avoid exposure.

## 2.10 Incident Response and Preparedness

Sample Client must respond to information security incidents to ensure the protection of confidential consumer information. The federal Anti-Cybersquatting Consumer Protection Act (ACCPA) allows the company to initiate immediate action in federal district court under section 43(d) of the Lanham Act, 15 USC 1115(d). The following resources can be used to disable a spoofed website, recover customer information and mitigate other types of security threats:

- A complaint can be filed with the Internet Fraud Complaint Center a partnership of the FBI and the National White Collar Crime Center at: <http://www.ifccfbi.gov/>
- The Uniform Domain Name Dispute Resolution Process (UDRP) resolves disputes for names or trademarks that have been illegally infringed upon. The company is to take action against domain name registrars to stop a spoofing incident. Information is explained at: <http://www.icann.org/udrp/udrp-policy>
- Digital Phishnet is a joint initiative of industry and law enforcement designed to support apprehension of perpetrators of phishing-related crimes, including spoofing. The FTC, FBI and Secret Service and other electronic crimes tasks forces assist financial institutions in identifying persons involved in phishing-type crimes. <http://www.digitalphishnet.com/>

## 2.11 Document Destruction

Credit reports, mortgage applications, financial statements, tax returns, paystubs, W-2 forms, retirement income documentation, etc. and numerous other documents that contain the borrower's Social Security Numbers, names of financial institutions, account numbers, etc. must be destroyed using any of the following methods:

- *Commercially-built Mechanical Shredder*
- *On-site Services provided by Shredding Service company (such as Shred-It, or other licensed commercial provider)*

Wrinkling of documents, tearing into sections and disposing into the office trash is not acceptable, as long as there is any way that confidential information can be retrieved. Original loan documents that are removed from the office for the purpose of at-home work must be kept in a safe, secure area during travel and the off-site location. Any lost or misplaced confidential documents must be reported to the Security Compliance Officer immediately. Any employee, representative or affiliate of the company found disposing credit reports or any income, asset, liability information of consumers in any outside of public accessible area shall be subject to disciplinary action, including termination.

## 2.12 Breach of Security

A breach of security occurs when there is an unauthorized use of or access to encrypted or unencrypted personal identifying information of a resident of the Commonwealth. A security breach may also include an entity or person who creates a substantial risk of identity theft or misuse of personal identifying information against a citizen of the Commonwealth. An unauthorized but good faith acquisition of personal information for lawful purposes by a person, agency, employee, or agent is not a breach unless the information is further disclosed or at risk of further disclosure or is used in an unauthorized manner.

Sample Client will execute disciplinary measures for violations of this written information security plan as well as prevent terminated employees from having access to any personal identifying or company information.

**2.13**      **Monitoring**

Sample Client will engage in regular monitoring to ensure compliance with this written information security plan and to detect unauthorized access to personal identifying information. The company will monitor this plan to determine any changes or improvements needed to scrupulously protect consumers' personal identifying information. The Security Compliance Officer is responsible for monitoring compliance of vendors. The officer may designate an internal or outsourced auditor to conduct a review of the company's vendor management at least once per year and to report the results of the audit, including management responses, to management.

SAMPLE