MASSACHUSETTS HOUSING FINANCE AGENCY

INFORMATION SECURITY PROGRAM

Effective: November 1, 2016

I. SCOPE

A. Statement of Policy

Federal and state laws require that the Massachusetts Housing Finance Agency ("MassHousing" or the "Agency") protect certain personal information related to individuals who are our customers, business partners, vendors and employees. This Information Security Program ("Program") addresses how we keep such information secure and reduce the risks of its unauthorized disclosure.

MassHousing recognizes the importance of the personal information we maintain and the trust our customers, business partners, vendors and employees place in us to keep that information secure. MassHousing is committed to ensuring the security and confidentiality of sensitive personal information we have in our possession, including information that comes to us from our customers, business partners, vendors, or employees.

Because of the complex nature of ensuring information security, this Program is meant to serve only as a framework. This Program is intended to be used in conjunction with other policies and procedures developed by MassHousing, such as the Acceptable Use Policy which is part of the Human Resources Manual. This Program contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and activities of MassHousing; (b) the amount of resources available; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information.

Additional information security policies and procedures may be developed as necessary to implement the goals of this Program. This Program may be updated from time to time as necessitated by changes in law, industry practices or risk profile.

B. Information Covered by this Program

This program relates to information pertaining to individuals that MassHousing has in its possession ("Protected Information" or "PI"). This information falls into three main categories:

- "Nonpublic personal information" ("NPI") subject to protection under Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 *et seq.*) and implementing regulations (12 C.F.R. Part 1016);

- "Consumer reports" subject to protection under the federal Fair Credit Reporting Act, as amended by the 2004 FACT Act (15 U.S.C. § 1681 *et seq.*); and

- Other information pertaining to individuals subject to data security, data security breach notification and identity theft prevention laws in Massachusetts and various other states where applicable.

Definitions of "Protected Information", "nonpublic personal information" and "consumer reports" are set forth at Attachment 1 hereto. Information such as customer lists, account numbers, or any other nonpublic information relating to customers of MassHousing will likely be NPI.

Additionally, state laws protecting information pertaining to individuals, including Mass. Gen. Laws ch. 93H, define the information protected in a broader manner. Generally, to constitute Protected Information under state law, information would include an individual's name along with another identifier such as a driver's license number, social security number or account number.

C. Legal Compliance

Regulations promulgated by the Consumer Financial Protection Bureau at 12 C.F.R. Part 1016, as well as SPR Bulletin No. 1-08 issued by the State Public Records Supervisor, Executive Order No. 504 (Order Regarding the Security and Confidentiality of Personal Information), 201 CMR Part 17, and other regulations, require MassHousing to develop a written information security program that describes our plan to protect such Protected Information. This Information Security Program constitutes MassHousing's compliance with these requirements.

II. RISK ASSESSMENT

In order to maintain information security, MassHousing should engage in an ongoing risk assessment and mitigation process. This process should review internal and external threats to information security (*e.g.*, hackers, employee misconduct, loss of data, *etc.*) and devise strategies for protecting against or mitigating such risks to acceptable levels.

MassHousing may augment its assessment of external threats with information received from industry information sharing sources, such as the Financial Services Information Sharing and Analysis Center, and federal and state government cybersecurity resources.

Actual security risks are subject to corrective action. Information security measures should be reviewed and tested annually, at a minimum.

All staff should continuously consider potential risks to protected information and should advise the appropriate Privacy Officer (see Part VI of this Program) if they recognize any previously unforeseen risks or potential solutions for mitigating risks. Part III of this Program contains controls designed to mitigate risks known to MassHousing. Additional controls may be added in the future to address unforeseen risks as they are discovered.

III. SUBSTANTIVE AREAS OF PROGRAM

Three areas are particularly important to MassHousing's information security: (A) employee management and training; (B) information systems; and (C) managing system failures.

A. Employee Management and Training

The success or failure of this Program depends largely on the employees who implement it. The term "employee" – in the context of this Program – also includes workers retained through a contractual arrangement for services who are provided access to MassHousing's network and/or data. Therefore, the following steps should be taken:

- All candidates for employment – including those workers from service providers who are granted access to MassHousing's network – are subject to background checks as set forth in the MassHousing Human Resources Manual.

- Each employee must be informed of and be required to comply with MassHousing's confidentiality and security standards for handling Protected Information. All employees will from time to time be required to acknowledge that they have read and will comply with MassHousing's confidentiality and security standards for handling Protected Information. The current Information Security Program and all updates are posted on the internal and external MassHousing websites and are referenced in the Human Resources Manual.

- Employees receive training on and are required to take basic steps to maintain the security, confidentiality and integrity of Protected Information, including but not limited to:

    - locking rooms and file cabinets where paper records are kept;

    - utilizing the proper method for disposal of paper records or computer media containing Protected Information;

    - using password-activated screensavers;

    - using strong passwords (at least eight characters long, and contains at least one uppercase letter and a combination of two or more of the following: lower case letters, numbers, punctuation marks);

    - changing passwords periodically, and not posting passwords near employee's computers;

    - ensuring that malicious code is not downloaded onto MassHousing's network (*e.g.*, by not opening attachments on suspicious emails, or by not accessing social media websites and/or applications which may contain viruses and/or malware, *etc.*); and

    - recognizing any fraudulent attempt to obtain Protected Information and reporting it to supervisors and/or Privacy Officers.

- Employees who believe their password has been compromised must notify the Help Desk immediately.

- Employees and other authorized network users:

  - are not permitted to connect non-MassHousing approved devices to the MassHousing network or to MassHousing's computers;

  - should not use web-based email services such as Hotmail, Gmail, Yahoo! Mail and others to conduct MassHousing business. Such web-based e-mails may be accessed from MassHousing's network but for incidental personal use only; but

  - may share and store files on an Internet-based (sometimes called a "cloud computing") service (*e.g.*, DropBox, Google, *etc.*) managed by an Agency business partner, provided that users must not share or store Protected Information on those services.

- All employees have been instructed regarding MassHousing's policy – and the legal requirement – to keep Protected Information secure and confidential. Reminders about employees' responsibility for security are posted in common areas.

- Each employee is responsible at all times for any Agency equipment provided to him or her and must report any loss of this equipment to the Help Desk immediately by calling the Help Desk during business hours, or if the loss is detected after normal business hours by sending an email to the Help Desk.

- Access to Protected Information is limited to employees who have a business reason for accessing the information. Access to Protected Information is granted to employees who respond to customer inquiries, but only to the extent they need it to do their job.

  - All employees with a business need to work with or have access to Protected Information are instructed to work with Protected Information in MassHousing's office space (in the case of paper records) or through MassHousing's computer network (in the case of electronic information).

  - All employees with a business need to work with Protected Information off-site must do so with prior approval from a Privacy Officer and use of an encrypted MassHousing-owned device.

  - All employees with a business need to work offsite and access applications or systems on MassHousing's network must do so through a secure, VPN connection, or using MassHousing-supplied security software (such as GoToMyPC).

  - No MassHousing data is allowed to be stored on devices not owned or controlled by MassHousing. Employees may use a non-Agency device to access Agency eMail using Outlook Web Access (OWA) or may access Agency computing resources using GoToMyPC or other security software supplied by MassHousing's

Information Technology Division (IT), so long as no MassHousing data is stored on the non-Agency device and MassHousing is allowed to wipe any sensitive information or applications from such device, if applicable.

- MassHousing prohibits the removal from MassHousing's office space, any Protected Information that is not encrypted, and it further prohibits the transmission of any Protected Information to an employee's home email account, home computer, personal device or an information store including "Cloud computing services" referenced above, except as otherwise explicitly permitted by this Program.

- Users may share Protected Information with governmental agencies and government-sponsored enterprises (*e.g.*, HUD, FNMA, DHCD, *etc.*) that partner with MassHousing, either by using the MassHousing encrypted methods listed below or the method specifically requested by that partner agency:
  - by sending an encrypted email (via the "Send Secure" feature in Outlook);
  - by sending an encrypted CD-ROM or DVD (available through the IT Help Desk) by overnight courier or another method whereby delivery and receipt may be tracked;
  - by using a portal established for that purpose by IT on MassHousing.com; or
  - by using a secure mechanism provided by IT specific to that business partner.
- Users may share Protected Information with non-government business partners that have entered into a contract with MassHousing in accordance with Section IV.B of this Program, provided that Protected Information is encrypted using one of the following methods:
  - by sending an encrypted email (via the "Send Secure" feature in Outlook);
  - by sending an encrypted CD-ROM or DVD (available through the IT Help Desk) by overnight courier or another method whereby delivery and receipt may be tracked;
  - by using a portal established for that purpose by IT on MassHousing.com; or
  - by using a secure mechanism provided by IT specific to that business partner.
- MassHousing may monitor employees' activities on MassHousing's network and may periodically test employees' sensitivity to potential cyber-threats (*e.g.*, by testing responses to simulated "phishing" email messages or simulated malware attachments).
- Disciplinary measures shall be imposed for any breaches of MassHousing's Information Security Program, as provided for in MassHousing's Human Resources Manual.

- Disclosing confidential and proprietary information to parties who are not specifically authorized to receive such information may constitute a fraudulent act under MassHousing's Fraud Policy.

- Immediately upon termination of employment, the departing employee is no longer authorized to access MassHousing's network or information. The departing employee's access to MassHousing's network is removed by IT staff.

B. Information Systems

Information systems include the network and software applications, and information processing, storage, transmission, retrieval, and disposal. MassHousing will maintain security throughout the life cycle of Protected Information – that is, from data receipt to data disposal – in the following manner:

- Records containing Protected Information are stored only in secure areas, and only authorized employees will have access to such areas.

    - Paper records are stored only in a room, cabinet, or other container that is locked when unattended.

    - MassHousing's IT data center is restricted to authorized staff through a security card system. The data center is further monitored by closed circuit television equipment.

    - MassHousing's IT data center is monitored by an alarm system for heat, humidity, smoke, fire and water. If the alarm activates, building management and IT staff are notified (24 hours a day).

    - Secure backup media are maintained and archived data is kept in a secure area.

- Secure data transmission (with clear instructions and simple security tools) are provided whenever Protected Information is collected or transmitted by MassHousing. Specifically:

    - When Protected Information is collected or transmitted, a Secure Sockets Layer (SSL) or other secure connection must be used so that the information is encrypted, using 128-bit encryption (at a minimum), in transit.

- MassHousing recognizes the emergence of cloud computing services as a valuable business tool and endeavors to make the use of such services available to its employees and authorized users, provided that such use does not expose the Agency, its customers, business partners, vendors or employees to unacceptable levels of risk.

    - Placement of Agency business-related data in data centers managed by third parties requires careful consideration and contractual arrangements, thus decisions to utilize cloud computing services will be made on a case-by-case basis as follows:

- Privacy Officers may propose the use of cloud computing services to meet a business need. The Director of Information Technology must evaluate the requested cloud computing service to ensure information continuity and security. If the service meets Agency information continuity and security standards, then the Privacy Officer may negotiate and enter into an appropriate contract for the service in accordance with Section IV.B of this Program. Such contracts cannot be entered into without this review being completed. Furthermore, such contracts cannot be entered into unless they are in compliance with the Agency's Procurement Policy.

- In those cases where the Agency contracts for services with a cloud computing service provider, the service must be configured to provide backup of the Agency's data or a provision must be made for the data to be duplicated on the Agency's computing platform. To the extent that either of these alternatives is not feasible, the Privacy Officer is responsible for maintaining an inventory of Agency information stored on a cloud computing service.

- All other provisions of this Program apply to cloud computing services to the same extent such provisions relate to the transmission, storage and security of information using other media.

- Laptops and other portable equipment such as notebooks, tablets, portable digital assistants (PDAs), cell phones and cell phone/PDA combinations supplied by the Agency are Agency assets. They are to be used for business purposes, in adherence with this Program and MassHousing's Acceptable Use Policy. All Protected Information on portable equipment must be encrypted, using 128-bit encryption (at a minimum).

- Password reset requests should only be provided to employees via voicemail to a pre-determined phone number (*i.e.*, home number, office number) or in person. The IT Help Desk staff will not provide a password to someone over the telephone.

- MassHousing's servers and computing facilities are equipped with technology that allows for the detection of intrusion, including, for example, repeated denied log-in requests.

- Protected Information must be disposed of in a secure manner, consistent with applicable laws, including the federal Fair Credit Reporting Act and Mass. Gen. Laws ch. 93I.

    - Administrative Services will provide secure disposal mechanisms for paper records (shredders, disposal shred-it bins, bulk disposal arrangements, *etc*.);

    - Information recorded on paper will either be shredded or stored in a secure container until a shredding or secure disposal service picks it up;

- Computer Services will provide secure destruction mechanisms for electronic media prior to releasing media to Administrative Services for disposal;

- When disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that may contain Protected Information, all data must be erased using a method that ensures that it cannot be reconstructed;

- Outdated Protected Information must be promptly disposed of in accordance with applicable MassHousing policies and procedures; and

- When any media containing Protected Information must be disposed, it must be redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed.

> Note: MassHousing's obligation to retain documents containing Protected Information may be governed by other federal and state requirements, including those relating to public records and financial services regulation. The disposal policies contained in this Information Security Program relate solely to records that may be destroyed consistent with applicable laws and MassHousing policies and procedures.

- Appropriate oversight and monitoring is used to detect the improper disclosure or theft of Protected Information in whatever form.

- A detailed inventory of MassHousing computing resources is maintained.

C. Managing System Failures

Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. Therefore, MassHousing will:

- Maintain up-to-date and appropriate programs and controls by:

  - following a written contingency plan to address any breaches of its physical, administrative or technical safeguards;

  - checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities;

  - using anti-virus software that updates automatically;

  - maintaining up-to-date firewalls; and

  - providing central management of security tools for employees and providing notification concerning any actual or potential security risks or breaches.

- Take steps to preserve the security, confidentiality and integrity of Protected Information in the event of a computer or other technological failure.
    - MassHousing's data are backed up regularly per the Agency data backup schedule.
- Maintain systems and procedures to ensure that access to Protected Information is granted only to legitimate and valid users. Strong passwords combined with personal identifiers are used to authenticate the identity of internal and external users who are authorized to do business with MassHousing electronically.
- Take action under MassHousing's Security Incident Response Plan, if Protected Information is the subject of loss, damage or unauthorized access.

IV. VENDOR MANAGEMENT

A. Access and General Requirements

Service providers should be granted access to Protected Information on the same "need to know" basis as MassHousing employees. Service provider personnel who are granted access to MassHousing's network should be issued network access IDs by the same process that applies to MassHousing employees. MassHousing must seek to ensure that when service providers are allowed access to MassHousing Protected Information, such service providers:

- Abide by all terms of this Program while working at MassHousing's facility, while using MassHousing Protected Information, or while connected to MassHousing's network;
- Do not allow access to MassHousing information, whether Protected Information or not, to the vendor's or service provider's employees who have not been subject to the same pre-employment screening procedures to which other service provider personnel are subject;
- Cooperate with MassHousing in any investigation or audit in the event of any kind of security breach or lost or corrupted data;
- Cooperate with any regulatory inspection, investigation or other governmental action to which MassHousing is subject;
- Do not retain, resell, transfer, or convert for its own use any information, whether Protected Information or not, supplied by or obtained from MassHousing for any reason without MassHousing's prior consent;
- Have appropriate confidentiality and safeguard procedures for Protected Information;

- Provide MassHousing with documentation relative to security controls in place and in force upon request;

- Provide notification immediately upon a breach or suspected breach of any organization controls that may impact MassHousing Protected Information; and

- Maintain all MassHousing data within the United States.

B. Contracts with Vendors and Service Providers

For all vendor arrangements, MassHousing should ensure that that each contract with the vendor contains provisions requiring the vendor to:

- implement and maintain measures designed to meet the information security objectives of applicable law;

- use and disclose the customer information received from MassHousing solely for the purposes of performing its services for MassHousing; and

- provide MassHousing with copies of external audit reports or tests of the effectiveness of its information security measures.

The foregoing provisions shall be incorporated by reference into any agreement with a vendor that has agreed to comply with this Information Security Program.

C. Ongoing Monitoring and Oversight of Service Providers

Periodically during the term of MassHousing's agreement with vendors whose services include the handling of Protected Information, MassHousing's Director of Information Technology reserves the right to request evidence of compliance with the Information Security Program including but not limited to copies of external audit reports or tests of the effectiveness of such vendor's information security measures.

In the event that the reports or tests indicate that such vendor's information security measures are inadequate or otherwise put MassHousing's Protected Information at risk, MassHousing's Director of Information Technology shall report such results to MassHousing's General Counsel and Chief Administrative Officer, and they shall either take appropriate steps to cause the vendor to remedy the deficiency or terminate the arrangement.

V. INCIDENT RESPONSE

Any incident where Protected Information is subject to accidental public release or unauthorized access (or suspected unauthorized access) is extremely serious and must be reported immediately. Any MassHousing employee who becomes aware of or suspects that there has been an incident involving Protected Information must report that incident to a Privacy Officer and the Help Desk as soon as possible.

The specific incident response activities must be handled in accordance with MassHousing's Security Incident Response Plan, which contains procedures that address data security breach notification requirements. MassHousing shall document the nature of any such event in sufficient detail to compile any notices required by applicable law and such other information as may be required to assess the nature of the event. As soon as practicable following completion of MassHousing's investigation of any accidental public release or unauthorized access of Protected Information, MassHousing will review applicable policies and procedures and make such changes as are appropriate in light of the findings of such investigation.

VI. INFORMATION SECURITY & COMPLIANCE TASK FORCE

The Information Security & Compliance Task Force shall be responsible for identifying, from time to time, the Agency positions which serve as the "Privacy Officers." Privacy Officers shall be responsible for coordinating, implementing, testing and monitoring this Information Security Program. The current Privacy Officers are identified in Attachment 2. The Information Security & Compliance Task Force will take reasonable steps to periodically adjust this Information Security Program in light of routine testing and monitoring of the current program, any material changes to MassHousing's operations or business arrangements, or any other circumstances that MassHousing Privacy Officers know or have reason to know may have a material impact on this Information Security Program.

Attachment 1

Definition of Protected Information

For this Information Security Program, the term "Protected Information", abbreviated as "PI", is an all-inclusive term for information that is defined in various laws referenced in Section B – Information Covered by this Program, and in Section C – Legal Compliance, of Part I – Scope of this document. These laws use a variety of terms including "Personal Information", "Nonpublic Personal Information" (NPI) and "Consumer Reports". This attachment summarizes each of their definitions.

Definition of Personal Information

The following definitions are included in Mass. Gen. Laws ch. 93H, §1

"Person": a natural person, corporation, association, partnership or other legal entity.

"Personal information": a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

(a) Social Security number;

(b) driver's license number or state-issued identification card number; or

(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Definition of Nonpublic Personal Information

Nonpublic Personal Information ("NPI") is any "personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available."

NPI is:

- any information an individual gives you to get a financial product or service (for example: name, address, income, Social Security number, or other information on an application or personal financial statements). Even if a MassHousing financial product or service is requested by a business entity, any individual information, such as personal Social Security numbers on HUD Form 2530, is NPI;

- any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or

customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or

- any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

NPI does not include information that you have a reasonable basis to believe is lawfully made "publicly available." In other words, information is not NPI when you have taken steps to determine:

- that the information is generally made lawfully available to the public; and
- that the individual can direct that it not be made public and has not done so.

For example, while telephone numbers are listed in a public telephone directory, an individual can elect to have an unlisted number. In that case, that phone number would not be "publicly available."

Publicly Available Information Includes:

- federal, state, or local government records made available to the public, such as the fact that an individual has a mortgage with a particular financial institution; and
- information that is in widely distributed media like telephone books, newspapers, and websites that are available to the general public on an unrestricted basis, even if the site requires a password or fee for access.

Information in a list form may be NPI, depending on how the list is derived. For example, a list is not NPI if it is drawn entirely from publicly available information, such as a list of a lender's mortgage customers in a jurisdiction that requires that information to be publicly recorded. Also, it is not NPI if the list is taken from information that is not related to a lender's financial activities, for example, a list of individuals who respond to a newspaper ad promoting a non-financial product offered by a lender.

But a list derived even partially from NPI is still considered NPI. For example, a creditor's list of its borrowers' names and phone numbers is NPI even if the creditor has a reasonable basis to believe that those phone numbers are publicly available, because the existence of the customer relationships between the borrowers and the creditor is NPI.

Definition of Consumer Reports

"Consumer report" is defined as any communication or information "bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or

insurance to be used primarily for personal, family, or household purposes; or [any other permissible purpose].”[1] Information relating solely to transactions between the disclosing party and the consumer are not consumer reports.[2] Thus, any information that MassHousing receives from third parties bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living could potentially constitute Protected Information.

[1] 15 U.S.C. § 1681a(d)(1).

[2] 15 U.S.C. § 1681a(d)(2).

Attachment 2

Privacy Officers

The following positions are designated MassHousing's Privacy Officers and will coordinate implementation, testing and monitoring of this Information Security Program:

- Director of Rental Business Development
- Director of Rental Underwriting
- Director of Rental Management
- Director of Home Ownership Lending
- Director of Home Ownership Servicing & Operations
- Managing Director of Government Affairs and Communication
- Director of Information Technology
- Internal Auditor
- General Counsel
- Deputy General Counsel
- Financial Director (CFO)
- Managing Director of Administration
- Manager of Network and Computer Services
- Manager of Finance and Bond Compliance
- Director of Diversity & Inclusion