

Remote Access
Acceptable Use Policy and Guidelines
for MaineHousing Business Partners

INTRODUCTION

MaineHousing and its business partners rely on powerful computer technology to facilitate our ability to serve clients throughout the state of Maine. Every day, our information systems process, store, and transmit confidential client information and sensitive data. Securing this data and using care when it is accessed reduce the chances of harm.

Everyone at MaineHousing, as well as MaineHousing agents and contractors, share in the responsibility for maintaining the security of our information systems, data, equipment, and processes. The purpose of this document is to help you understand what you need to do in order to comply with MaineHousing's expectations for protecting our client's confidential information.

WHAT ARE "INFORMATION RESOURCES"?

The information resources covered under this Remote Access Acceptable Use Policy include both computer technology and confidential information.

Computer Technology: the equipment, systems, and networks used to acquire, process, transmit, and manage the information required to accomplish MaineHousing's mission, programs, and services. This technology includes all equipment used to connect to MaineHousing systems or store MaineHousing client information:

- computers, servers, and networking equipment
- hardware and software
- desk top computers and portable laptops
- portable data storage devices, such as CD's, DVD's, USB drives, and
- telecommunications equipment, such as desk phones, cell phones, fax services, mobile email and smartphone devices.

Confidential Information: protected or proprietary knowledge regarding MaineHousing's clients, staff and business.

- Protected information is any data that can be used to distinguish or trace an individual's identity. Maine State Statute specifically defines confidential information regarding applicants and clients participating in MaineHousing programs. MaineHousing must comply with other laws and agreements which govern management of confidential employee and/or financial information, including the protection of information verified or provided by the Social Security Administration.
- Proprietary information is data about MaineHousing's operation that could lead to breaches of security or degradation of services, such as account access information (passwords, etc.), server configurations or network diagrams.

MAINEHOUSING'S RESPONSIBILITY

In most organizations, an Information Security Officer (ISO) is responsible for coordinating information security programs and activities to ensure that compliance is maintained. At MaineHousing, because no one person performs all of the responsibilities of the ISO, an Information Security Committee (ISC) has been formed. The responsibilities of the Information Security Committee include:

- ensuring that appropriate processes are implemented to identify, measure, monitor, and control information security risks, and
- implementing security recommendations and changes resulting from compliance reviews, information technology audits, third-party vulnerability assessments and penetration tests.

YOUR RESPONSIBILITY

It is your responsibility to read, understand and comply with the Remote Access Acceptable Use Policy and Guidelines for MaineHousing Business Partners. Misuse of these Information Resources can result in damage to the reputation of MaineHousing and its business partners and lead to legal liability. Violation of these policies may result in the suspension of remote access privileges. Additionally, violators may be subject to civil and criminal prosecution.

Keeping protected information secure is an obligation mandated by state and federal laws, along with contractual agreements between MaineHousing and its partners – and it's the right thing to do.

If you have any doubt or questions regarding the security of computer resources or protected information, please alert your supervisor, who will then contact MaineHousing.

In a constantly changing technical environment, it is critical that everyone understands and follows the rules for utilizing technology and handling information.

INFORMATION PROTECTION

Personally Identifiable Information (PII) is any information about an individual that can be used to distinguish or trace an individual's identity. PII is also any other information that is linked (or linkable) to an individual, such as medical or financial information.

Examples of PII include, but are not limited to:

- **any** information provided by applicants or participants in MaineHousing programs (includes information provided by third parties working on behalf of an applicant/participant),
- personal identification numbers, such as social security number (SSN), passport number, driver's license number,
- financial account or credit card information, including account numbers, card numbers, expiration dates, cardholder name, or service codes,
- healthcare / medical information disclosed to MaineHousing,
- names and addresses of clients participating in MaineHousing programs or on waiting lists,
- the address of a shelter or other living accommodations for victims of domestic violence, or
- confidential information verified or provided by the Social Security Administration.

The format that the information is in **does not** matter! Paper records, electronic files, voice mail messages, and email can all contain protected information.

INFORMATION PROTECTION EXPECTATION

Do not disclose or discuss any protected information about MaineHousing clients to anyone – unless specifically authorized by your supervisor.

Any protected information must be encrypted or be handled by a secure delivery process. This includes emails, email attachments, CDs, USB drives, laptop drives, cell phones and other portable devices that contain files and emails with protected information.

WAYS TO PROTECT PERSONALLY IDENTIFIABLE INFORMATION

- Access only the protected information that relates directly to your job responsibilities. You must have business justification when accessing any protected information.
- Do not discuss client information with others unless it is required for you to perform your job responsibilities.
- Do not send protected information via e-mail unless the data is encrypted using a secure method.
- Protected information stored electronically must use encrypted media (e.g. encrypted flash drives, CD's, DVD's, etc.)
- Paper copies of protected data are just as important to protect as electronic versions.
 - Remove all documents that contain protected information from printers and fax machines immediately.
 - Do not leave protected files or paperwork on your desk or work area unattended, and do not leave protected information out in the open during non-working hours.
 - Lock up or secure all files at the end of the day.
 - Shred (or place in a secure container for shredding at a later time) all paper documents containing protected information that are no longer needed.
- Protected information must be transported only by an employee, the US Postal Service, an authorized courier, or other “track-able” delivery services.

Reporting: If you suspect or become aware of a failure to protect personally identifiable information, notify your contact at MaineHousing immediately, or ask your supervisor to immediately notify MaineHousing. MaineHousing has strict reporting requirements to appropriate State regulators and to the Social Security Administration within ***one hour*** of learning a breach or potential breach has occurred.

E-MAIL

Regular email is NOT a secure way to transmit protected information!

- Regular (non-secure) email should never be used to send or transmit protected data – contained in the body of the e-mail message or within attachments.
- If a client or another business partner sends you an unsecure e-mail containing protected information, be sure you DO NOT “reply” or “forward,” as this will re-send the information over the Internet. Compose a new email in response and request that the sender find an alternative method for sending protected data. Notify your supervisor, who will report the event to MaineHousing.
- If you do not have access to an application that encrypts e-mail, you may send an e-mail to your contact at MaineHousing and request that they send you a secure e-mail. You can then reply back to that e-mail (using the same secure e-mail system) and your e-mail and attachments will be encrypted.

All messages that reside on the MaineHousing.org mail server are the property of MaineHousing and *may be regarded as public information*, based on MaineHousing's obligations under the Freedom of Information Act. MaineHousing has the right to review, examine, archive, retrieve, restore, investigate, and delete all email messages.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

This means do not put anything into your e-mail messages that you would not want to see on the front page of the newspaper or be required to explain in a court of law.

CARE AND SAFETY OF PORTABLE COMPUTERS, PDAs, OTHER PORTABLE DATA STORAGE DEVICES

Be extremely careful how you handle laptop computers, CDs, DVD's and USBs (thumb drives, memory cards, sticks, etc.) or any other media that contain protected information.

- Portable storage devices should always be secured and properly stored. Never take portable data storage devices home or off-site with you unless you are specifically authorized to do so by your supervisor and you have a secure place to store them. If you are authorized to take protected information home or off premises, you must use encrypted media (e.g. encrypted flash drives, CD's or DVD's).
- Never dispose of portable data storage devices by putting them in the trash.
- Make sure your diskette drive, CD drive and USB ports are not easily accessible by clients. For example, if clients sit in your office, they shouldn't be able to easily reach the drives or ports. Your PC screen and paperwork should also be situated so that clients cannot easily view them. This may mean re-locating the PC screen and paperwork to a less visible place.
- When not in use, portable data storage devices must be secured and kept out of sight, even if you work in an area that is closed to the public.

ACCESS RESTRICTIONS

MaineHousing employees, as well as agents and contractors, are permitted access to areas of Information Resources appropriate to their job requirements. All users requiring the use of remote access for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs. Application forms must be approved and signed by the user's unit manager, supervisor, or department head before submission to MaineHousing.

Access to resources is achieved based on assigned user credentials, including a username, password, and a hardware security token.

- **The sharing of credentials is not permitted. You may not use the user name / password or security token assigned to someone else. In addition, leaving your credentials visible in plain sight or "hidden" in an obvious place is prohibited.**
- **You are prohibited from accessing or attempting to access information resources that are not specifically required to perform your job functions. If you inadvertently enter an unauthorized site or access unauthorized information (such as a folder, document, or database), end the access immediately, and report the event to your supervisor.**

PASSWORDS

The following password rules are required when accessing MaineHousing systems, and are recommended guidelines when logging in to any system (depending on system requirements).

- Never disclose or discuss your passwords, or anything about your passwords, with anyone, including clients, co-workers, friends, and family.
- When selecting a password, do not use familiar names, your name, the company name, a season, your child's name, or terms that relate to you personally.
- You must use three of the four following requirements for creating a password:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Numerals (0 through 9)
 - Special characters (such as % * \$ # @ = &)
- Passwords must be at least 8 characters in length.
- Never write down a password and leave it in or on your desk, under your keyboard, or posted on your computer or wall.
- When you change your password, don't use a modified version of the previous password. Create a completely new one.
- You are required to change passwords when prompted, and you are not allowed to re-use the past several passwords that have expired.
- Unless special need is demonstrated and permission granted by MaineHousing management, no user will have more than one account to any system.
- If you think your password may have been compromised, notify your supervisor immediately, who will alert MaineHousing.

SOCIAL ENGINEERING

Social engineering refers to a criminal attempt to get you to reveal your password or other confidential information. Examples of social engineering include:

- You get a phone call from someone claiming they are from the MaineHousing Information Services Department and they need your password to fix a malfunction.
- A visitor to your work area observes you when you enter your password and memorizes the sequence.
- A co-worker casually asks you for your password for what appears to be a legitimate business reason.
- Someone you know engages you in a seemingly innocent conversation about MaineHousing security.
- Be aware of anyone who voluntarily offers their password to you; this could be part of an elaborate scheme to gain fraudulent access to information or systems.
- Be especially wary of unexpected emails containing links or attachments. Copy and paste the link into your internet browser if possible.
- If information is solicited over the phone, call the person back before providing any information.

Immediately report all instances of suspected social engineering to your supervisor, who will report the incident to MaineHousing.

CONSIDERATIONS FOR WORKING OFF SITE

Remote Access Acceptable Use Policies and Guidelines are applicable when you conduct MaineHousing business from your home computer system or other off-site locations too.

- Unencrypted protected data may not be sent by regular (unencrypted) email or transported on a portable device.
- All remote access sessions must be conducted via the MaineHousing Citrix Secure Gateway by using homeport.mainehousing.org.
- You must shred any printed documents containing Personally Identifiable Information that are no longer needed. Do not dispose of confidential materials in regular trash.
- You have a responsibility to maintain security on the computer equipment used to access MaineHousing resources:
 - You must apply current security patches to your computers used at home or off-site.
 - You must have Virus Protection software running with the latest version installed.
 - You must not leave an active session/connection to MaineHousing unattended.

MONITORING AND PRIVACY

- **Monitoring of Computer Resources and Internet Usage.** MaineHousing has the right to monitor and log any and all aspects of usage of its Information Resources, including but not limited to file downloads, application use, and sent or received communications.
- **No Expectation of Privacy.** Authorized users are provided Information Resources to assist them in the performance of their assigned duties. Users should have no expectation of privacy in anything they create, store, view, send, or receive using MaineHousing's Information Resources.
Information Resources are the property of MaineHousing and may be used only for MaineHousing purposes. Anything stored on Information Resources is subject to legal discovery and freedom of information processes.
- **Waiver of privacy rights.** Users waive any right of privacy in anything they create, store, execute, view, send, or receive using MaineHousing's Information Resources. Users consent to MaineHousing's access to and audit of all :
 - Information Resources and MaineHousing-provided equipment, software, and network connections wherever they may be located.
 - Information Resources settings for hardware and software.
 - Applications loaded and executed on Information Resources, and
 - All materials created, stored, viewed, sent, or received by users through any Information Resource or through any Internet (or other network) connection provided by MaineHousing.



I hereby state that I have received and read a copy of the Remote Access Acceptable Use Policy for MaineHousing Business Partners and that I fully understand all of the provisions therein.

- I understand and acknowledge my personal obligations and responsibilities.
- I agree that I will not engage in any activity that may compromise the security of personally identifiable information.
- I agree that I will not engage in activity that may:
 - ✓ degrade the performance of Information Resources,
 - ✓ deprive an authorized MaineHousing user access to a company resource,
 - ✓ obtain extra resources beyond those allocated, or
 - ✓ in any way circumvent Information Resource security measures.
- I understand that MaineHousing reserves the right to monitor Information Resource activity and usage. My signature (electronic or physical) on this document signifies that I have consented to this monitoring.
- I further understand that violation of these policies may result in suspension of remote access privileges. Additionally, I understand that I may be subject to civil and/or criminal prosecution if I violate these policies.

Acknowledged and agreed to by:

Printed

Name: _____

Signature: _____

Date: _____