Objective of the Plan

A Data Security Breach Response Plan is required to bring needed resources together in an organized manner to deal with an adverse security event related to the safety, soundness, and security of MaineHousing data.

The Response Plan is designed to be a working document for use whenever a data security breach occurs that meets the response criteria (defined below). The Data Security Breach Response Plan is a component of MaineHousing's Disaster Recovery / Business Continuity Plan.

MaineHousing Data Security Breach Criteria

MaineHousing defines a data security breach as an unexpected or unplanned event that has the potential to adversely impact MaineHousing, its clients, its business partners, and/or its employees.

To determine if response procedures should be invoked, the following criteria should be considered:

- Actual or suspected unauthorized access to protected client information, including
  - personal identification numbers, such as social security numbers (SSN), passport numbers, driver's license numbers,
  - financial account or credit card information, including account numbers, card numbers, expiration dates, cardholder name, or service codes,
  - healthcare / medical information,
  - names and addresses of clients participating in MaineHousing programs or applicants on waiting lists,
  - the address of a shelter or other living accommodations for victims of domestic violence,
  - or any other information provided by MaineHousing program applicants or participants (including any information provided by a third parties working on behalf of an applicant/participant).
- Triggers legal or statutory requirements
- Could reasonably be considered an extraordinary event
- Results in a disruption of service
- Will negatively affect the organization's reputation

Roles and Responsibilities

Employees, Business Partners, Contractors, and Vendors

Employees, business partners, contractors, and vendors are expected to report actual or suspected incidents immediately.

Data Security Breach Response Coordinator

Initial notification of potential incidents can flow from a variety of sources, but ultimately all reports must funnel to one person: the Data Security Breach Response Coordinator.

The Data Security Breach Response Coordinator is the central point of contact for all incidents.

The Response Coordinator will:

- evaluate and verify all reports of potential incidents,
- notify the MaineHousing Director and Deputy Directors,
- convene and chair the Data Security Breach Response team if necessary,
- manage all incident documentation, and
- maintain communication with MaineHousing management, the Audit Committee, and if necessary, the Board of Commissioners.

Data Security Breach Response Team

The response team is a standing committee consisting of cross-departmental expertise whose function is to provide support and assistance responding to and managing a data security breach incident.

- The Data Security Breach Response Team is convened and chaired by the Response Coordinator.
- Core members of the Data Security Breach Response Team include:
  - the Response Coordinator,
  - MaineHousing Deputy Director,
  - MaineHousing Legal Counsel,
- Principal members to be called in as necessary include:
  - Department Directors tasked with the response to and management of a specific data breach incident that is related to their department and/or area of expertise.
  - Members of the Information Services Department team -- if the breach involves the use of MaineHousing computer systems in any way.
  - Communications / Planning Department (CPD) – if media inquiries are expected. Members of CPD are also responsible for designing and maintaining mail and email templates, as well as press releases for notifying clients, regulatory agencies, etc. as needed.
  - Sage Data Security, MaineHousing's Information Security Officer Advisory team.

Data Security Breach Response Team (continued)

- Tasks of the team include:
  - overall management of the incident,
  - triage and impact analysis to determine the extent of the situation,
  - development and implementation of containment strategies,
  - compliance with government and/or other regulations,
  - communication and follow-up with affected parties and/or individuals,
  - communication and follow-up with other external parties, including the Audit Committee / Board of Commissioners, business partners, government regulators (including federal, state, and other administrators), law enforcement, representatives of the media, etc. as needed,
  - preparation of root cause analysis and lessons learned, and
  - revision of policies/procedures necessary to prevent any recurrence of the incident.

Primary and Alternate members of the Data Security Breach Response Team:

Core Members	Primary	Alternate
Response Coordinator	Linda Grotton, Manager, Audit and Compliance	Jason Dupuy, Director, Information Services
Executive Management	Peter Merrill, Deputy Director	John Gallagher, Director
Compliance/Legal	John Bobrowiecki, Counsel	Linda Uhl, Chief Counsel
Principal Members	**Primary**	**Alternate**
Information Systems	Jason Dupuy, Director, Information Services	Jason Bullock, IT Manager
Communications / Research	Denise Lord, Senior Director of Communications and Planning	Deb Turcotte, Public Information Manager
Safety and Security	Jane Whitley, Director of Human Resources and Facilities	John Bobrowiecki, Counsel
Information Security Officer (ISO) Advisory	Representative of Sage Data Security	
Plus designated Department Directors or Managers depending on the location / area of responsibility where the data security breach occurred.		

Documentation & Reporting

Initial Reporting

- Business partners, contractors and vendors are expected to report actual or suspected incidents ***immediately*** by directly communicating with their MaineHousing contact.

- Employees are also expected to report actual or suspected incidents ***immediately***. The preferred method of notification for employees with knowledge of a suspected breach is to directly contact the Data Security Breach Response Coordinator.

  - If the primary Response Coordinator cannot be reached immediately, then the alternate Response Coordinator should be contacted.
  - In the event that neither the primary nor the alternate Response Coordinators can be reached immediately, a MaineHousing Deputy Director should be alerted.

Post Data Security Breach Review

- The Response Coordinator must log all incidents on the "Summary of Data Security Incidents" spreadsheet. A copy is located at I: Share/Audit/Data Security Breach.

- A report of High and Medium severity incidents is to be completed by the Response Coordinator upon return to normal operations. A copy of the report template is also located at I: Share/Audit/Data Security Breach.

  - The "Information Security Incident Report" should be completed no later than 30 days from conclusion of the data security breach.
  - The final report should document the timeline of the incident and the complete knowledge about the incident, its cause, and the end result.
  - Information from this report will be copied to the Audit Committee. At their discretion, the Audit Committee may forward the report to the Board of Commissioners.

Monthly Information Security Committee Reporting

Data security breaches will be reviewed at the monthly Information Security Committee meeting. Minutes of these meetings will reflect a summary of incidents, if any, that were handled both automatically and by the Data Security Breach Response process.

If no incidents occurred during a given month, the meeting minutes will state this fact.

Notification

Maine Regulatory Requirements for Notification

Maine Statute Title 10, Chapter 210-B: *Notice of Risk to Personal Data* states that "it is a violation of this chapter for an unauthorized person to release or use an individual's personal information acquired through a security breach." A copy of the statute can be downloaded from: www.mainelegislature.org/legis/statutes/10/title10ch210-B.pdf

In the event of a security breach, the Statute requires an investigation be conducted to determine the likelihood that a resident's "personal information has been, or is reasonably believed to have been, acquired by an unauthorized person" or "misuse of personal information has occurred or if it is reasonably possible that misuse will occur." If either of these provisions apply, the Statute requires:

- notification to Maine residents "as expediently as possible and without unreasonable delay,"
- notification to persons / entities maintaining personal information,
- notification to consumer reporting agencies if the breach requires notification to more than 1,000 persons at a single time, and
- Notification to appropriate state regulators (Department of Professional and Financial Regulation or the Attorney General).

Social Security Administration (SSA) Requirements for Notification

In the event that a data security breach involves information verified or provided by the Social Security Administration (SSA), MaineHousing is required to **report that breach to the SSA within one hour** of learning that the breach or potential breach occurred. A copy of MaineHousing's Information Exchange Agreement with SSA, current SSA contact information, and the SSA's required *Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information* when reporting a breach are all located on I: Share/Audit/SSA Documents.

Process for Legally-Required Notification

In the event a data security breach meets the definition of the Maine State Statute or the SSA requirements (above), notification to MaineHousing program participants, applicants, employees, and /or other clients is necessary:

- The decision to notify clients must be authorized by the MaineHousing Director.
- Prior to notification, members of the Audit Committee must be informed by the Data Security Breach Response Coordinator.
- Legal Counsel will identify and notify appropriate regulators and law enforcement agencies.
- CPD will generate press releases and external communications as required, and will create scripts for the switchboard operators.

Client Notification

Client notice should be given in a clear and conspicuous manner and include the following information:

- Description of the incident,
- Type of information subject to unauthorized access,
- Measures taken by MaineHousing to protect clients from further unauthorized access,
- Information regarding MaineHousing's offer of free credit monitoring protection, and
- Telephone numbers clients can call for additional information and assistance.

Delivery of client notification: Client notice should be delivered in a manner designed to ensure that a client can reasonably be expected to receive it. Depending on the situation, MaineHousing may choose to contact all clients affected by telephone or by mail, or by electronic mail for those clients who have agreed to receive communications electronically.

Other Notification

Business Partners: In cases where data and/or systems are shared with business agents and associates, the business partner may need to be notified of the security incident.

Vendors: In cases where the data security breach affects systems that are supported by the vendor, the vendor may need to be contacted to assist in the investigation.

Training & Testing

MaineHousing staff, as well as all employees of MaineHousing business partners, should be trained to recognize and respond to data security breach incidents. Initial training should take place during the new employee's the orientation period and subsequently on a periodic basis.

The Data Security Breach Response Coordinator and members of the Response Team should be trained periodically on their roles and responsibilities.

The incident response plan should be reviewed and tested periodically.

Appendix A: Incident Classification Guidance

Incident classification and notification is the responsibility of the Data Security Breach Response Coordinator. Incident classification and notification guidelines:

Classification	Action
Low Severity • attacks that are automatically thwarted by the system. Knowledge of the occurrence is important; response to the event is not necessary OR • internal situations that are caused by the inappropriate use of information systems or unintentional violations that do not impact protected data.	• to be logged and documented as appropriate through Sage's nDiscovery service. • to be addressed as appropriate
Medium Severity An incursion on non-critical systems or information that results in limited impact to business operations. Protected Data is impacted.	Medium severity incidents are serious and should be addressed within 24 hours. The Data Security Breach Response Coordinator must convene the Data Breach Response Team. Initial response should be to contain the incident. Subsequent activity should focus on eradication and recovery.
High Severity A data security breach that could have significant impact on: • clients, • protected data, • operational stability, • financial strength, • regulatory compliance, or • reputation.	High severity incidents are the most serious in nature. Because of the gravity of the situation and the high potential for harm, these incidents should be handled immediately. The Data Security Breach Response Coordinator must convene the Data Breach Response Team. MaineHousing management must be notified, as well as the Audit Committee. Initial response should be to contain the incident. Subsequent activity should focus on eradication and recovery.

Appendix B: Response Process Checklist

- ☐ Incident is reported to Data Security Breach Response Coordinator
- ☐ Incident Triage
  - Verification
  - Scope
  - Initial Assessment
- ☐ Incident Classification
  - Low – address, log, and document as appropriate
  - Medium -- address within 24 hours
  - High -- notify MaineHousing management; address immediately
- ☐ Incident Containment
  - Determine whether to continue or suspend services
  - Contact relevant service providers and advisory services
- ☐ Internal Communications
  - Internal notification of impact to management
  - Internal notification to appropriate employees
- ☐ Analysis/ Eradication
  - Consult evidence handling guidance
  - Consult evidence retention requirements
- ☐ Notification of Relevant Authorities
  - Contact Law Enforcement
  - Contact Regulatory Agencies
  - Contact Social Security Administration
- ☐ Notification of Third Parties
  - Contact relevant service providers
  - Contact affected business partners
- ☐ Notification of Clients
  - Consult internal approval process
  - Follow client notification guidelines
- ☐ Data Security Breach Reporting
  - Complete "Summary of Data Security Incidents" spreadsheet.
  - If appropriate, complete "Information Security Incident Report."
  - Complete post incident review (lessons learned)
  - Monthly reporting

Appendix C: Analysis and Evidence Handling

The Data Security Breach Response Coordinator is responsible for analyzing the impact of the incident while concurrently addressing the source of the data security breach. This may require a personnel and/or forensic investigation.

Evidence Handling

In particular cases, evidence will be used in criminal or civil legal cases against the perpetrator. Since it may not be apparent at the beginning of an incident investigation that the outcome will be a legal case, every investigation must be treated as though it will lead to a court case. Therefore, members of the Data Security Breach Response Team must establish and maintain an evidentiary chain for all electronic and physical evidence collected during the investigation. Do not include MaineHousing confidential information unless it is absolutely necessary.

To maintain an evidentiary chain, the following information needs to be recorded:

- Where, when, and who discovered the evidence
- Who has handled or examined the evidence and when
- Who has had custody of the evidence, during what time period, and where it was stored and secured
- If the evidence has changed custody, how and when the transfer occurred.

The relevant person should sign and date each entry in the record.

If the investigation leads to a court case, MaineHousing must be able to prove that the evidence discovered has been securely handled and not been tampered with.

All evidence, logs, and data associated with the incident should be placed in tamper resistant containers, grouped together, and put in a limited access location. Only incident investigators, executive management, and legal counsel should have access to the storage facility. If and when evidence is turned over to law enforcement, create an itemized inventory of all the items, verify the inventory with the law enforcement representative, and have the representative sign and date the inventory list. Give the original records to legal counsel, and save a copy for MaineHousing's records. It is recommended that MaineHousing legal counsel be present in all meetings with law enforcement relevant to ongoing investigations.

Evidence Retention

Evidence retention parameters are required to ensure that the evidence is available when it is needed, but they should also consider the costs involved so evidence is not retained indefinitely. Legal counsel shall be involved in identifying the retention requirements.

	Internal Incident	HR Case	Legal Case
Original	Save for duration of analysis.	Save according to HR requirements.	Save until legal says to dispose.
Copy/Image	No requirements.	Save according to HR requirements.	Save until legal says to dispose.