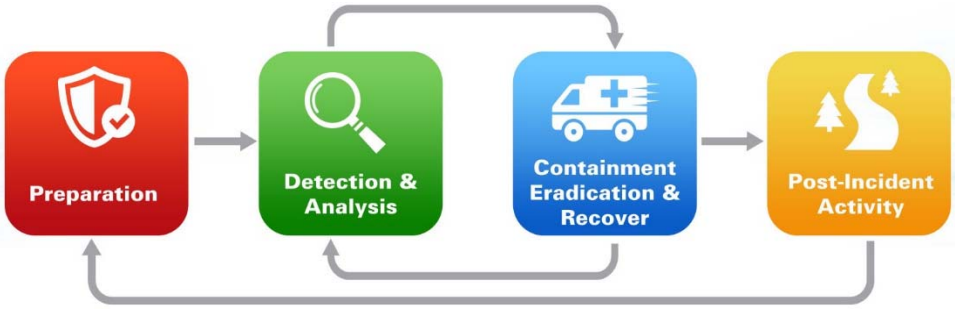
KING COUNTY HOUSING AUTHORITY
CYBER INCIDENT RESPONSE PLAN

Version	Owner	Major Changes	Date
1.0	David Matthews (Critical Informatics)	First draft	07/19/2017
2.0	Lisa Halvorsen	Second Draft	11/19/2019
3.0	Lisa Halvorsen; CIRT	From Lewis Brisbois Template	8/12/2020
3.1	Lisa Halvorsen, Ginger Peck, Norris Feury, Gary Leaf	Review of IT Policies & Procedures & Preparation of Final Draft	2/5/2021
3.2	Lisa Halvorsen, Ginger Peck, Norris Feury, Gary Leaf	Incorporation of Feedback from Senior Staff	3/12/2021

Contents

1.0 Purpose

The purpose of this Incident Response Plan (the "IRP" or "Plan") is to provide a framework for responding to an information security incident at the King County Housing Authority (KCHA), or an incident against a business partner that exposed KCHA protected or secured data, that might involve the loss of Sensitive Information or the disruption of information technology services. It follows the framework established by the National Institute of Standards and Technology ("NIST") which divides the



incident response life cycle into four major phases, as represented in the following graphic[1]:

Each section of the Plan is color-coded to a specific phase. The Plan is a central reference text that identifies and outlines the responsibilities of the internal and external personnel responsible for responding to and managing an information security incident - the Incident Response Team (the IRT or Team) - and for incorporating lessons learned from each incident to increase the effectiveness of the Plan.

At the end of the Plan are a series of appendices that are designed to support the effective implementation of the Plan during a potential incident. For ease of reference, they are summarized below:

Appendix A - Incident Response Team Members

Contains the names and contact information of KCHA personnel that will play active or supporting roles during a potential incident.

Appendix B - Information Technology Incident Response Policies and Procedures

Summarizes current KCHA policies and procedures for Incident Response.

Appendix C - Incident Response Checklist

Provides a checklist, color coded for each section, to be used as a step by step reference tool for the Incident Team Leader during an incident.

Appendix D - Evidence Collection Guidelines

Contains detailed guidelines for evidence collection.

Appendix E - Legal and Regulatory Incident Response Guidelines

Summarizes the legal and regulatory guidelines to which KCHA is expected to comply.

[1] Computer Security Incident Handling Guide, NIST SP 800-61 Rev. 2

Appendix F - External Communications Guidelines

Outlines protocols for communicating with outside entities and providing appropriate messaging regarding an incident.

Appendix G - IT Incident Notification Form

Provides a template to serve as a unified incident reporting form.

Appendix H – Data Breach Notification Laws

Provides summaries of the relevant data breach notification statutes.

Appendix I – Law Enforcement Reporting

Lists best practices and contact information for reporting an incident to law enforcement.

Appendix J – Consumer Notification Templates

Provides templates to serve as unified notification letters.

Appendix K – CJIS/CHRI Data Breach Reporting Policy

Defines KCHA's reporting process when there has been a cyber-attack on Criminal Justice Information.

The Plan is an umbrella document and is intended to provide an overarching structure for Incidents. It is not intended to eliminate or replace more detailed operational procedures that specific departments or groups may have, except where noted. In the event of a conflict between this Plan and any operational procedures, the Plan shall take precedence unless the IRT agrees to a deviation for the incident in question.

1.1 Objectives

The objectives of the Plan are to:

- Identify the King County Housing Authority IRT members and their responsibilities;
- Provide a systematic and efficient means of response and recovery in a manner and timeframe that meets or exceeds contractual and regulatory requirements;
- Minimize disruption to business operations and loss or theft of Sensitive Information;
- Minimize negative impact to third parties, including customers and employees; and
- Minimize any negative impact to KCHA's financial health and reputation.

1.2 Scope

The Plan applies to:

- Business, customer, or employee information owned or managed by KCHA in electronic or non-electronic form (the "In-Scope Information");
- Infrastructure, systems, and devices that are used to process and store information or are necessary for business operations, that are maintained, owned, shared, or supported by KCHA;
- Third party infrastructure (i.e. vendors) upon which KCHA relies to transmit, process, or store In-Scope Information, or for other business operations.

1.3 Important Plan Principles

Reports of potential Incidents can come from many avenues. The initial notification of an incident may be made by phoning the Senior Network Systems manager or the risk manager. Once identified, all Incidents should be submitted as a Help Desk ticket to the Information Technology Department and tracked via the Help Desk ticketing system. When an incident is urgent or emailing Help Desk isn't an option, incidents should be reported by telephone to any member of the IT team who will route it to the Senior Network Systems Manager. It will then be the responsibility of the Senior Network Systems Manager to determine whether to escalate the matter. In the absence of the Senior Network Systems Manager, the IT director or the risk manager will determine escalation.

Not every Incident triggers state or federal reporting requirements. If it appears that Sensitive Information may be at risk, the Senior Network Systems Manager must refer the matter to the Risk Manager who will conduct a risk assessment. The risk assessment will determine whether any Sensitive Information was potentially accessed or acquired without authorization as soon as possible after the discovery of an Incident. If any Sensitive Information is determined to have been accessed or acquired without authorization, a collaborative decision will be made whether to engage Legal Counsel. A determination must then be made about which state or federal notification laws apply based on the category of data at risk and number of individuals affected. The following personnel are the only individuals authorized to make decisions regarding:

- Declaring an Incident: The personnel authorized to formally declare an Incident by email to the IRT and activate the Plan are the Senior Network Systems Manager, IT Director, Risk Manager, or designee
- Insurance: The personnel authorized to contact the insurance carrier(s) are the Risk Manager, Senior Network Systems Manager, IT Director, Deputy Executive Director, or designee.
- External Vendors: Several breach response vendors have been pre-approved by the insurance carrier. Prior to engaging external resources, the insurance carrier must be notified and must approve of the action. KCHA must consult with crisis management vendors pre-approved by the insurance carrier but is not required to use them. The only personnel authorized to engage external resources is the Senior Network Systems Manager, IT Director, Risk Manager, Chief Administrative Officer, or designee, in consultation with Legal Counsel.
- Communications: All information regarding Incidents must be treated as confidential and often will be privileged. The only personnel authorized to approve external communications is the Director of Communications, in consultation with the IRT, the Executive Director, and Legal Counsel.

1.4 When the IRT Should Be Convened

The IRT should be convened for "high-visibility" or "significant" Incidents in which KCHA business operations may be impacted or Sensitive Information may be at risk. These terms are subjective, requiring individual judgment in each case with the severity level of the Incident depending on the likelihood that business operations will be impacted or Sensitive Information will be accessed or acquired without authorization. However, for the purposes of guidance, the following are some examples of Incidents that would be considered high-visibility or significant:

- Incidents involving key KCHA personnel;
- Incidents for which a press release may or will be issued, or media coverage is anticipated;
- Incidents likely to result in a regulatory reporting obligation;
- Incidents likely to result in litigation or regulatory investigation;
- Incidents involving criminal activity;
- Incidents in which Sensitive Information may have been accessed or acquired without authorization; and
- Incidents in which business operations are impacted.

1.5 Definitions

Asset - Any information system (cloud and on-premises), hardware, software, and user account used to conduct official business.

Business Partner and Third Party - Any agency, vendor, or individual doing business with KCHA.

Event – An observable, measurable occurrence in computer network systems, or a reported system interruption or compromise of Sensitive Information. An Event can be observable by someone or reported by automated tools. Or, an event experienced by a business partner. Once verified, Events may be escalated to incidents and handled according to risk and priority categorization by the IRT.

Incident - Any event that compromises or may potentially compromise the confidentiality, integrity, or availability of an information asset – which may include one or more of the following:

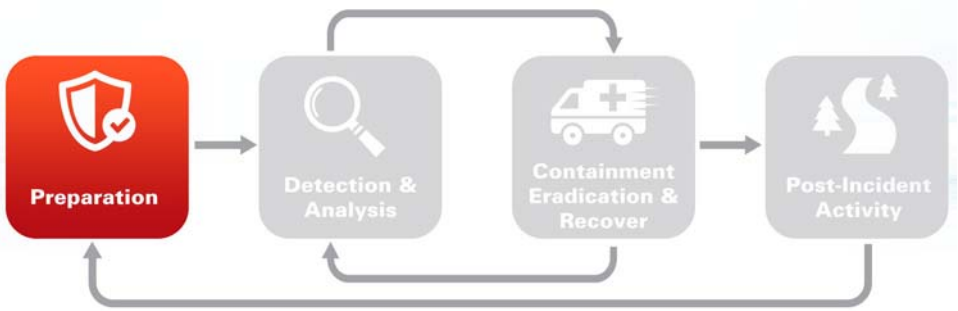
- Unauthorized access to or acquisition of Sensitive Information;
- Corruption of information;
- Denial of service;
- Theft of IT resources;
- Any evidence of unauthorized activity, including the detection of unauthorized wireless access points, critical intrusion detection alerts, and reports of unauthorized critical system or content file changes.

Sensitive Information – Sensitive Information is defined as the following:

- First name or first initial and last name of a person, in combination with one or more of the following data elements of the person:
    - Social Security number;
    - driver's license number or state identification card number;
    - passport or national identification number;
    - tax identification number;
    - a financial account or payment card number and the means to access the account;
    - biometrics used to authenticate the identity of the person;
    - health insurance policy identification number;
    - medical information identifying a physical or mental health condition; and
    - passwords, personal identification numbers, or other access codes that would permit access to financial or online accounts.

- Information system credentials which would allow access to Sensitive Information or the disruption of service; and
- Proprietary information that, if accessed without authorization, would cause competitive and/or economic harm to King County Housing Authority.

2.0 Preparation



Preparation is the most important step in the incident life cycle – the cycle begins and ends with preparation. This Plan is intended to be flexible and scalable. The Incident Manager will be the primary point of contact for receiving reports of Incidents, and will document them in the Cyber Incident Response Team folder on the shared drive, accessible only to members of the IRT. The Incident Manager will create a subfolder with the naming convention of year, month and day of incident (YYYY-MM-DD) to contain all documents pertaining to the Incident. The Incident Manager will make an initial analysis, rate the potential severity level of the Incident in accordance with Table 1 in Section 3.2, and determine whether to convene the IRT in accordance with Table 2 in Section 3.3. If convened, the IRT will use the appropriate elements of this Plan for guidance.

The Incident Manager should always consult with the Risk Manager about whether an IRT should be formed regarding Incidents in which King County Housing Authority business operations may be impacted or when any Sensitive Information may be at risk to determine consumer and/or regulatory reporting obligations. If a technology disruption occurs in which it can be confirmed that no information is at risk of unauthorized access or acquisition, the event can be identified and resolved by the IT Department without forming an IRT or conducting a data loss investigation.

2.1 IRT Reporting to Management and Oversight

The IRT must report significant Incidents to the Executive Leadership Team. The membership of the IRT is set forth in **Appendix A**. The Incident Manager will be designated by the IT Director or Risk Manager and have primary responsibility for reporting to the IRT and on behalf of the IRT to the Executive Leadership Team. Further management reporting instructions are set forth in Section 3, using the guidelines set forth in subsections 3.2 and 3.3.

2.2 IRT Responsibilities

The IRT has the following responsibilities:

- Implements and monitors an Incident identification and escalation procedure;
- Supports the Incident Manager, based on Incident Level and characteristics;

- Ensures the IRT has appropriate resources, tools, personnel and access to carry out the Incident response process;
- Monitors the progress of ongoing investigations;
- Reviews Incident Reports after Incidents have been remediated;
- Conducts training and drills so that Team members are trained to execute the Plan;
- Plans annual communication to employees and new-hires regarding the procedures for reporting an Incident and related business continuity procedures, as needed; and
- Updates the Plan on an annual and as-needed basis.

2.3 Incident Manager Responsibilities

The Incident Manager has primary responsibility for managing and coordinating the Team response. The Incident Manager for each incident may vary based on the type and severity of the Incident, but each Incident Manager responding to technology-related Incidents will generally follow the Information Technology Incident Response Policies and Procedures set forth in **Appendix B**. The Incident Manager will ensure, directly or indirectly through the Team, that the activities identified in the general Incident Response Checklist (set forth in **Appendix C**) are completed. The Incident Manager has the following responsibilities generally:

- Primary contact for incidents reported;
- Convenes the IRT, as necessary;
- Determines necessary members of the IRT for each Incident;
- Coordinates and manages the IRT, including establishing an onsite room that can be used as a centralized meeting place and information repository;
- Oversees communication during the Incident Response process;
- Coordinates Incident briefings with the IRT to review the nature of the Incident and develop the response strategy;
- Conducts regular IRT updates;
- Conducts regular briefings for Senior Management;
- Develops an action plan which documents the nature of the Incident and the goals and strategies of the IRT in responding to the Incident;
- Obtains appropriate approval of the recommended action plan and other key decisions throughout the Incident response process;
- Continuously monitors and assesses the Incident status and the severity level (e.g., level of technology disruption and implications for Sensitive Information), and appropriate IRT strategic and tactical objectives;
- Oversees execution of the recommendations and tracks progress;
- Ensures tactics are in place for meeting applicable regulatory and contractual deadlines and obligations;
- Coordinates “lessons learned” after action review with IRT;
- Ensures each IRT member is aware of his or her general responsibilities set forth in the Incident Response Checklist in **Appendix C**.

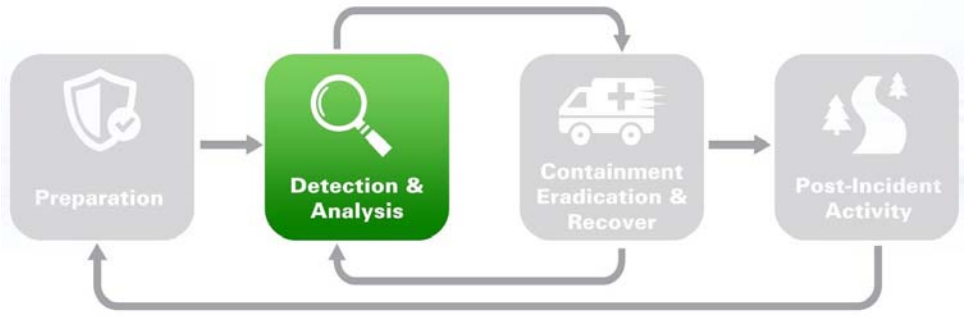
2.4 IRT External Resources

The IRT may need to call upon external resources in response to an Incident. These external resources may include outside Legal Counsel, forensics investigators, credit monitoring/identity restoration services, and public relations firms. The Senior Network Systems Manager is responsible for procuring external IT resources, such as network analysis and forensics investigations. The Risk Manager is responsible for communication with external resources concerning an incident or initiating legal counsel, credit monitoring/identity restoration services, and public relations.

2.5 Testing the Plan

If an actual Incident does not occur within a 12-month period, a simulated Incident will be run to exercise the IRT and this Plan. These exercises will improve the performance of the IRT and help identify issues with related policies, procedures, and communication. The Data Governance Committee in consultation with the IT Director and Risk Manager will be responsible for determining when a simulated Incident should be planned, the type and severity of the Incident to be tested, and facilitating the event.

3.0 Detection and Analysis



3.1 Identification and Escalation of an Incident

Reports of potential privacy or data security concerns can come from many sources. Identification typically begins after a user, system operator, employee, customer, vendor or third party, or business partner has noticed unusual or suspicious behavior in a system, network, or other business process. Employees, customers, vendors, telephone calls, emails, business associates or authorities may all report a potential Incident in a variety of entry points throughout the organization. King County Housing Authority conducts annual and new-hire training to educate and encourage immediate reporting of an Incident to the IT Department. The reporting form in **Appendix G** should be used for gathering information. The Senior Network Systems Manager will conduct an initial review of the details of a newly reported event and establish the IRT as necessary. The Incident Manager will be responsible for, directly or through delegation, the collection of documents and evidence, as well as documenting the chronology of the investigation and resolution.

The Identification phase involves a determination of whether or not an Incident has occurred, and if so, the nature and severity of the Incident. However, because regulatory reporting deadlines may be short, it is better to err on the side of caution and rule a suspected Incident as an actual Incident until it is proven otherwise. The procedures outlined here should be used immediately upon notification of a suspected Incident. This phase also includes informing and soliciting help from people who can assist in investigating, escalating and scoping the Incident (i.e., establishing the IRT).

3.2 Risk Assessment – Is this a Significant Incident?

Table 1: Examples of the Magnitude of Data Related Incidents

Sensitive Information Impact/Degree of Visibility				
	No Data at Risk	**Incident May Lead to Risk to Data**	**Reasonable Likelihood of Risk to Data**	**Information at Risk**
No technology disruption	--	**Unidentified individual** reported within King County Housing Authority facilities.	**Unidentified individual** seen **removing files** from King County Housing Authority.	**Unauthorized individual** seen **removing files** from King County Housing Authority that **contain customer or employee information**. **Known unintentional sharing of SPII (unencrypted email)**
Tier 1 • Localized, minor; • No critical or revenue generating systems affected	**Sustained attempt at intrusion, scanning** or pinging of King County Housing Authority devices	**Phishing email** to which employee responds to sender or clicks on a link from an unknown source that **may involve download or malware.**	**Phishing email** to which employee responds to sender or clicks on a link from an unknown source that is **known to involve download or malware**.	**Phishing email** to which employee responds to sender by **transmitting information**, but no Sensitive Information involved.
Tier 2 • No critical or revenue generating systems affected • Will affect service if unaddressed	**Missing IT devices** with **no** storage capabilities	**Missing** King County Housing Authority **IT devices** with storage capabilities	**Theft** of King County Housing Authority **IT devices** with storage capabilities	**Theft** of King County Housing Authority **IT devices that store proprietary information,** including employee contact information (names, physical addresses, email addresses, and telephone numbers)
Tier 3 • Critical systems	**Webhosting** system availability **response time is below the required SLA.**	**Webhosting** system availability **response time is below the required SLA** and King County Housing Authority received **one unqualified threat of a hacking attempt**.	**Webhosting** system availability **response time is below the required SLA** and King County Housing Authority has identified **multiple attempts to hack** into servers storing sensitive customer information	**Webhosting** system availability **response time is below the required SLA** and there is **evidence** that customer **files containing social security numbers/PI** may have been taken as part of incident.
Tier 4 Incidents producing unexpected widespread or large scale impact or unavailability to critical business process	**Large number** of users report **slow system response time.**	**Malware** identified on laptops in multiple business units and **quarantined** throughout system.	**Malware** identified on laptops in multiple business units, but **uncertainty** exists whether it is designed to exfiltrate data.	**Malware** on laptops in multiple business units that **exfiltrates** email system **exposing large volumes** of sensitive customer and employee information.

3.3 Management Reporting

The Team will report Incidents to the following management personnel as they are identified, and provide periodic updates through the resolution of the Incident. Reporting to management will vary based upon the degree of technology disruption and the risk to Sensitive Information.

		Data Impact			
		No data at risk P4	**Incident May Lead to Risk to Data P3**	**Reasonable Likelihood of Risk to Data P2**	**Information at Risk P1**
	No technology disruption	**(Low)** No Reporting	**(Medium)** IRT consulted	**(High)** IRT Convened Legal Counsel notified and regularly updated.	**(Critical)** IRT Convenedand Legal Counsel notified and engaged; senior management regularly updated.
	Tier 1				
	Tier 2	IT procedures govern reporting			
	Tier 3				
	Tier 4				

During the detection and analysis phase, the Team can begin to implement containment as needed to isolate the issues, preserve evidence and protect affected systems in accordance with the Information Technology Incident Response Policies and Procedures as set forth in **Appendix B**. A few key actions to consider are:

- **Physically Secure Area.** Restrict physical access to the area where the Incident or compromised system(s) are located if possible and applicable.
- **Documentation & Communication.** Clearly communicate and document all information regarding the Incident in accordance with the Communications Protocol set forth in Section 3.4.
- **Identify Data at Risk.** If Sensitive Information is at risk, the investigation should focus on obtaining details that will assist the Legal Counsel in the assessment of risk and regulatory obligations.

3.4 Confidentiality and Privilege

Confidentiality: All information regarding Incidents must be treated as confidential. DO NOT discuss, share, forward or otherwise disseminate any information related to an Incident to any person not directly involved in the investigation. Likewise, no information about an Incident should ever be sent to or discussed with any person who is implicated in the report other than as necessary to investigate the incident, even if the person to whom you report is implicated. If you are involved in an Incident that implicates your direct supervisor you should immediately notify the IT Director, Risk Manager, and/or Legal Counsel.

Privilege: All investigations are done at the direction of an attorney (i.e. Legal Counsel), for the purpose of providing legal advice to the King County Housing Authority, and thus, are privileged. Discussions conducted at the direction of Legal Counsel by and between Team members and other witnesses are governed by the Attorney-Client privilege. Investigative reports and notes are governed by the Work Product Doctrine. However, the Incident itself and the underlying facts are not covered by privilege.

All physical or electronic documentation (emails, reports, notes, summaries, etc.) should include or be marked with a privilege disclaimer like, "Privileged Communications; Produced at the Request of Counsel" or "Privileged and Confidential." Display this disclaimer prominently in the header and/or at the top of each document.

Prior to disclosing or discussing information, all participants should be reminded of their obligation to keep the matter confidential. See the Evidence Collection Guidelines (**Appendix D**) for more information on the Corporate "Miranda" Statement which should be read at the beginning of each interview.

Corporate "Miranda" Statement: When conducting an interview in the course of investigating a Security Incident, you MUST inform the person being interviewed of the following:

- The investigation is being done at the request of an attorney who represents King County Housing Authority, not the employee;
- The purpose of the interview;
- The interview is subject to the attorney-client privilege as between King County Housing Authority and the attorney who is directing the investigation;
- The interview is regarded as confidential and the employee may not disclose the substance of the interview with third parties, including their supervisor, without prior approval; and
- King County Housing Authority, as the holder of the privilege, may decide to provide the substance of the interview to a third party, without the employee's consent.

It is important to make these statements clearly and unambiguously.

3.5 External Communications

Contact external parties as part of the response, as needed, but only after proper approval has been secured. The Team may consider additional third parties depending on the type of Incident, such as Internet Service Providers, software or hardware vendors, or special interest groups (security specialists or professional associations).

The Legal and Regulatory Incident Response Standards and Guidelines (**Appendix E**) include guidance on contacting third parties with a potential notification requirement, such as:

- Impacted parties (i.e. customers, employees, or third party vendors).
- Acquirers (i.e. financial institutions that initiate and maintain relationships with merchants to accept and process credit card transactions.
- Card member organizations (i.e. Visa, MasterCard, etc.).

Only authorized individuals will be involved in external communications, such as to the media or to customers, and they will issue only approved messaging. **No external communications are permitted without the prior consent of the Director of Communications in consultation with the IRT, Executive Director and/or Legal Counsel.** All information is shared on a need-to-know basis with only the necessary people engaged and informed as information leakage can damage the effectiveness of response.

3.6 Handling of Systems Involved in the Incident

If the Incident stems from a compromise of security of electronic records, computer systems, computer networks, or the physical environment wherein assets exist, IRT members will follow the additional procedures in the Information Technology Incident Response Policies and Procedures in **Appendix B**.

3.7 Documentation

From the very beginning of a suspected Incident, all Team members should take notes of each step in their process and involvement. It is best if the notes are chronological, with the time of each entry indicated. The notes should be as factual as possible; care should be taken to avoid speculation, as speculation can confuse the evaluation of the Incident. The Incident Manager or delegate will be responsible for correlating all Team members' notes.

3.8 Collect and Preserve Information

Collect all information related to the Incident. Unless there is an emergency situation requiring that the compromised system be isolated and powered down to minimize further the damage, the process of identifying evidence should begin before the computer is altered in any way. Powering down can actually damage evidence and machines should only be powered down under supervision and/or approval of the technical lead. Log files should include the date and time of the captured events, and describe the location and serial numbers or other identifying information. Law enforcement agencies may request that suspect disk drives or entire systems be removed and sealed as evidence. Identifying information must be recorded from these drives. Older system backups and logs that predate the Incident may provide valuable evidence. Whenever copies of electronic data are made, the original data and media, not the copy, should be sealed for evidence.

Backup the system. A backup should be made as soon as there are indications that an Incident has occurred. New media should always be used to avoid suspicion of overwritten "old" information.

Making a full system backup immediately captures evidence that otherwise may be lost or altered. Ideally, two backups should be made; one to be used for forensic investigation, and the other to use as a source of additional backups. The original system disks should never be used for forensic analysis or as the source for making more than one backup copy.

Ensure evidence is captured and preserved securely. An evidence custodian should be identified who manages the secure container of evidence. Only a small group of people should have access to this

container and a record of their identities should be kept. By policy and practice, each person with access must understand that they are required to control access to evidence. Each person with access may be called upon to testify if the Incident results in legal action. All evidence collection should be performed in accordance with the Evidence Collection Guidelines as set forth in **Appendix D**.

4.0 Containment, Eradication and Recovery

4.1 Containment

The Incident Manager, as designated in the Information Technology Incident Response Policies and Procedures, is responsible for developing a containment recommendation for review and approval by the IRT.

4.2 Eradication

The goal of the eradication phase is to eliminate or mitigate the factors that resulted in a compromise of system security. If the source of the compromise is not eradicated, it will likely be magnified, resulting in a much larger compromise. The Senior Network Systems Manager, working with the Information Technology Department, should perform a vulnerability analysis, improve system defense, remove the cause of the Incident, and address other viruses, malicious codes, network intrusions and encryption attacks.

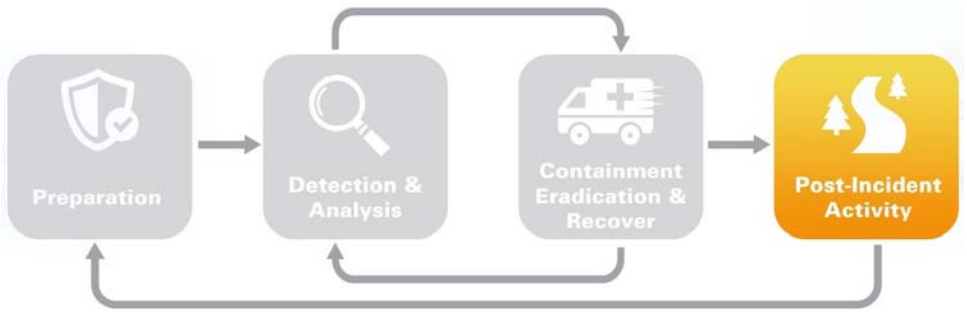
4.3 Remediation

Technical remediation involves providing whatever technical support is necessary to update software, repair hardware, or otherwise move the system toward recovery. Legal remediation involves assessing the impact on affected consumers, identifying legal notification obligations, and determining whether offering credit monitoring or identity theft restoration services would be appropriate.

4.4 Recovery

The recovery phase returns the system to full operational status.

5.0 Post-Incident Activity



This Section will provide the Team with mitigation plans for Incidents and a framework for the post-Incident response. After recovery, the King County Housing Authority will hold a "lesson learned" meeting for all Team members after distributing a detailed Incident description. The Incident Manager will plan and facilitate the meeting, addressing the following questions:

- What happened exactly? At what times?
- How well did staff and management deal with the Incident? Were documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps taken that might have inhibited recovery?
- What would staff or management do differently the next time a similar Incident occurs?
- What corrective actions can prevent a future similar Incident?
- What additional tools or resources are needed to detect, analyze and mitigate future Incident?
- What can be done in both the short-and long-term to increase our security posture?

Using the information from the meeting, the Incident Manager will draft a follow-up report, in coordination with the IRT, highlighting how information learned can better protect data in the future. All affected parties should review the report. Responses, disagreements, additions, and suggestions from all interested parties should be gathered and documented as part of the report.

The Incident Manager will submit the final report to the IRT for approval. Upon approval, the Incident Commander may provide an executive summary of the Incident and recommendations to Senior Leadership. Relevant information might include: education or training for employees identified as contributing to the Incident, costs and impacts, a prioritized set of recommended changes, a cost estimate of said changes, a high-level schedule, and the impact of implementing or not implementing the recommended actions.

Changes should be considered at three levels:

- **Incident:** Improve defenses specific to preventing the actions that led to the most recent Incident.
- **Process:** Improve the people, process and technology elements of the Plan based on the most recent response with a goal of reducing the risk of further Incidents.
- **Program:** Improve elements of the overall security program based on the most recent Incident and response.

The Incident Manager and key Team members shall prepare a mitigation plan. The steps taken for corrective action will be documented by the Incident Manager and included in the Incident documentation.

Appendix A: Incident Response Team Members

ROLE	EMAIL	DESK PHONE	CELL PHONE
Incident Manager: Director of IT or Risk Manager or Senior Network Systems Manager			
IT Director Gary Leaf	GaryL@kcha.org	206-574-1175	206-450-2929
Risk Manager Ginger Peck	GingerP@kcha.org	206-574-1124	253-279-7007
Senior Network Systems Manager	NorrisF@Kcha.org	206-574-1172	206-395-4798
Executive Lead: Chief Administrative Officer			
Craig Violante	CraigV@kcha.org	206-574-1274	206-852-4660
Public Information Officer: Director of Communications			
Rhonda Rosenberg	RhondaR@kcha.org	206-574-1185	206-755-7899
Operations Lead: Director of Information Technology, Chief Information Officer			
Gary Leaf	GaryL@kcha.org	206-574-1175	206-450-2929
Logistics Lead: Senior Network Systems Manager			
Norris Feury	NorrisF@kcha.org	206-574-1172	206-395-4798
Planning Lead: Risk Manager			
Ginger Peck	GingerP@kcha.org	206-574-1124	253-279-7007
Finance Lead: Chief Financial Officer or Assistant Finance Director			
Windy Epps	WindyE@kcha.org	206-574-1166	(not listed)
Research & Evaluation: Data Manager			
Anita Rocha	AnitaR@kcha.org	206-693-6404	(not listed)
Incident Support Lead: Risk Management Analyst			
Lisa Halvorsen	LisaHal@kcha.org	206-693-6422	541-512-9806
Affected Department(s) and/or Business Partner			
Head of the affected department(s) and/or business partner designate			

Appendix B: Information Technology Incident Response Policies and Procedures

The Incident Manager will implement the applicable elements of the following policies and procedures in responding to an Incident under the Cyber Incident Response Plan.

PREPARATION

IT IRT Roles and Responsibilities

Key subject matter resources for the Incident, including their IRT responsibilities and their contact information are set forth in the Plan. The Incident Manager or his or her designee will select other Team members, depending upon the nature of the technical, organizational, and legal issues involved in an Incident. The IRT should include subject matter resources, as appropriate.

DETECTION & ANALYSIS

Guidance for Handling of Systems Involved in the Incident

The Team will consider the following procedures in analyzing and preparing a response to an Incident involving certain systems or technology threats:

Copy and Examine Logs. Log files are a critical source of information that can be used to identify and assess an Incident. Typical logs that should be copied, preserved and reviewed include:

- Server event logs
- Application logs
- Firewalls
- Intrusion detection systems
- Network devices
- Search other systems

Because of the high level of connectivity typical between systems, it is important to examine the state and history (logs) of systems that are linked to the system of interest. These connected systems could be owned and managed by King County Housing Authority, or those of third parties (partners, suppliers, and customers).

Information Assessment. A preliminary forensic examination should be conducted to determine whether an event is an Incident, and if so, to determine the scope, impact, and cause.

Collect All Information Related to Incident. Unless there is an emergency situation requiring that the compromised system be isolated and powered down to minimize further damage, the process of identifying evidence should begin before the computer is altered in any way. Powering down can actually damage evidence and machines should only be powered down under supervision and/or approval of the technical lead. Log files should include the date and time of the captured events, and describe the location and serial numbers or other identifying information of affected devices. Law enforcement agencies may request that suspect devices or systems be removed and sealed as evidence. Identifying information must be recorded from these devices or systems. Older system backups and logs

that predate the Incident may provide valuable evidence. Whenever copies of electronic media are made, the original media, not the copy, should be sealed for evidence.

Backup the System. A backup should be made as soon as there are indications that an Incident has occurred. New media should always be used to avoid suspicion of overwritten "old" information. Making a full system backup immediately captures evidence that otherwise may be lost or altered. Ideally, two backups should be made; one to be used for forensic investigation, and the other to be used as a source of additional backups. The original system disks should never be used for forensic analysis or as the source for making more than one backup copy.

Evidence Capture and Preservation. An evidence custodian should be identified who manages the secure collection and containment of all technology evidence. The custodian should follow all Evidence Collection Guidelines.

CONTAINMENT, ERADICATION & RECOVERY

Containment Procedures

The containment phase of the Incident response procedure isolates the threat and enables King County Housing Authority to prevent further damage or exposure through the network and systems. The following are suggested actions to address during containment:

1. **Determine Risk of Continued Operation.** After consulting with the Senior Network Systems Manager and Legal Counsel, and evaluating the business and technical risks, the Incident Manager must jointly decide whether to shut down a system entirely, disconnect it from the network, or allow it to continue to run in its normal operational status so that activity on the system can be monitored.
2. **Disable Accounts and Change Passwords.** Intruders commonly target root or administrator account names and passwords. When a system is compromised, change the passwords on that system and on all systems with which it regularly interacts. Only do this once it is determined that no further evidence needs to be collected. If there is reason to believe the system has been subjected to a password sniffer attack, passwords on all systems on the affected LAN or subnet may have been affected and must be changed.
3. **Isolate System & Monitor Activities.** If and when the Team decides to isolate the compromised system(s), consider the following levels of isolation.
    - Temporarily shut down the compromised system after copies of any volatile (e.g. live memory) and non-volatile (e.g. saved data on disk drives) are made and preserved
    - Leave system running but disconnect it from the network to isolate it from other internal systems and the Internet
    - Disable selected system services (e.g. file sharing, print services) to isolate the system from those services
    - Disable physical access to tainted area
    - If compromised by an encryption attack, immediately disable the affected network share to isolate the attack and following the procedures set forth below

- If a decision is made to leave the system running normally, carefully monitor its operating system, system services, and inbound and outbound network traffic. If this is done in order to collect more information about an intruder and an intrusion, there may be additional liability if a King County Housing Authority system is used as a launch point to attack another site.

4. Verify Backup Systems. Carefully check all backup systems supporting the compromised system and regularly check their integrity and functionality. Many backup systems operate in an automated fashion and therefore may replicate undesired configuration elements of the compromised system, such as deleted or modified files, viruses, Trojans, unauthorized accounts or elevated privileges. Additional monitoring of these systems may be needed for a period of time after the Incident.

Eradication Procedures

The eradication phase of the Incident response procedure removes and purges the threat from the system to restore operations and functionality. The following are suggested actions to address during eradication:

1. **Perform Root Cause Analysis.** Information collected during the identification and verification steps may not be sufficient to determine the root cause of the Incident. In most cases, there are multiple causes for a compromise. For example, the absence of adequate technical controls may result from the failure to adequately select and train system administrators; the lack of documented security policies and procedures; the absence of management emphasis; or all of these reasons. Team members must conduct a comprehensive review of the information gathered realizing that more than one factor may have contributed to the compromise. Correlation of information from multiple sources is usually necessary to understand the cause of an Incident. Some suggested information gathering and examination actions include:

    - Recovering as much information as possible, including deleted files
    - Uncovering IP addresses, host names, network routes and Web site information
    - Extracting the contents of hidden, temporary, and swap files used by both application and operating system software
    - Accessing the contents of protected or encrypted files
    - Analyzing relevant information found in special disk storage areas
    - Analyzing file access, modification and creation times
    - Analyzing system, service, network and application logs
    - Analyzing e-mails for source information and content
    - Performing file integrity checks to detect Trojan horse files and files not originally on the system
    - Analyzing, if applicable, physical evidence, for example fingerprints, property damage, video surveillance, alarm system logs, physical access logs, and interviewing witnesses

2. **Perform Vulnerability Analysis.** The use of vulnerability assessment tools can assist the Team not only to validate the correctness of eradication procedures, but also to anticipate and correct additional factors that might facilitate a future attack. It is critical to ensure that other platforms within the organization are not subject to the same vulnerability that allowed the compromise. Team members can use automated assessment tools to search for these vulnerabilities on other systems. An accurate inventory of computing resources on the network is needed to support this.

3. **Improve Defenses.** Once a system has been compromised, its password file, IP address, and operating system may be published in the hacker community. As a result, the system may be repeatedly probed or attacked for a period of time following the initial Incident. New attackers will typically have enough information to launch focused attacks. The original attacker may also be unaware that the compromise has been discovered and may continue to return to the compromised system to obtain additional information and to use the compromised system as a host for attacks on other systems. A compromised host should not be allowed to reestablish network connections until the Team fully understands the cause of the Incident, and can direct the system's owner to follow specific eradication procedures that will preclude a recurrence. Appropriate protection techniques should be implemented, such as firewall and/or router filters, moving the system to a new name/IP address, or in extreme cases, porting the machine's function to a more secure system. The Incident Manager should verify the correct implementation of the eradication procedures before reconnection. The Incident Manager should also serve as the liaison with any entities that may be responsible for implementing some of the eradication procedures to ensure adequate protection.
4. **Remove Cause of Incident.** The basis for removing the cause of the Incident is the root cause analysis and/or scenario-based analysis.

Procedures for Specific Types of Threats

The following are protocols suggested for specific types of threats:

1. **Viruses and Other Malicious Code.** Virus or malicious code eradication requires removing the virus from all systems and media, usually with commercial software. King County Housing Authority should maintain up-to-date malware detection and correction software in anticipation of this type of attack. There is the potential for re-infection, given that it may be difficult to find and disinfect all compromised media, particularly backup media. The Team must ensure that there is an effective procedure in place to update commercial anti-malware programs.
2. **Network Intrusions.** In the case of a network-based intrusion, eradication is more difficult. Many attacks over a network come in two parts. First there is an initial phase when system vulnerability is exploited and the system is accessed. Once inside, the intruder often installs a tool (backdoor) to provide continued access. Attackers often install backdoor access programs and sniffers to collect additional passwords and user IDs. It is important to find these programs and eliminate them.

   The Team must determine whether or not the attacker has modified the compromised system in any way. The most effective way to do this is to immediately disconnect the compromised system from the network until such time as the forensic analysis has been completed. This assumes knowledge of the baseline configuration of the system before compromise, and access to a clean, uncompromised copy of the system, applications, and information installed prior to the compromise.

   If there are business reasons that preclude disconnection, then the Team must consider alternatives. For example, it may be possible to place a firewall directly in front of the compromised system and establish an access control list (ACL) to preclude an attacker's access. Another possibility may be to filter incoming and possibly outgoing connections to and from the compromised system at the organization's network perimeter.

3. If law enforcement considerations dictate that monitoring the attacker takes precedence over eradication, then the system may be left in place with appropriate sensors to capture evidence of the attacker's activities. The Incident Manager along with Legal Counsel must approve such a course of action. Law enforcement may be allowed to monitor communications of an attacker if four requirements are met:

    - The Incident Manager or Legal Counsel authorize, in writing, the interception of the attacker's communications;
    - The person who intercepts the communications must be "lawfully engaged in an investigation;"
    - The person who intercepts the communications must have "reasonable grounds" to believe that the contents of the attacker's communications will be relevant to the investigation;
    - The interception should not acquire any communication other than those transmitted to or from the attacker.

    Team members should refrain from direct contact with an attacker without the approval of Legal Counsel. If such contact does occur, Team members must maintain detailed audit records of all contact. Once law enforcement personnel have responded to an Incident, they may manage these contacts.

4. **Encryption Attacks.** Containment and eradication is more difficult in the case of an encryption attack because much of the evidence may be inaccessible due to the encryption. When such an attack is detected, the following should be done:

    - The network share – all devices connected to the infected computer - should be immediately disabled to prevent the continuation of the attack;
    - All backups, if they have not been affected, should be taken off line to ensure they are preserved and available;
    - All affected devices and other evidence, if possible, should be preserved pending a digital forensics investigation;
    - A forensics investigation should be deployed to determine:
        - how the attack occurred
        - the variant of the malware and its algorithmic behavior
        - whether a decryption key is available
        - the various devices affected
        - the various files affected
        - whether personally identifiable information was accessed and/or exfiltrated
        - whether the attack was a decoy for other malware inserted into the system
        - whether any malware remains in the system

    Encryption attacks typically target backup systems to provide leverage to the attacker's extortion attempts. Consequently, in preparation for such an attack, the following should be done:

    - Regularly check the integrity and functionality of backup systems
    - Maintain a current secondary offline backup
    - Maintain a current offline "golden" image in the event devices have to be wiped and a new image installed
    - Maintain a procurement channel for immediate ordering and supply of new devices

5. **Third Party and Business Partner Incidents.** When it is learned that an incident has occurred involving information transmitted, processed or stored by a third party vendor, there are a number of items that need to be reviewed immediately: contractual obligations, regulatory obligations, and industry obligations.

   Regarding contractual obligations, the following needs to be reviewed:

   - Notice:
     - What does the contract provide regarding notice obligations?
     - Although the only statutory obligation of the third party vendor is to notify the business of an incident, it is recommended that contracts be revised to place the responsibility for consumer notification on the party that contributed to the breach.
   - Liability:
     - What does the contract provide regarding liability?
     - Although conventional contracts limit liability to the amount of annual fees paid to the third party vendor, it is recommended that contracts be revised to place liability for expenses of a breach on the party that contributed to the breach.
     - The contract should also require cyber liability insurance to cover the expenses.
   - Indemnification:
     - What does the contract provide regarding indemnification?
     - Although conventional contracts typically require businesses to indemnify the breached third party vendor, it is recommended that contracts be revised so that the breached entity indemnifies the business against any third party claims.
   - Consumer remediation expenses:
     - What does the contract provide regarding remediation expenses?
     - Although conventional contracts typically do not address remediation expenses, it is recommended that contracts be revised so that the breached entity accepts responsibility for the expenses of all consumer notification and remediation expenses, such as credit monitoring and identity monitoring.

   Regarding regulatory obligations, the following needs to be reviewed:

   - Based on the nature of the vendor, what are the regulatory obligations?
   - Does the vendor handle protected health information on behalf of the business?
     - If so, there should be a business associate agreement in place with the business if it is a covered entity under HIPAA.
     - If regulated data in the custody or control of a third party vendor has been acquired without authorization, notification obligations for the business must be immediately reviewed and calendared to ensure compliance with regulatory requirements.

   Regarding Industry obligations, the following needs to be reviewed:

   - Based on the nature of the vendor, what are the industry obligations?
   - Does the vendor handle payment card industry data on behalf of the business?
     - If so, the business needs to be prepared to notify its merchant processor within 24 hours of being notified by the third party vendor of a breach.

- Although the payment processor often has the responsibility of notifying the payment card brands, the best practice is to also notify each payment card brand individually at the same the time merchant processor is notified.

6. **Fraudulent Wire Transfer Incidents.** When it is learned that an incident has occurred involving an attempt to fraudulently transfer funds, the following should immediately be done:

   - Report the matter to the local FBI cyber task force. If the matter is reported within 24 to 72 hours of the initiation of the wire transfer, the FBI can work with FinCEN and attempt to stop the transfer and remit the funds to originating account.
   - Report the matter to the originating bank and request that they hold the funds and preserve all evidence of the transaction.
   - Report the matter to the destination bank and request that they hold the funds and preserve all evidence of the transaction.
   - Preserve all evidence of the incident.

7. **Email Compromise Incidents.** When it is learned that an incident has occurred involving an apparent email account compromise, the following should immediately be done:

   - Reset the password to the account;
   - Enable two-factor authentication;
   - Engage a digital forensics firm to determine the following:
     - When the compromise first occurred;
     - The malicious IP address(es) used to effectuate the compromise;
     - Which rules were changed;
     - Which search terms were deployed;
     - Which emails were accessed/viewed;
     - Which attachments were accessed/viewed;
     - Whether personally identifiable information was accessed/viewed for purposes of determining consumer and regulatory notification obligations.

Technical Remediation Procedures

Technological remediation involves assessing the damage to a system and implementing repairs, including the replacement of hardware and the upgrading or patching of software. As new security controls are identified, remediation will include implementing and monitoring such controls.

Recovery Procedures

The recovery phase of the Incident response procedure returns the system to fully operational status. The following are suggested actions to address during recovery:

1. **Restore System.** Some Incidents, such as malicious code attacks, may require a complete restoration of the system from backups. In this case, it is essential to first determine the integrity of the backup itself. If no backups were made just prior to compromise, the system may have to be rebuilt from trusted media, and then have patches applied. It may be possible to use a backup from a similar system that has not been compromised.

   System restoration will typically include these system elements:

- Operating system
- System services
- Applications
- Updated patches
- Incident
- Shared file systems
- Local network access
- Internet access

2. **Verify System.** There should be a system test plan to verify the integrity and functionality of the restored system. As an alternative, the system can run through its normal tasks while being closely monitored by a combination of techniques, such as network loggers and system log files. It should be noted that sometimes patches or techniques used to prevent vulnerability will cause the system to function differently than it did before the event.
3. **Restore Normal Operations.** The decision to return to normal operations should be made by the IT Director, based upon a recommendation by the Incident Manager.
4. **Monitor Systems.** Once the system, including the operating system, system services, and network traffic (inbound and outbound), is back in production, monitoring should continue for at least two weeks.

Appendix C: Incident Response Checklist

The Incident Response Checklist will be used by the Incident Commander to ensure all activities of the CIRP are followed. Each section is described in detail under the corresponding Sections of the CIRP.

Date/Time	Action	Status	Owner
Preparation Phase			
	Identify reporting source		
	Complete initial Team assignments		
	Start Incident documentation		
Detection and Analysis Phase			
	Secure physical area		
	Identify and verify Incident		
	Copy and examine logs		
	Search other systems		
	Complete initial assessment		
	Assist in interviews when requested		
	Collect and preserve information		
	Engage outside Legal Counsel		
	Perform damage assessment/collect the following information: ➢ all data attributes ➢ how the data was exposed ➢ number of records ➢ likelihood that the data was accessed or taken		
	Backup target system(s)		
	Manage internal communications		
	Manage external communications		
	Notify insurance carrier(s)		
	Notify merchant bank		
	Notify payment card brands		
	Notify law enforcement, as appropriate		
	Record factual information necessary to create a chronology of the incident		
	If Criminal Justice Information is compromised, contact the Washington State Patrol ACCESS Information Security Officer (see Appendix K – CJIS/CHRI Data Breach Reporting Policy)		
Containment, Eradication, Remediation and Recovery Phase			
	Containment		
	Determine risk of continued operation		
	Disable accounts and change passwords		

Date/Time	Action	Status	Owner
	Isolate system		
	Monitor system and network activities		
	Continuously monitor and assess the incident priorities and review incident strategy and tactical objectives		
	Perform status briefings as needed		
	Document activities, actions, and all related items		
	Verify backup systems		
	Eradication Phase		
	Complete root cause / scenario analysis		
	Perform vulnerability analysis		
	Improve defenses		
	Remove cause of Incident		
	Select clean backup		
	Remediation Phase		
	Repair/replace hardware		
	Replace/upgrade software		
	Notify consumers and regulatory officials		
	Provide credit monitoring and/or identity theft restoration services		
	Complement physical security controls as needed. This may require the use of more guards and or placement of additional surveillance equipment both in an overt and covert manner		
	Recovery		
	Restore system		
	Verify system		
	Return to normal operations		
	Monitor systems		
Post Incident Activity			
	Document activities, actions, and all related items		
	Coordinate with Legal Counsel regarding any unique knowledge of customer regulatory needs or policies		
	Hold “lessons learned” meeting		
	Write follow-up report		
	Record factual information necessary to create a chronology of the incident		
	Preserve, if necessary, documents that may be needed by King County Housing Authority business partners, or regulators concerning the incident		

Appendix D: Evidence Collection Guidelines

During and after an Incident, the IRT will follow the evidence collection policies and procedures set forth herein.

1. **Collect All Information Related to an Intrusion**

   Collect information about all relevant system and network logs from the compromised system(s), including written log records made by any members of the IRT, any other auditing information produced by tools, full backups, partial backups, screen shots, videotapes, and photographs.

   Document all information that addresses the questions who, what, where, when, why, and how, including:

   - Name of system
   - Date and time of each entry
   - What actions were taken?
   - What was said?
   - Who was notified?
   - Who had access?
   - What Incident was collected?
   - What information was disseminated, to whom, by whom, when, and for what purpose?
   - What was submitted to Legal Counsel, to whom, by whom, and how it was verified (e.g., notarized)

   Any notes may be subject to subpoena in any legal proceeding, so document responsibly and follow all guidance regarding documentation in this Data Incident Response Plan. There should be separate documentation, when possible, for each intrusion so if it is subpoenaed, it does not contain information about other intrusions.

2. **Collect and Preserve Evidence**

   The Incident Manager, in consultation with Legal Counsel, is responsible for maintaining contact with law enforcement and other external agencies. To ensure the legal community will accept the evidence, it should be collected according to predefined procedures in accordance with all laws and legal regulations. Additionally, complete the following:

   - Document, use, and maintain a procedure for preserving the compromised system and any associated evidence in case of a criminal investigation.
   - Analyze a replica of a compromised resource, not the original, whenever possible, to avoid inadvertently tampering with evidence.
   - Ensure that replicating the compromised resource does not change the original. This can be accomplished by write-protecting the original information prior to copying it.
   - Document all actions performed by all participants from detection through analysis, response and recovery that preserve the chain of custody (refer to the next two steps).

3. **Ensure Evidence is Captured and Preserved Securely**

   Archive all information offline media that is physically secure. Ensure that all critical information is duplicated and preserved both onsite at a King County Housing Authority facility and offsite in a

secure location. This includes policies, procedures, contact information, tools, critical Incidents, configurations, cryptographic checksums, and system backups. Onsite alternative storage provides for quick access in the event of an emergency.

Ensure that all log files containing information about an intrusion are retained for at least as long as normal business records, or possibly longer if the investigation is ongoing.

Define and document a procedure for authorizing access to both onsite and offsite information so you can access it quickly in case of an emergency.

4. Preserve the Chain of Custody for all Evidence

This is accomplished by having verifiable documentation indicating the sequence of individuals who have handled a piece of evidence and the sequence of locations where it was stored (including dates and times).

For a proven chain of custody to occur:

- The evidence is accounted for at all times;
- The passage of evidence from one party to the next is fully documented; and
- The passage of evidence from one location to the next is fully documented.

5. Corporate "Miranda" Statement

IRT members need to understand that the investigation is privileged, but anyone they talk to about the Incident also needs to understand the privilege as well. Prior to disclosing or discussing any information, all participants should be reminded of their obligation to keep this matter confidential and not discuss or disclose anything regarding the investigation except to an IRT member.

Prior to conducting an interview in the course of investigating an Incident, the IRT member must inform the person being interviewed and obtain their acknowledgement of understanding for the following:

- The interview is subject to the attorney-client privilege as between King County Housing Authority and the attorney who is directing the investigation; the attorney represents King County Housing Authority and not the interviewee/employee;
- The purpose of the interview;
- The interview is regarded as confidential and the employee may not disclose the substance of the interview with third parties, including their supervisor without prior approval; and
- King County Housing Authority, as the holder of the privilege, may decide to provide the substance of the interview to a third party, without the employee's consent.

Evidence Collection Form

DATA INCIDENT EVIDENCE COLLECTION FORM					
Instructions Use the following form to capture the evidence collection process. Collect information about all relevant system and network logs from the compromised system(s), including written log records made by any members of the IRT, any other auditing information produced by tools, full backups, partial backups, screen shots, videotapes and photographs.					
Evidence Documentation					
System/Incident Name	Click here to enter text.			**Date**	Click here to enter text.
Location of Breach	Click here to enter text.		**Cause**	Click here to enter text.	
Time Start	Click here to enter text.		**Time End**	Click here to enter text.	
Date/Time *Record the date and time evidence collected.*	**Evidence Collected** *Provide a description of the evidence.*	**Action** *What was said / who was notified/ who had access/what evidence was collected/ what info was disseminated*	**Instructions Given**	**Assigned To**	**Comment**

Appendix E: Legal and Regulatory Incident Response Guidelines

The Legal Counsel advises the IRT and Management as to legal obligations. In order for the Legal Counsel to advise King County Housing Authority concerning the risk of litigation resulting from an Incident, Legal Counsel will conduct and oversee documentation of the Incident following appropriate procedures to preserve attorney client privilege and work product doctrines before, during and after an Incident. The legal role in the Cyber Incident Response Plan ("Plan") is referred to as "Legal Counsel," and is intended to include the General Counsel, a representative of the General Counsel's office, or Outside Counsel, as applicable. Legal Counsel has full responsibility for regulatory breach reporting at the federal and state levels, and will work closely with the Team to assess and comply with those obligations.

When handling an Incident, the Legal Counsel will make the following determinations with support from the Team as needed:

- Determine whether law enforcement should be notified (if criminal activity);
- Determine insurance notification requirements (consult with Risk Manager);
- Determine whether cyber insurance coverage requires specific third party vendors for breach response;
- Prepare and supervise any litigation;
- Determine if senior management should receive notice;
- Determine if and when regulatory filings are required (consult with IT Director and Risk Manager or designee).

These policies and procedures set forth guidance and checklists for the Legal Counsel and IRT members to follow during an Incident.

1. Guidance for Consumer, Employee or Other Individual Data

Legal analysis and remediation in an Incident involving affected individuals requires assessing the impact on affected individuals, identifying legal notification obligations, and determining whether offering credit monitoring or identity theft restoration services would be appropriate.

It may include any of the following steps:

- Determine what category of data was compromised. If it includes any individual's Sensitive Personally Identifiable Information (SPII), the state data breach notification statutes where affected consumers reside must be considered;
- Identify specific data elements exposed;
- Assess volume of potential data records affected;
- Determine which business clients, financial institutions, healthcare companies, or other third parties are impacted, and see guidance below for third party;
- Verify if data was encrypted and method/level of encryption;
- Address legal requirements for different categories of data, and see guidance below for personally identifiable consumer information, payment card information, and protected health information;
- Determine number of affected consumers and the states in which they reside;
- Determine whether state allows "risk of harm" analysis (likelihood of damage?);
- Determine whether state allows "safe harbor" for encrypted data;

- Determine state incident notification requirements, including timing, content and method of communication;
- Determine whether state Attorneys General or other governmental entities require notice;
- Determine whether there is a suggested or required notice format;
- Determine whether breach occurred as result of third party and if so, analyze notice of contractual indemnity obligations;
- Determine remediation efforts (i.e. credit monitoring services) and contract your external vendor; and
- Determine if notice should be provided to public (consult with Director of Communications, Risk Manager and Executive Director or designee).

The Team will consider the additional factors in analyzing and preparing a response to an Incident involving certain categories of data.

Personally Identifiable Consumer Information. In the event an incident is believed to involve the unauthorized acquisition of personal information (Sensitive information as defined in Section 1.5 of the Plan), the following process should be followed:

- Inform Legal Counsel;
- Identify specific data elements involved;
- Verify if data was encrypted and method/level of encryption;
- Identify any (client or vendor) contractual provisions for breach notification (See Third Party Obligations below);
- Determine which, if any, state regulations may affect notification timing or methodology;
- Assess International-specific requirements, if relevant;
- Assess requirements for Telecommunications Service Providers or hosting vendors, if relevant;
- Define notification strategy;
- Engage the Director of Communications, Risk Manager and Director of Human Resources when appropriate to help develop and manage internal and external communication, including media strategy;
- Draft notification letters or scripts, along with internal talking points;
- Ensure all communication is approved by Legal Counsel;
- Coordinate and execute third party notification;
- Monitor social media and communication plans; and
- Execute de-brief on incident for process improvement.

Criminal Justice Information Services (CJIS) / Criminal History Record Information (CHRI). In the event an incident is believed to involve CJIS / CHRI data, King County Housing Authority shall promptly report incident information to the ACCESS Information Security Officer (ISO) by email to ACCESS@wsp.wa.gov using the FBI Security Incident Reporting Form available on the ACCESS webpage: http://www.wsp.wa.gov/_secured/access/docs/access_cjis_security_incident_report.pdf

See **Appendix K** for the CJIS/CHRI Data Breach Reporting policy.

Payment Card Information. In the event an incident is believed to involve the loss of payment card information, the following additional procedures should be assessed:

- Determine which financial institutions and other third parties are involved or impacted;

- Verify if data was encrypted and method/level of encryption;
- Determine whether payment processing agreement requires notification to the payment processor or payment card networks;
    - Payment card networks (Visa / MC) may require you to retain a Payment Card Industry ("PCI") forensic investigator ("PFI"). Note that a PFI may not be necessary unless a payment card network requests such an investigation. However, if requested, King County Housing Authority will need to have a PFI in place within the time frame specified by the payment card network, which may be as short as 72 hours;
    - Evaluate whether an independent forensic investigator (non-PFI) should be retained to work with PFI and evaluate their findings;
- Determine which, if any, state regulations may affect notification timing or methodology;
- Assess PCI-related notification requirements in conjunction with Legal Counsel;
- Inform/engage Management as appropriate;
- Engage Director of Communications, Risk Manager and Director of Human Resources when appropriate to help develop and manage internal and external communication, including media strategy;
- Draft notification letters or scripts, along with internal talking points;
- Coordinate and execute third party notification;
- Ensure all communication is approved by the Legal Counsel;
- Monitor social media and communication plans; and
- Assess notifying the payment card brands as follows:

Pursuant to the King County Housing Authority merchant processing agreement, King County Housing Authority is required to notify the processor "immediately" if King County Housing Authority "determines or suspects" that Payment Instrument Information has been compromised. Notification must be given in writing. For specific payment card network contact information and policies, please refer to the chart below.

American Express	Refer to the following documentation online: https://www260.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US.pdf, and contact the American Express Enterprise Incident Response Program (EIRP) at (888) 732-3750
Discover	Refer to the documentation from Discover website: http://discovernetwork.com/fraudsecurity/databreach.html, and call **800-347-3083**
Visa	Refer to documentation online at https://usa.visa.com/support/small-business/data-security.html, and contact (650) 432-2978 or usfraudcontrol@visa.com
MasterCard	Refer to the following documentation online: http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf and contact 800.627.8372 or account_data_compromise@mastercard.com

2. Guidance for Services Offered to Individuals Impacted by an Incident

In the event an Incident causes Sensitive Information to be accessed or acquired without authorization, Legal Counsel will determine if King County Housing Authority will provide credit monitoring or identity restoration services to affected individuals. Legal Counsel, the Finance Director and Risk Manager shall consider the following factors when making this determination:

- Would the breached data permit a third party to open a financial account or commit identity theft?
- Have consumers requested that King County Housing Authority offer specific services?
- Has the offering of credit-related services become a standard practice in the industry in connection with type of data breached?
- Would offering credit-related services confuse or mislead consumers concerning the nature of the information at issue and the possible impact of that information's misuse?

Legal Counsel should consult with the Risk Manager to determine whether such services are covered by insurance.

3. **Third Party Obligations**

Client / Business Partner. In the event an Incident is believed to involve any client data, the following additional procedures should be assessed:

- Inform the Legal Counsel before any external communication is issued to the client/business partner;
- Legal Counsel should ensure that notice is provided to the legal notice designee of the client/business partnerwhen necessary;
-
- Draft notification letters or scripts, along with internal talking points;
- Coordinate and execute third party notification;
- Ensure all communication is approved by the Legal Counsel; and
- Monitor social media and communication plans.

In the event that Legal Counsel and the client/business partner disagree about what notifications or disclosures are required, the following procedures will be followed in analyzing the risk, assessing King County Housing Authority's separate legal and regulatory obligations, and provide a basis for determining the required action:

- Legal Counsel will inform the IRT Manager, or designee;
- Legal Counsel will inform the Director of Communications and the IRT, including Risk Manager prior to notifying the client/business partner;
- Ensure all communication is approved by the Legal Counsel.

Appendix F: External Communications Guidelines

The IRT will follow the policies and procedures herein when preparing or distributing any external message or communication regarding an Incident.

The following factors should be considered when deciding what information should be communicated outside of King County Housing Authority, the timing of any communications, and the content of any communications:

- Federal and state statutory requirements to notify consumers and law enforcement concerning some types of data security breaches.

- Contractual requirements to notify clients or business partners, including, Customer or Vendor Guidelines or a Business Associate Agreement.
- Whether notification may jeopardize King County Housing Authority's ability to continue to investigate a data security incident by, among other things, alerting an individual who may have attempted to access information as to King County Housing Authority's knowledge of the incident.
- Whether notification is likely to permit impacted clients, consumers or employees to take steps to protect themselves from harm that may result from the incident.
- Whether premature notification may inadvertently result in transmitting inaccurate or incomplete information to consumers or to the public.
- Whether sufficient resources are capable of being deployed to respond to questions or concerns regarding the information conveyed.
- Whether notification or a failure to notify will cause reputational harm to King County Housing Authority.

If King County Housing Authority determines that informing third parties may be premature, unnecessary, or harmful, the Director of Communications and Risk Manager, in consultation with the Legal Counsel, should consider, during the course of an incident investigation, appropriate responses in the event that there is a media inquiry about an incident.

Appendix G: IT Incident Notification Form

This checklist is to be utilized to report a suspected information security incident in the King County Housing Authority information system. Some key words that may trigger this notification:

- **Hack**
- **Breach**
- **Virus**
- **Intrusion**
- **Denial of Service**

1. DISPATCHER/ CALL-TAKER INFORMATION

Name:	
Date:	Time of initial report:

2. CALLER INFORMATION

- Gather as much information as they are willing to share
- Let caller know that someone from the King County Housing Authority IT Department may call them back for additional information about the suspected incident

Name:	
Organization/Agency:	
Address:	
Email:	
Phone number:	

3. GATHER INCIDENT INFORMATION

- What type of incident occurred? Can you describe what happened?
- How was the incident detected or discovered?
- Do you know what system, network or data has been affected?

Notes:

IF INCIDENT HAS POTENTIAL TO AFFECT SENSITIVE INFORMATION OR DISRUPT SERVICE, OR IF UNSURE ABOUT NATURE OF INCIDENT, NOTIFY THE IT HELP DESK: HelpDesk@kcha.org

Appendix H: Data Breach Notification Laws

Contact Legal Counsel for Current State and Federal Law and Policy Requirements

The following are selected laws and regulations relating to the breach of personal information about an individual. Legal Counsel should be consulted to determine whether, when, and how to disclose a data breach. Washington State is the primary jurisdiction to which King County Housing Authority is subject and for which it must comply with its data breach notification law. The procedures are summarized below to provide insight as to the definition of personal information and the time frames for disclosure. Resources at the federal level are also listed. Proper notification is an important part of King County Housing Authority's responsibility in the event of a data breach or loss of credit card data. Each decision on notification should be made on a case-by-case basis in consultation with Legal Counsel.

Data Breach Notification Laws (50 States/D.C./Territories):

http://lewisbrisbois.com/privacy/US

Washington Data Breach Notification Law

http://app.leg.wa.gov/RCW/default.aspx?cite=19.255.010 (Wash. Rev. Code § 19.255.010-020)

Washington law requires businesses which experience the unauthorized acquisition of computerized and non-computerized data that materially compromises the security, confidentiality or integrity of personal information, to notify affected consumers in the most expeditious manner possible, without unreasonable delay, and not more than 30 days from discovery of the breach. If more than 500 Washington residents must be notified, the Washington Attorney General must also be notified. See https://www.atg.wa.gov/identity-theft-and-privacy-guide-businesses#Report, "Identity Theft and Privacy Guide for Businesses" on the Attorney General's website for more information. Personal information is defined as a first name or first initial and last name of a person, in combination with one or more of the following data elements of the person:

- Social Security number;
- Driver's license number or Washington identification card number;
- Account number or credit or debit card number and the means to access the account;
- Full date of birth;
- Private key that is unique to the individual and is used to authenticate or sign an electronic record;
- Student, military or passport identification number;
- Health insurance policy number or health insurance identification number;
- Information about the individual's medical history, mental or physical condition, or medical diagnosis or treatment; or
- Biometric data including fingerprints, voiceprints, eye retina and iris scans, or other unique characteristics that are used to identify a specific individual.
- Username or email address in combination with a password or security questions and answers that would permit access to an online account; and
- Any of the data elements or any combination of the data elements described in (a)(i) of this subsection without the consumer's first name or first initial and last name if:
    - Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and

- The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Public Officers and Agencies, Public Records Act
Personal Information – Notice of Security Breaches

1. Any agency that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.
2. Any agency that maintains or possesses data that may include personal information that the agency does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
3. The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
4. For purposes of this section and except under subsection (5) of this section and RCW 42.56.592, notice may be provided by one of the following methods:
    a. Written notice;
    b. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or
    c. Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
        i. Email notice when the agency has an email address for the subject persons;
        ii. Conspicuous posting of the notice on the agency's web site page, if the agency maintains one; and
        iii. Notification to major statewide media.
5. An agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.
6. Any agency that is required to issue notification pursuant to this section shall meet all of the following requirements:
    a. The notification must be written in plain language; and

b. The notification must include, at a minimum, the following information:
    i. The name and contact information of the reporting agency subject to this section;
    ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
    iii. A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and
    iv. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

7. Any agency that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall notify the attorney general of the breach no more than thirty days after the breach was discovered.
    a. The notice to the attorney general must include the following information:
        i. The number of Washington residents affected by the breach, or an estimate if the exact number is not known;
        ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
        iii. A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach;
        iv. A summary of steps taken to contain the breach; and
        v. A single sample copy of the security breach notification, excluding any personally identifiable information.
    b. The notice to the attorney general must be updated if any of the information identified in (a) of this subsection is unknown at the time notice is due.

8. Notification to affected individuals must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered, unless the delay is at the request of law enforcement as provided in subsection (3) of this section, or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. An agency may delay notification to the consumer for up to an additional fourteen days to allow for notification to be translated into the primary language of the affected consumers.

9. For purposes of this section, "breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

10. a. For purposes of this section, "personal information" means:
    i. An individual's first name or first initial and last name in combination with any one or more of the following data elements:
        A. Social security number or the last four digits of the social security number;
        B. Driver's license number or Washington identification card number;
        C. Account number, credit or debit card number, or any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account;

D. Full date of birth;
E. Private key that is unique to an individual and that is used to authenticate or sign an electronic record;
F. Student, military, or passport identification number;
G. Health insurance policy number or health insurance identification number;
H. Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or
I. Biometric data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;

ii. User name or email address in combination with a password or security questions and answers that would permit access to an online account; and

iii. Any of the data elements or any combination of the data elements described in (a)(i) of this subsection without the consumer's first name or first initial and last name if:
A. Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and
B. The data element or combination of data elements would enable a person to commit identity theft against a consumer.

b. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

11. For purposes of this section, "secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

Washington State Auditor

All fraudulent activity must be reported to the State Auditor per RCW 43.09.185.

Washington ID Theft Resources:

http://www.atg.wa.gov/identity-theftprivacy

Federal Resources:

Health and Human Services/Office for Civil Rights

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Federal Trade Commission ID Theft Resource

https://www.consumer.ftc.gov/topics/privacy-identity-online-security

Postal Inspection Service Resource

https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/mailtheft/IdentityTheft.aspx

Appendix I: Law Enforcement Reporting

Law enforcement reporting on significant data security incidents can provide a number of benefits in the incident response process including:

- Receipt of additional known indicators regarding threat actors
- Ability to report law enforcement contact to affected individuals and regulators
- Development of relationship which helps foster a better understanding of the latest available intelligence and trends
- Potential "safe harbor" benefit and/or additional time for required reporting of incident
- Opportunity to good corporate citizenship

Federal Bureau of Investigation – Cyber Division

The FBI has cyber trained personnel assigned to each of its 56 field offices nationwide. In addition, the CyWatch command center, located in the Washington DC/national capitol region maintains 24/7 incident response capability.

FBI Seattle Division
Supervisory Special Agent Carrie Kingston
1110 3rd Avenue
Seattle, Washington 98101
(206) 287-3635 (office)

SSA Kingston leads a team of Special Agents, Analysts, Computer Scientists, and other professional support personnel to respond to a host of data security incidents which might involve a violation of federal law or threat to national security.

Seattle Switchboard: (206) 622-0460
Ask to speak with a Duty Agent who can connect you with other on-call cyber personnel.

CyWatch – 24/7 Operations Center
CyWatch is staffed with individuals from several federal, state and local agencies participating in the National Cyber Investigative Joint Task Force. It is a 24/7 cyber operations center and will receive an initial report of the incident and arrange for follow-up from cyber trained personnel, as appropriate.

Email: cywatch@fbi.gov
Phone: 855-292-3937

Appendix J: Consumer and Regulatory Notification Letter Templates

(draft on current letterhead)

Date

Name
Address
Address
Email Address – *Also sent via email*

RE: Notice of Data Security Incident

Dear Name,

We are writing to inform you of a data security incident that (may have) involved your personal information. We recently learned that (insert facts – i.e. there was an unauthorized access to an email account containing your information; or, an email attachment containing some of your personal information was sent to the wrong person.) We wanted to notify you of the incident, (insert information about remediation services, i.e. offer you free credit monitoring services), and inform you about steps that can be taken to protect your personal information.

What Happened. (Insert facts – i.e. In late March, we detected unusual activity in our email system. We immediately took steps to ensure the security of those accounts and our system. We also engaged a digital forensics firm to determine whether any client information had been accessed without authorization. On *date,* our investigation determined that your information may have been accessed without authorization. Or, On *date*, an employee processing your Section 8 voucher into our system intended to send an email to our Finance department but unintentionally sent it to an individual who does not work for the King County Housing Authority. Within 34 minutes, the sender recognized the error and attempted to recall the message but was unsuccessful. An hour later, the unintended recipient of the email reported that they had deleted the message and its contents.)

What Information Was Involved. Your full name and Social Security Number (for example).

What We Are Doing. As soon as we discovered the incident, we took the measures referenced above. We also (explain what measures were taken) and what measures we are doing to protect their information.) We are offering you free credit monitoring service for one year. We are also obtaining a signed statement from the unintended recipient declaring that they have not shared your personal information and that all information has been permanently deleted.

What You Can Do. We recommend that you (insert information about enrollment in credit or identity monitoring services, if appropriate.) Please contact *name, phone, email* to sign up. We also recommend that you follow the guidance on protecting your personal information on the second page of this letter.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you. Thank you for your continued trust and support.

Sincerely,

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

(draft on current letterhead)

DECLARATION REGARDING PUBLIC RECORDS

I, _____ (print full name) declares and affirms as follows:

1. *(Nature of improper receipt of records) I received an email on date from King County Housing Authority that contained documents with protected personal information. I forwarded the email to name(s) relationship, etc., and to no one else.*

2. *I have not provided any information from the email to any other person.*

3. *I deleted the email and its contents from my email account on all my electronic devices.*

4. *I deleted downloaded documents from the hard drive of my computer and electronic devices.*

5. *I understand that disclosing a KCHA benefit recipient's name or social security number is a violation of law.*

I declare under penalty of perjury under the laws of the State of Washington that the foregoing is true and correct.

EXECUTED in _____ (county and city),

Washington, this _____ day of _____, 2020.

_____ *[signature]*

_____ [*printed name*]

Appendix K: CJIS/CHRI Data Breach Reporting Policy

Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of Criminal Justice Information (CJI), agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

Reporting Security Events

King County Housing Authority shall promptly report incident information to the ACCESS Information Security Officer (ISO) by email to ACCESS@wsp.wa.gov using the *FBI Security Incident Reporting Form* available on the ACCESS webpage: http://www.wsp.wa.gov/_secured/access/docs/access_cjis_security_incident_report.pdf to any authorities appropriate to the local agency.

Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).