King County

Procedures for Managing a Security Breach Under the "Personal Information – Notice of Security Breach" Law

Codified under RCW 42.56.590

Ralph Johnson
Chief Information Security and Privacy Officer
Updated - October 2007
Version 3.0

Revision History

Version #	Revision Date	Revised by	Description
1.0	8-2005	Ralph Johnson	Initial Draft
2.0	5-2007	Ralph Johnson	Updated, modified formatting
3.0	10-2007	Ralph Johnson	Revised to include suggestions from PAO

Acknowledgements:

OIRM would like to thank the following individuals for their assistance in developing and reviewing this document:

Marcine Anderson – Office of the Prosecuting Attorney

Sharon Glein – OIRM

Jennifer Hills – Risk Management

Ralph Johnson – OIRM

Anh Nguyen – Office of the Prosecuting Attorney

David Ryan – Office of the Prosecuting Attorney

Table of Contents

Procedures for Managing a Security Breach Under the "Personal Information – Notice of Security Breach" Law (RCW 42.56.590).

Introduction

On May 10, 2005 the Washington State Legislature passed Substitute Senate Bill 6043 entitled "Personal Information-Notice of Security Breaches". This law became effective on July 24, 2005 and that part applicable to public agencies was codified into RCW 42.56.590. The law is intended to give individuals warning when their Personal Information may have fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to mitigate the impact of the security breach.

Purpose

In order to ensure compliance with this law, the Office of Information Resource Management is publishing these recommended practices and procedures for providing notice in cases of security breach involving Personal Information. The purpose of the processes outlined in this document is to allow individuals to take actions to protect themselves against, or mitigate the damage from identity theft or other possible harm. Each agency must determine its own specific methodology for identifying and reporting a security breach. OIRM's office of Information Security and Privacy may assist in making the determination upon request.

This document is intended to provide recommendations to agencies on how to prevent, detect and identify a security breach consistent with this legislation. It also provides suggestions on preparing and distributing notice to affected individuals.

In addition this document presents a mandatory county wide reporting, communications, coordination and management process to ensure consistency in the processing and documentation of all such security breaches.

Security Breaches

Security is an essential component of information privacy. It is one of the basic principles of fair information practice: **Organizations that collect or manage individuals' Personal Information should use security safeguards to protect that information against unauthorized access, use, disclosure, modification or destruction**. Implementing an effective information security program is essential for an organization to fulfill its responsibility to the individuals who entrust it with their Personal Information. It is the best way to reduce the risk of exposing individuals to the possibility of identity theft. It is also the best way to reduce the risk of exposing the organization to the damage to its reputation and finances resulting from an information security breach.

Most business and all government agencies today acknowledge their responsibility for ensuring the security of the Personal Information in their care. In its 2000 report to Congress on the privacy practices of companies doing business online, the Federal Trade Commission found that the privacy policies of 74 percent of the 100 most popular Web sites included a statement that the companies took steps to provide security for the information they collected. Many organizations in the U.S. are legally required to protect the security of Personal Information. The two major federal laws on privacy enacted in recent years—the Gramm-Leach-Bliley Act and the Health Information Portability and Accountability Act—include security and privacy rules that apply to a broad range of financial institutions and health care organizations.

Nevertheless, information security studies have indicated that the number of security breaches has increased over time, along with their frequency, severity and the costs to business of responding. Washington's Personal Information – Notice of Security Breach law was passed to address this situation.

California passed a similar law in 2003 for the same purpose. In order to get an early look at how a number of major corporations had prepared to implement the law in California the Ponemon Institute conducted a preliminary benchmark survey in early July 2003, as the law first took effect. The study suggests that corporations have been prompted to take action by the law, including acquiring enabling technologies to protect their information technology infrastructure from security breaches, and that the law does not create a significant cost-of-compliance burden. The study also revealed some areas where best practice guidance was sought, such as encryption and coordination of notification responsibilities of third parties with whom data is shared. King County takes protection of Personal Information seriously (See the King County Privacy Policy at http://kcweb/oirm/governance/policies/KCIT_Privacy_Policy.doc). The following recommendations and procedure represents initial guidance on coordination, investigation, communication and notification. Agencies may have more specific and stronger policies, procedures and legislation that govern their actions.

Identity Theft

We now know that identity theft is much more common than reports in recent years suggested. A national survey conducted by the Federal Trade Commission found that the number of victims in 2002 approached 10 million, and two other recent surveys estimated the number at seven million. That's nearly 10 times greater than the previously quoted estimate of less than a million a year. According to the Gartner Group identity theft has increased by 50% since 2003. According to the Office of the Attorney General, Washington ranks seventh per capita in reported identity theft.

The surveys also confirmed the opinions of law enforcement and others that identity theft is on the rise in the U.S. showing a dramatic increase between 2001 and 2002.

The costs of the crime are alarming. Recent studies estimate the average victim's out-of-pocket expenses at $500 to $740, and the time spent clearing up the situation at between 30 and several hundred hours. The Federal Trade Commission estimates the total annual cost to business as $50 billion for 2002, based on an average loss from the misuse of a victim's Personal Information of $4,800.

Studies also show that the cost of an identity theft incident, both for victims and for business, is significantly lower if it is discovered quickly.

Definitions

The following are the definitions of key terms used in the remainder of this document.

Security Breach Coordinator: Each agency should designate a person to manage internal security breach procedures and coordination with the Chief Information Security and Privacy Officer.

Data Custodian: The individual or organization that has responsibility delegated by the Data Owner for maintenance and technological management of a system. This is usually the IT organization.

Data Owner: The individual or organization with primary responsibility for determining the purpose, function, sensitivity and classification of a system. This is usually a management level person responsible for oversight of the program/agency that uses the data.

High-Risk Personal Information: Not only the Notice-Triggering Information that could subject an individual to identity theft, but also health information, other financial information and other Personal Information the disclosure of which would violate the privacy of individuals.

Notice-Triggering Information: As provided in Washington law, this is unencrypted, computerized first name or initial and last name plus any of the following: Social Security number, driver's license number, Washington Identification Card number, or financial account number, credit or debit card number, in combination with any code or password permitting access to an individual's financial account where such a code or password is required.

Personal Information: The Washington state law uses a very narrow definition of Personal Information. (See page 8 Type of information) For purposes of this document Personal Information is any data that can be used to identify, contact, or locate an individual. Some examples include home address, cell phone number, or driver's license number.

Substitute Notice: Notice other than via US mail. Used in instances where the cost of notifying individuals is prohibitive (in excess of $500,000) or the number of potentially affected individuals exceeds 250,000.

Technical Security Breach: A security breach that does not seem reasonably likely to subject individuals to a risk of criminal activity. An example of this would be an unauthorized Workforce Member viewing a file containing Personal Information.

Workforce Member: Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County.

Summary of the Personal Information – Notice of Security Breaches Law

The Personal Information – Notice of Security Breaches (RCW 42.56.590 aka Washington State Breach Law) applies to all governmental agencies. The main provisions are summarized below.

Security Breach (as defined in the law)

- Security breach is defined as unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of Personal Information.

Type of Information (what is Personal Information according to this law?)

- Unencrypted computerized data including certain Personal Information.
- Personal Information that triggers notice requirement under the law:

    1. Name (first name or initial and last name)

    in combination with any of the following:

    2. Social Security number,
    3. Driver's license or state identification card number, or
    4. Financial account number, credit or debit card number

    in combination with:

    - Any security code, access code or password required to access the account.

Whom to Notify

- Notice must be given to any individual whose Personal Information is compromised or reasonably suspected to be at risk of compromise who is a Washington resident.

When to Notify

- Timing: "in the most expedient time possible and without unreasonable delay." RCW 42.56.590(1)(2). Time may be allowed for the following:

    1. Legitimate needs of law enforcement if notification would impede a criminal investigation or,
    2. Taking necessary measures to determine the scope of the security breach and restore reasonable integrity to the system.

How to Notify

- Notice may be provided in writing, electronically (as consistent with provisions on electronic records and signatures per 15 USC 7001), or by Substitute Notice.
- Substitute Notice may be used if the cost of providing individual notice exceeds $250,000 or if more than 500,000 people would have to be notified or the County does not have sufficient contact information to provide notice. Substitute Notice consists of all of the following:

    1. E-mail when the e-mail address of the individual is available, and

2. Conspicuous posting on King County web site, and
3. Notification via major statewide media.

- Alternatively, an agency may use its own notification procedures as part of an information security policy for Personal Information, if its procedures are consistent with the timing requirements of the law and if it notifies subjects in accordance with its policy.

Relief

The statute is not clear regarding "relief" relative to public agencies. A "business" can be enjoined however It is not clear that a public entity is a "business" under the statute. [RCW 52.56.290(10)(b)].

Also it is not clear that the County has "customers" as referred to in the statute.

- In the event of a security breach what relief can the law provide?
    1. Any "customer" injured can institute a civil action to recover damages.
    2. If the County is found to be a "business" under the statute it may be enjoined (stopped) from its activities related to Personal Information.

King County's Procedure and Recommended Practices

King County will centrally manage the coordination, investigation and communications process for all security breaches. Most of the following recommendations are intended to assist organizations in supplementing their information security and privacy programs. The recommendations are not limited to the scope of the Washington law on notice of security breach, but rather they represent a broader approach and a higher standard. However central coordination, investigation and communication are requirements. King County must be assured that all such incidents are managed in a consistent manner.

These "best practices" recommendations can serve as guidelines for organizations, to assist them in providing timely and helpful information to individuals whose Personal Information has been compromised while in the Countys care. Unlike many best practices, these recommendations do not contain all the procedures that should be observed. Information-handling practices and technology are changing rapidly, and organizations should continuously review and update their procedures to ensure compliance with the laws and principles of privacy protection. It is recognized that specific or unique considerations, including compliance with other laws, may make the recommendations inappropriate for some organizations.

While the law on notice of security breach applies only to records in electronic media ("computerized data") and defines a limited set of items of Personal Information as triggering the notification requirement, agencies should consider applying these practices to records in any media, including paper records and extending the notification process to High-Risk Personal Information.

The following sections provide procedures to follow in preparing for, detecting and reacting to a security breach. Sections I and II are activities that agencies should engage in immediately to protect data from a security breach and prepare the agency for a security breach. Section III and IV are activities that take place if a security breach has occurred.

I: Protection, Prevention and Detection

While an organization's information security program may be unique to its situation, there are recognized basic components of a comprehensive, multilayered program to protect Personal Information from unauthorized access. An organization should protect the confidentiality of Personal Information whether it pertains to members of the public, employees or other individuals. For both paper and electronic records, these components include physical, technical and administrative safeguards. The following safeguards are recommended practices which are more inclusive than those required by RCW 42.56.590.

1. Collect the minimum amount of Personal Information necessary to accomplish the business purposes, and retain it for the minimum time necessary.
2. Collect notification contact information (mailing address and/or e-mail address) from individuals when notice-triggering Personal Information is collected. If the procedure calls for contacting affected individuals by e-mail, obtain the individuals' prior written consent to the use of e-mail for that purpose (as provided in the federal Electronic Signature Act, Public Law No: 106-229).
3. Create an inventory of records systems, critical computing systems, databases, files and storage media containing Personal Information. Include laptops and handheld devices used to store Personal Information. In order to assist agencies in this identification process the System/Database Inventory Form is provided on page35.

4. Classify Personal Information in records systems according to sensitivity (notice-triggering, private information and High-Risk Personal Information). Identify systems containing Notice-Triggering Information and those containing High-Risk Personal Information in the inventory.
5. Use physical and technological security safeguards as appropriate to protect Personal Information, particularly High-Risk Personal Information such as Social Security number, driver's license number, Washington state identification card number, financial account numbers and any associated passwords and PIN numbers, other financial information, and health information, in paper as well as electronic records.
    - Authorize Workforce Members to have access to only the specific categories of Personal Information that are required by their job responsibilities.
    - Where possible, use technological means to restrict internal access to specific categories of Personal Information (e.g. access rights).
    - Monitor Workforce Member access to notice-triggering and High-Risk Personal Information (e.g. via system audit logs).
    - Immediately remove access privileges of former Workforce Members.
6. Promote awareness of security and privacy policies and procedures through training and communications. OIRM provides a web based course on Information Security and Privacy and several one hour classroom courses in information privacy, watch email for future sessions or contact OIRM to schedule a session. Course materials can be found at: http://kcweb.metrokc.gov/oirm/projects/security_privacy.aspx.
    - Monitor Workforce Member compliance with security and privacy policies and procedures.
    - Include all Workforce Members in security and privacy training prior to assigning work tasks that involve processing Personal Information.
    - Develop personnel policies, communicate and impose penalties for violation of security and privacy policies and procedures.
7. Require written agreement from third-party service providers and business partners who have access to Personal Information to follow agency security policies and procedures.
    - Make privacy and security obligations enforceable by including provisions in all third party contracts.
    - Monitor and enforce third-party compliance with privacy and security policies and procedures.
8. Use intrusion detection/prevention technology and procedures to ensure rapid detection of unauthorized access to High-Risk Personal Information. OIRM offers Host Intrusion Detection services to agencies for servers and workstations. This service can assist in protecting databases and systems containing High-Risk Personal Information. Host intrusion detection can identify unauthorized attempts to obtain such information. For information on Host Intrusion Detection systems contact the Chief Information Security and Privacy Officer.
9. Ensure that audit logging is active on systems and that logs are reviewed regularly. Ensure that logs are analyzed, unusual access to High-Risk Personal Information is investigated and logs are retained.
10. Conduct periodic penetration tests to determine effectiveness of systems and staff procedures in detecting and responding to security breaches. Contact the Chief Information Security and Privacy Officer for assistance.

11. Wherever feasible, use data encryption, in combination with host intrusion detection\prevention and access control, to protect High-Risk Personal Information. Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard (AES).
12. Dispose of records (according to the records retention schedule) and equipment containing High-Risk Personal Information in a secure manner, such as shredding paper records with a cross-cut shredder (strip shredders are not sufficient) and using a program to "wipe" and overwrite the data on hard drives. Destroy CDs, diskettes, and hard drives using proper methodologies. If you need assistance in this area contact the Chief Information Security and Privacy Officer.
13. Review agency security plans at least annually or whenever there is a material change in business practices that may affect the security of Personal Information. For example, if an organization decides to outsource functions that access Personal Information, such as using a call center, the plans should be revisited to take the new third parties into account.

II: Preparations in Advance of a Security Breach

Identification of a security breach, reporting and notification are the responsibilities of each agency. To ensure timely notice to affected individuals when appropriate, the following practices are among those that to be included in every agency's procedures:

1. Each agency should develop and adopt an incident response plan. This plan should include methodologies and technology that will assist in identifying the occurrence of a security breach of Personal Information.

2. Deploy and use all available systems that can assist in detecting and preventing a security breach. This would include but is not limited to Host Intrusion Prevention Systems (on all workstations and all mission critical servers or those containing higher risk Personal Information), vulnerability scanners, encryption systems, Anti-virus and Anti-Spyware tools. Carefully configure alerts and check logs regularly in order to detect inappropriate activity.

3. Adopt written procedures for internal reporting of security incidents that may involve unauthorized access to High-Risk Personal Information. **Each agency must define a reporting methodology** (see Agency Activities in section III: Security Breach Reporting, Coordination, Communication and Investigation Procedures for assistance).

4. Designate one staff member as the Security Breach Coordinator for the agency. This person manages internal procedures and coordination with the Chief Information Security and Privacy Officer.
5. Regularly train Workforce Members for their roles and responsibilities during incident response.
6. Establish an incident response team. Collect 24/7 contact information for response team members. Ensure that all team members have this information.
7. Identify responsible individuals in the agency response plan and define key terms.
8. Plan for and use measures to contain, control and correct any security incident that may involve High-Risk Personal Information.
9. Require the data custodian or others who detect an information security incident to immediately notify the Data Owner upon the detection of any security incident that may involve unauthorized access to High-Risk Personal Information. The Data Owner then notifies others in the proper hierarchy of the agency and/or county.

10. Require third-party service providers and business partners to adopt and follow reporting procedures. Monitor and contractually enforce third party compliance.

III: Security Breach Reporting, Coordination, Communication and Investigation Procedures

Unauthorized Access:

In determining whether unencrypted Notice-Triggering Information has been inappropriately accessed, or is reasonably believed to have been accessed, by an unauthorized person, consider the following factors, among others:

- Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer, CD, diskette, report or other device or media containing unencrypted High-Risk Personal Information.
- Indications that the information has been downloaded, emailed, faxed, printed or copied by an unauthorized individual.
- Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Each agency must determine its own specific methodology for identifying such a security breach. OIRM's office of Information Security and Privacy may assist in making the determination upon request. Once it has been determined that Personal Information (as defined on page 8) may have been accessed by an unauthorized person the following procedure begins:

Agency Activities:

Agencies may augment the following notification process with additional notification steps..

1. Data Custodian or person detecting unauthorized access notifies Data Owner.
2. Data Owner notifies IT group (ITSDM, IT Manager, TMB member, etc)
3. Data Owner notifies agency management (Department/Division Manager, BMC member, etc)
4. TMB/BMC member notifies agency Security Breach Coordinator
5. Data Owner and Data Custodian completes the following incident forms and presents them to the Security Breach Coordinator
    - Security breach Identification Form (see page 29)
    - Security breach System Survey Form (see page 31)
6. Security Breach Coordinator completes the following incident forms
    - Security Breach Contact List (see page 32)
    - Security Breach Communications Log (with any communications to date) (see page33)
7. Security Breach Coordinator provides Chief Information Security and Privacy Officer (CISPO) with copies of all report forms

> Note: All forms involved in this process could contain confidential information. Keep all copies in a safe secure location at all times. Do not send electronic copies through unencrypted email. Since time is of the essence in such cases. hand carried

documents may be necessary rather than using King County's inter-office mail system.

The following text should be attached to each form either as a footer or affixed in some other manner:

"This information is considered confidential security information.

All or part of this document may be exempt from disclosure pursuant to RCW 42.56 et seq. the Washington Public Disclosure Act. It contains information about the infrastructure and security of King County, Washington's computer and/or telecommunication networks. Accordingly, every effort must be made to control access to this document and the information contained within the document. Requests for public disclosure of this document, or any parts thereof, should be immediately referred the Chief Information Security and Privacy Officer and the King County Prosecuting Attorney's Office."

OIRM Chief Information Security and Privacy Officer (CISPO) Coordination:

The CISPO will notify and coordinate with the following agencies (if necessary). Actions taken will be documented in the Security Breach Communications Log for law enforcement and debrief sessions.

1. Security Breach Coordinator
    - Receives incident reports
    - Provides ongoing status reports
    - Authorizes notification process. Unless investigation is underway by a designated law enforcement agency, this authorization will be provided within 10 business days of CISPO notification of incident.
2. Prosecuting Attorney's Office
    - CISPO notifies PAO representatives
    - Seeks legal advice in coordination of incident and involvement of law enforcement for criminal prosecution if warranted
3. Risk management
    - CISPO Notifies Risk Management for purposes of insurance and future claims management
4. OIRM Management
    - CISPO will notify CIO and other OIRM management as appropriate to assist in coordinating digital forensics investigations, both network and host.
    - OIRM technical staff would review intrusion detection and auditing logs in cooperation with agency technical staff and possibly law enforcement.
5. Executive Office Communications Directory
    - If necessary CISPO will discuss with Media Relations options relative to press releases
6. Law Enforcement

- As advised by PAO and in discussion with the agency, the CISPO will notify law enforcement via the King County Sheriff's Office (KCSO).
- KCSO will assist CISPO in identifying and notifying appropriate local jurisdiction(s) to assist in conducting
    - Criminal Investigation
    - Digital Forensics analysis (if criminal prosecution is expected)
- Appropriate law enforcement agencies include the King County Sheriff's Office, Washington State Attorney General's Office, Federal Bureau of Investigation, the U.S. Secret Service, the National Infrastructure Protection Center, and the local police departments.

7. Consumer Credit Reporting Agencies

- A security breach involving a large number of individuals can potentially have a significant impact on consumer credit reporting agencies and their ability to respond efficiently. High volumes of calls could impede access to these agencies and therefore their ability to assist affected individuals. The CISPO will contact the three consumer credit reporting agencies (Equifax, Experian and TransUnion) before King County agencies send out notices in cases in excess of 10,000 individuals.
- The CISPO will make notification to the consumer credit reporting agencies during notice preparations. The coordination with consumer credit reporting agencies will not delay the notice to individuals.
- The CISPO will provide contact information for the three consumer credit reporting agencies to include in the notification letters if different from that in the letter templates in appendix 3.
- The CISPO will contact the following three consumer credit reporting agencies using the method detailed below:
    - **Experian**: E-mail to BusinessRecordsVictimAssistance@experian.com.
    - **Equifax**: Chris Jarrard, Vice President – US Customer Services, Equifax Information Services, LLC, Phone: 678-795-7090, Email: chris.jarrard@equifax.com.
    - **TransUnion**: E-mail to fvad@transunion.com, with "Database Compromise" as subject

Notification:

Agencies will conduct notification as described in the section IV on page16. The notification process may, depending upon the nature of the security breach involve the implementation and/or staffing of a call center. This is also the responsibility of the agency.

Remediation:

Agencies will promptly repair and/or remediate the vulnerability or issue that allowed the security breach to occur. The method of repair and/or remediation must be approved by the Chief Information Security and Privacy Officer. The Chief Information Security and Privacy Officer will verify the effectiveness of the remediation taken.

Debrief:

CISPO will conduct debriefing sessions with:

1. Key agency staff

   To determine what worked, what did not work in the reporting and coordination process, how to prevent such incidents in the future, and additional protective measures to implement.

2. Department Director and CIO

   To discuss outcomes.

Documentation Retention:

After the debriefing sessions are documented all documentation associated with each incident will be transferred to Risk Management to correlate with future potential litigation and claims, if any. Copies will be retained by the CISPO for reference and reporting purposes.

IV: Notification of Affected Individuals

Openness or transparency is a basic privacy principle. An organization that collects or manages Personal Information should be open about its information policies and practices (see King County's Information Privacy Policy at http://kcweb/oirm/governance/policies/KCIT_Privacy_Policy.doc.) This responsibility includes informing individuals about incidents such as security breaches that have caused their unencrypted Personal Information to be acquired by unauthorized persons. The purpose of notifying individuals of such incidents is to enable them to take actions to protect themselves against, or mitigate the damage from identity theft or other possible harm.

ALL NOTIFICATION, CALL CENTER MANAGEMENT AND STAFFING, REQUIRED REMEDIATION AND CORRECTIVE ACTIONS ARE THE RESPONSIBILITY OF THE AGENCY.

THE FOLLOWING PROCESSES ARE THE RESPONSIBILITY OF THE AGENCY.

To ensure timely and helpful notice is given to affected individuals, the following practices should be followed.

Timing of Notification:

Notify affected individuals in the most expedient time possible after the discovery of an incident involving unauthorized access to High-Risk Personal Information.

- Take necessary steps to contain and control the systems affected by the security breach and conduct a preliminary internal assessment of the scope of the security breach. OIRM Information Security and Privacy Office can assist with this assessment.
- Once you have determined that the information was, or is reasonably believed to have been, accessed by an unauthorized person, begin the reporting process outlined in section III above and prepare to notify affected individuals within 10 business days from the time of discovery. Delays are only permitted if law enforcement authorities indicate that providing notice would impede an investigation.
- **Do not send letters of notification until authorized by the CISPO.** Agencies should be prepared to send notices immediately upon approval by the CISPO.

CONTACTING LAW ENFORCEMENT: DO NOT CONTACT LAW ENFORCEMENT DIRECTLY. THIS WILL BE COORDINATED BY THE CISPO AND REPRESENTATIVES OF THE SHERIFF'S OFFICE WITH APPROPRIATE LOCAL JURISDICTIONS.

If the agency believes that the incident may involve illegal activities, this must be discussed this with the CISPO so that it can be reported to appropriate law enforcement agencies.

- The CISPO will inform the law enforcement official in charge of the investigation that notification of affected individuals is intended to be sent out within 10 business days.
- It should not be necessary for a law enforcement agency to complete an investigation before notification can be given. However, if the law enforcement official in charge tells the CISPO that giving notice within that time period would impede the criminal investigation:
    - The CISPO will ask the law enforcement official in charge of the investigation to document, in writing the need for the delay in notification. The CISPO will forward a copy to the agency Security Breach Coordinator.
    - The law enforcement official will be asked to inform the CISPO as soon as notification can begin without impeding the criminal investigation.

Whom to Notify:

If an assessment leads to a reasonable belief that Notice-Triggering Information was accessed by an unauthorized person, implement the notification plan. Upon CISPO authorization:

- Consider providing notice when a security breach involves High-Risk Personal Information, even when it is not "Notice-Triggering Information", if being notified would allow individuals to take action to protect themselves from possible harm.
- Notify all individuals whose Notice-Triggering Information was acquired by an unauthorized person. The law requires that only Washington residents be notified. However it is a better business practice to notify all potentially affected persons. 34 other states have enacted similar legislation. Therefore it would be necessary to notify any individual whose residence is within any of these other 34 states. This suggests that notifying all individuals would be prudent.
- Notify affected individuals in situations involving unauthorized access of Notice-Triggering Information notwithstanding the media that contained the information, including computer printouts and other paper records.
- Avoid false positives. A false positive occurs when the required notice of a security breach is sent to individuals who should not receive it because their Personal Information was not accessed as part of the security breach. Consider the following when identifying the group that will be notified:
    - Before sending individual notices, make reasonable efforts to include only those individuals whose Notice-Triggering Information was likely accessed.
    - Implement procedures for determining individuals to be included in the notice. Have a staff member other than the one creating the mailing list check the list before sending the notice to be sure it is not over-inclusive.
    - Document your process for determining inclusion in the notified group.
- If you cannot identify the specific individuals whose High-Risk Personal Information was accessed, notify all those in the groups likely to have been affected, such as all whose information is stored in the files involved.

Contents of Notice:

Sample notice letters are attached as Appendix 3. Include the following information in your notice to affected individuals:

- A general description of what happened.

- If law enforcement is involved, provide the law enforcement agency and applicable case number.
- The nature of the Personal Information that was involved (not the actual Personal Information that was breached, such as a person's actual Social Security number).
- A description of what actions have been taken to protect the individual's Personal Information from further unauthorized access.
- What the organization will do to assist individuals, including providing an internal contact telephone number, preferably toll-free, for more information and assistance, credit monitoring etc.
- Information concerning the actions individuals can take to protect themselves from identity theft, including contact information for the three consumer credit reporting agencies.
- Contact information for the Washington State Attorney General's Office and/or the Federal Trade Commission for additional information on protection against identity theft.
    - Federal Trade Commission 877-ID-THEFT/877-438-4338 www.consumer.gov/idtheft/
    - Office of Attorney General (360) 753-6200 http://www.atg.wa.gov/consumer/idprivacy/IDTheftWhatToDo.shtml

Form and Style of Notice Letters:

Make the notice clear and helpful.

- Use agency letterhead. This is in order to ensure validity and assure the recipient that the notice is official.
- Use clear, simple language, subheadings, and plenty of white space in the layout.
- Avoid jargon or technical language.
- Avoid using a standardized format, which could result in making the public complacent about the process and thus undercut the purpose of the notice.
- To avoid confusion, the notice letter should be a standalone document, not combined as part of another mailing.
- The letters should be signed by the agency's Department Director.
- Provide a contact number for inquiries.

Means of Notification:

Individual notice to those affected is preferable whenever possible.

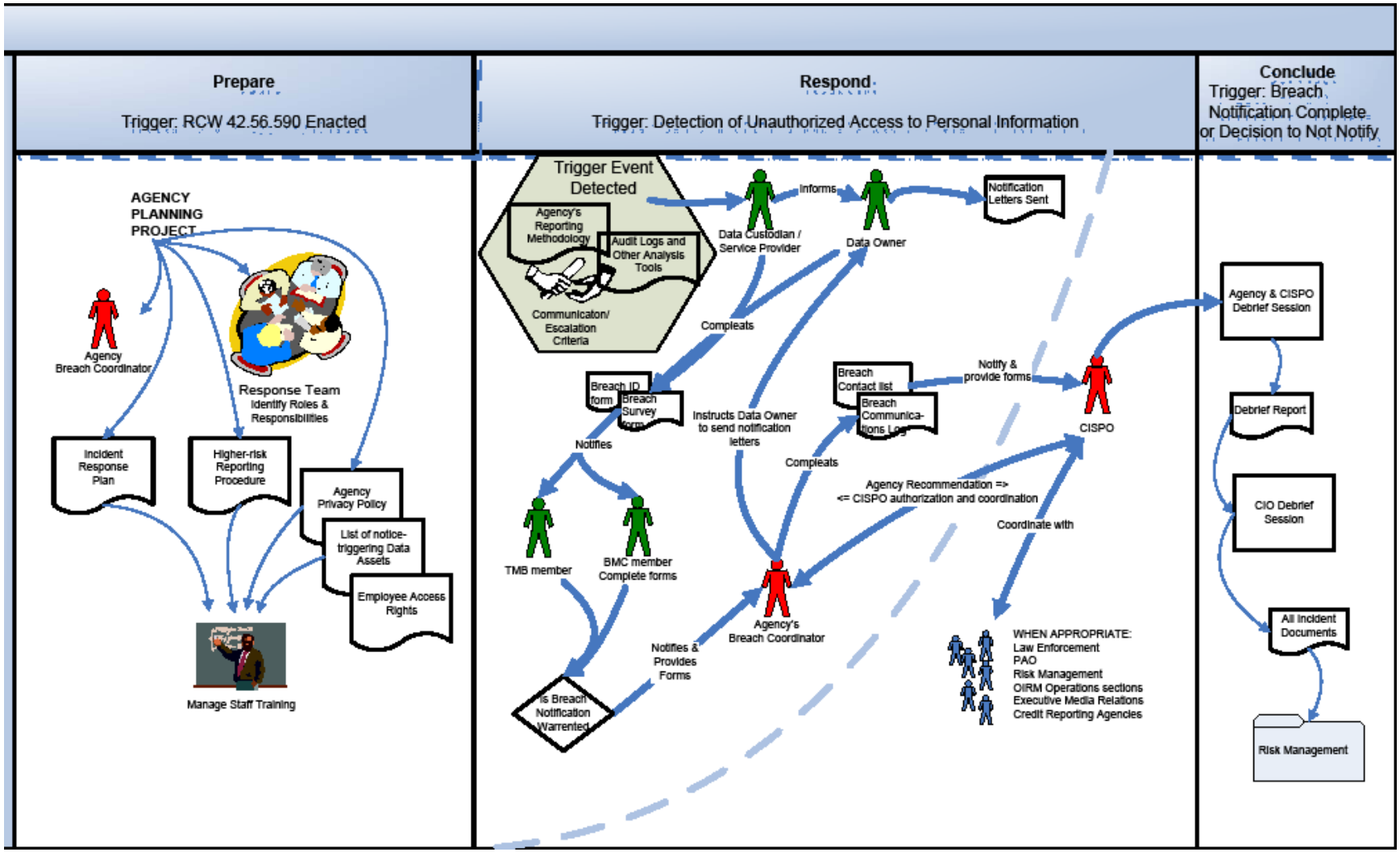
- Send the notice to all affected individuals.
- If more than 500,000 individuals were affected or if the cost of giving individual notice to affected individuals is greater than $250,000 and you are using the statutory Substitute Notice procedures, the CISPO and Executive's Office Media Relations will assist with this notification method:
    - Send the notice by e-mail to all affected parties whose e-mail address are available AND
    - Post the notice conspicuously on an appropriate web site; and
    - Notify major statewide media (television, radio, print).

Appendix 1: Process Flow Diagram

Page intentionally left blank

The following diagram shows the process flow for security breach notification process.

Figure 1 Security Breach Coordination and Notification Process Flow



Page intentionally left blank

Appendix 2: RCW 42.56.590 Personal Information – Notice of Security Breaches

Page intentionally left blank

RCW 42.56.590

Personal information — Notice of security breaches.

(1)(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) For purposes of this section, "agency" means the same as in RCW 42.17.020.

(2) Any agency that maintains computerized data that includes personal information that the agency does not own 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 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, "breach of the security of the system" means unauthorized acquisition of computerized 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.

(5) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(a) Social security number;

(b) Driver's license number or Washington identification card number; or

(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(6) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(7) For purposes of this section and except under subsection (8) of this section, 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) E-mail notice when the agency has an e-mail 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.

(8) 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.

(9) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

(10)(a) Any customer injured by a violation of this section may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this section may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

(d) An agency shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.

[2005 c 368 § 1. Formerly RCW 42.17.31922.]

Notes:

Similar provision: RCW 19.255.010.

Appendix 3: Reporting Forms

Page intentionally left blank

Security Breach Identification Form

General Information

Security Breach Detected By: Name: _____ Title: _____

Department/Division: _____

Phone: _____ Alt. Phone: _____

E-mail: _____ Fax: _____

Address: _____

Date and Time Detected: _____

Location Incident Detected From: _____

Additional Information: _____

_____

_____

Security Breach Summary

Security Breach Location:

Site: _____ Site Contact Person:_____

Phone:_____ Fax:_____

E-mail:_____ Address: _____

How was the security breach detected: _____

_____

_____

_____

_____

_____

Describe techniques used to detect the security breach: _____

_____

_____

If security breach is only suspected, please describe why you suspect a security breach has occurred.

_____

_____

_____

What Data Elements were compromised? (Do not provide the raw data just describe the data elements)

_____

_____

_____

Approximate number of individuals whose data was compromised: _____

Can WA State residents be determined from available data? Yes ☐ No ☐

Describe what action has been taken so far:

_____

_____

_____

_____

_____

Additional Information:

_____

_____

_____

Location(s) of affected systems:

_____

_____

_____

Describe affected information system(s): (one form per system is recommended)

Hardware Manufacturer:_____

Serial Number:_____ Asset Tag: _____

Was the affected system connected to the network? Yes ☐ No ☐

Is the affected system still connected to the network? Yes ☐ No ☐

System Name:_____

System IP Address:_____ MAC Address: _____

Was the affected system connected to a modem? Yes ☐ No ☐

Is the affected system still connected to a modem? Yes ☐ No ☐

Modem Phone Number: _____

Describe the physical security of the location of affected information systems (locks, security alarms, building access, etc.)**:**

_____

_____

_____

_____

_____

_____

Security Breach Contact List

Data Owner

Name:_____

Title:_____

Phone:_____

Alt Phone:_____

Fax:_____

E-mail:_____

Address:_____

_____

Notified? Yes ☐ No ☐

Department Security Breach Coordinator

Name:_____

Title:_____

Phone:_____

Alt Phone:_____

Fax:_____

E-mail:_____

Address:_____

_____

Notified? Yes ☐ No ☐

Department PAO Contact

Name:_____

Title:_____

Phone:_____

Alt Phone:_____

Fax:_____

E-mail:_____

Address:_____

_____

Notified? Yes ☐ No ☐

Department IT Manager

Name:_____

Title:_____

Phone:_____

Alt Phone:_____

Fax:_____

E-mail:_____

Address:_____

_____

Notified? Yes ☐ No ☐

Department Media Relations

Name:_____

Title:_____

Phone:_____

Alt Phone:_____

Fax:_____

E-mail:_____

Address:_____

_____

Notified? Yes ☐ No ☐

Department Risk Management

Name:_____

Title:_____

Phone:_____

Alt Phone:_____

Fax:_____

E-mail:_____

Address:_____

_____

Notified? Yes ☐ No ☐

Security Breach Communication Log

Date:_____ Time:_____ AM ☐ PM ☐ **Method: Mail ☐ E-mail ☐ Phone ☐ Other:_____**

Initiator Name:_____ Receiver Name:_____

Initiator Title:_____ Receiver Title:_____

Department:_____ Department:_____

Phone:_____ Phone:_____

Fax:_____ Fax:_____

E-mail:_____ E-mail:_____

Details:_____

_____

_____

_____

_____

_____

Date:_____ Time:_____ AM ☐ PM ☐ **Method: Mail ☐ E-mail ☐ Phone ☐ Other:_____**

Initiator Name:_____ Receiver Name:_____

Initiator Title:_____ Receiver Title:_____

Department:_____ Department:_____

Phone:_____ Phone:_____

Fax:_____ Fax:_____

E-mail:_____ E-mail:_____

Details:_____

_____

_____

_____

_____

_____

Page intentionally left blank

System/Database Inventory Form

(Use one form for each system)

Name of System/Database: _____

Describe the purpose of this system or database: (Describe its function, reason for existence, what business purpose it serves, why your agency collects this information.)

_____

_____

Hardware:
Identification information (Name, location, etc)

_____

_____

Hardware Manufacturer:_____

Serial Number:_____ Asset Tag: _____

List all fields contained in this database that contain Private Information:

_____

_____

_____

_____

List all fields contained in this database that contain potentially sensitive information:

_____

_____

_____

_____

_____

Describe the protective measures/policies/practices currently in place designed to detect/prevent security breaches: (i.e. Host intrusion/prevention systems, log management/monitoring practices, Access control processes/practices, etc.)

_____

_____

_____

_____

_____

_____

_____

_____

Additional Information: _____

_____

_____

_____

_____

_____

_____

Appendix 4: Sample Notice Letters

Page intentionally left blank

SAMPLE LETTER 1(on Department letterhead)

Data Acquired: Credit card Number or Financial Account Number

Dear :

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, what kind of Personal Information was involved, and what you are doing in response*.]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. We recommend that you immediately contact [*credit card or financial account issuer*] at [*phone number*] and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask [*name of account issuer*] to give you a PIN or password. This will help control access to the account.

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

Equifax	Experian	Trans Union
800-525-6285	888-397-3742	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for Personal Information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency and applicable case number investigating the incident*.] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft we suggest that you contact the Office of Attorney General. The telephone numbers is (360) 753-6200. Or you can visit their web site at http://www.atg.wa.gov/consumer/idprivacy/IDTheftWhatToDo.shtml. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing – Department Director's Signature*]

SAMPLE LETTER 2 (on Department letterhead)

(Data Acquired: Driver's License or Washington ID Card Number)

Dear :

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, how the drivers license or Washington state identification card was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. Since your Driver's License [*or Washington Identification Card*] number was involved, we recommend that you immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license.

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

Equifax	Experian	Trans Union
800-525-6285	888-397-3742	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for Personal Information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency and applicable case number investigating the incident*.] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft we suggest that you contact the Office of Attorney General. The telephone numbers is (360) 753-6200. Or you can visit their web site at http://www.atg.wa.gov/consumer/idprivacy/IDTheftWhatToDo.shtml. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing – Department Director's Signature*]

SAMPLE LETTER 3 (on Department letterhead)

(Data Acquired: Social Security Number)

Dear :

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, how the Social Security Number was involved, and what you are doing in response*.]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft.

We recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Then call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

Equifax	Experian	Trans Union
800-525-6285	888-397-3742	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for Personal Information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency and applicable case number investigating the incident.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft we suggest that you contact the Office of Attorney General. The telephone numbers is (360) 753-6200. Or you can visit their web site at http://www.atg.wa.gov/consumer/idprivacy/IDTheftWhatToDo.shtml. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing – Department Director's Signature*]

Page intentionally left blank