

Personal Information Protection Policy

Purpose: This policy outlines specific **employee responsibilities** in regards to safeguarding personal information. To this end, each employee has a responsibility to safeguard personal information in his/her care.

1. GENERAL PROVISIONS

Overview: Identity theft is a rapidly growing issue in Washington County. This policy provides guidance to county employees on how to protect and maintain files that contain personal information and implements the requirements of Oregon's recently enacted Consumer Theft Protection Act (Senate Bill (SB) 583). *Personal information means written or electronic information including a person's first and / or last name, social security number, drivers license number, passport number, financial account number or a combination of any of these which could be used to steal a person's identity.*

2. DEFINITIONS

The following are terms commonly referenced in this Policy. In the event of conflict or absence of a term, the definitions set forth in Senate Bill 583 and the implementing state statutes, ORS 646A.600 et seq., shall govern:

Personal Information: Any information that could be used to steal a person's identity. Specifically, written or electronic information including a person's first name or first initial and last name in combination with any one or more of the following:

- Social security number,
- Drivers license number or State identification card number issued by the Department of Transportation
- Passport number or other United States issued identification number
- Financial account number, credit or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account.
- Any of the above data individually or in combination, even if not combined with the consumer's first name, first initial or last name, if the data is not encrypted or redacted or otherwise rendered unusable, if the information would be sufficient to commit identity theft against the individual.

3. COMPLIANCE

Following is what is required of the County to comply with SB 583

I. Requirements

A. Security Breach Notification

The County is required to notify individuals if any electronically stored information or written document that contains personal information about that individual has been subject to a security breach. Any County employee who becomes aware of any potential breach of a document or electronic file containing personal information will immediately notify his/her supervisor. The employee's department Director, appointed Information Security Officer and Supervisor will follow the appropriate Centralized Breach Notification Process

(Attachment A), and work with the department appointed Information Security Officer County Public Information Officer to notify the affected persons, if warranted.

A breach occurs when any unauthorized individual or entity gains access to personal information or when unintended disclosure of personal information is made. Examples of a breaches include but are not limited to: loss or theft of an electronic device (such as laptops, Personal Digital Assistants (PDAs), Blackberries or thumb drives) upon which user has copied or stored personal information; loss or theft of a paper document containing personal information; unauthorized access to a network containing personal information; or a document containing personal information being sent to the wrong address.

Personal information should never be stored on portable media purchased and controlled by departments (such as CDs or thumb drives) unless the information has been encrypted. Notwithstanding that, a breach of personal information related to such devices must still be reported to the Supervisor and department appointed Information Security Officer.

B. Protection of Social Security Numbers (SSN)

No County employee will print a person's full SSN on any document that will be sent through the mail, without a written request from the person whose SSN will be printed on the document, except as required by law. County employees will use only the last 4 digits of a SSN on all documents unless there is a compelling business reason to use the entire SSN. If a document contains a full SSN, county employees will take steps to protect the document from unauthorized disclosure. Employees will not provide copies of a document containing a full SSN to anyone other than the person whose SSN is listed on the document, except as allowed by State or Federal law. Employees may provide a copy of a document to a third party with the SSN redacted if the document is otherwise allowed to be released. No County employee will publicly post or display a document containing a full SSN.

C. Safeguarding Personal Information

Any County department that collects personal information must develop, implement and maintain reasonable safeguards to protect the security and confidentiality of the information. Employees with access to personal information must take reasonable steps to prevent a breach of the information. Reasonable steps include but are not limited to: locking file cabinets; monitoring who has access to areas containing personal information; locking computer workstations if leaving the area; maintaining physical control over files, computer workstations and laptops which contain personal information; never saving personal information on your computer's c:\drive; never copying or storing personal information on portable media purchased by departments such as thumb drives or CDs unless the data is encrypted; securing Blackberries and PDA's with passwords and never sending emails containing personal information unless the data is encrypted .

Employees must also ensure the proper disposal of documents or other media which contains personal information. Contracting with a document shredding company will be considered proper disposal of paper documents. ITS will be responsible for properly disposing of or erasing electronically stored personal information on devices that have become obsolete and no longer in use. This would include workstations, Blackberries and laptop hard drives. Employees have a personal responsibility for properly disposing of or erasing electronically stored personal information on CDs, thumb drives or other media devices purchased through their department. If an employee is unsure of proper disposal methods of portable media devices purchased by their department, the media should be

sent to ITS for proper disposal. Note: Personal information should never be stored on portable media purchased and controlled by departments (such as CDs or thumb drives) unless the information has been encrypted.

As the internet allows the public to be able to access County information, departments must ensure that personal data that is acquired as part of the County's providing a service is not inadvertently made available to the public via the internet or through request for County information.

D. Department Directors must designate a Security Officer whose is responsible for the security of personal information, reducing its risk of exposure and ensuring that their department activities do not introduce risk to other County departments.

E. Department employees whose work involves maintaining personal information are responsible for protecting the confidentiality, integrity and availability of this data.

II. Violations

The requirements of SB 583 will be monitored and enforced by the State of Oregon, Department of Consumer and Business Services. Violations may result in penalties up to a maximum of \$500,000 per occurrence. Violation of this Policy may also constitute just cause for disciplinary action up to and including discharge.



COUNTY DATA BREACH INCIDENT ASSESSMENT FORM

Form Completion Instructions:

- To enter text, simply click on shaded area (it will turn black) and begin to enter information).
- To put a checkmark in a box, simply double click on square and choose "checked" under "default value".
- Save form to **secure** area before printing. **Note:** Pages 5-11 are standard best practices and need not be printed each time.

1. Department/Division Name:

2. Date/Time:

Part A: Risk Assessment

3. Incident Date/Time:

4 Provide detailed description of data breach incident:

5. What type of Personal Information is involved in this data breach? Check all that apply:

- First name or initial
- Last name
- Social Security Number
- Driver's License Number
- Passport Number or other United States issued ID Number
- Financial Account Number, credit or debit card # in combination with any required security code, access code or password
- Other, explain:

6. If the personal information was in electronic format (on the County's network or on a portable media device, was it encrypted? Check the appropriate box:

- Yes
- No

Provide detail:

7. Was the breach (check all that applies):

- Internal – breach committed by County employee or from within the County
- External – breach committed by non-County employee or from outside the County

- Intentional
- Unintentional

8. Estimated # of identity theft victims impacted by the data breach:

Part B – Breach Assessment Group Findings and Recommendations

9. Based on the Breach Assessment Meeting and the findings documented in PART A, the department’s recommendation below has been (check the appropriate box):

- Agreed upon
- Not agreed upon. State reason(s): _____

RECOMMENDATION (check the appropriate boxes):

<input type="checkbox"/> Notification based on SB 583 Statutes is warranted (See Notification Best Practices on page 5 of this document for guidance).	<input type="checkbox"/> There is no basis for notification under SB 583.
<input type="checkbox"/> A criminal act is believed to have been committed and notification will proceed in accord with the appropriate law enforcement agency.	<input type="checkbox"/> There is no basis to believe a criminal act has been committed.

SIGNATURES:

X Department Director (Print Name)	Signature/Date
X Information Technology Services (Print Name and Title)	Signature/Date
X County Counsel (Print Name and Title)	Signature/Date

Part C – County Administrator Decision (Completed only in case of Part B disagreement)

10. Based on the review of findings, the County will take the following course of action (check the appropriate boxes):

<input type="checkbox"/> Notification based on SB 583 Statutes is warranted (See Notification Best Practices on page 3 of this document for guidance).	<input type="checkbox"/> There is no basis for notification under SB 583.
<input type="checkbox"/> A criminal act is believed to have been committed and notification will proceed in accord with the appropriate law enforcement agency.	<input type="checkbox"/> There is no basis to believe a criminal act has been committed.

X

County Administrative Officer (Print Name)

Signature/Date

Part D – Safeguard Improvement Review and Recommendations for corrective Action

11. Provide detail here:



ATTACHMENT

Washington County SB 583 Notification Best Practices

Departments will work through the County Public Information Officer on all notifications.

1.0	Establish a process for determining who to notify, once the need for a breach notice has been triggered.	Required	Optional	N/A
1.1	Determine who has been affected, and notify each affected individual when possible. Double-check the list of recipients before sending.			
1.2	<p>Determine proper notification medium:</p> <ul style="list-style-type: none"> ○ Written (Sample on page 6) ○ Electronic if this is the person’s customary method of communication ○ Telephone, provided that the contact is made directly with the affected consumer ○ Substitute notice, if an agency can demonstrate that the cost of providing notice would exceed \$250,000, that the affected class of consumers to be notified exceeds 350,000, or if the agency does not have sufficient contact information to provide notice. Substitute notice consists of the following: <ul style="list-style-type: none"> ▪ Conspicuous post of the notice or a link to the notice on the Internet home page of the person if the person maintains one and ▪ Notification to major statewide television and newspaper media. ▪ Set up or use an existing toll free number for potential victims to call – train staff how to respond to callers – expect about 15- 20 % of potential victims to call ▪ Develop a list of FAQ’s and post on the Agency Web site (see Sample on page 9) ▪ Depending on the level of risk, determine the need to offer potential victims a credit monitoring service (generally for 6 months to a year – Sample letter provided on page 7) ▪ Consider the option of giving general public notice, on your Web site and/or through major media, where the group to be notified is very large or it is otherwise appropriate. 			
1.3	Try to ensure that only those individuals whose personally identifiable information was compromised are included in the group to be notified. If you cannot determine the exact individuals affected, consider notifying all members of the group affected if the likelihood of material harm outweighs the uncertainty that the individuals were affected.			
2.0	Considerations that affect the timing of a breach notice	Required	Optional	N/A

2.1	In general, notify affected individuals as soon as reasonably possible after a breach is discovered, unless law enforcement officials indicate that notice would impede their investigation.			
2.2	If you have reported the breach to law enforcement, ask them to inform you when it is safe to notify affected individuals. Send out notice as soon as practicable and in compliance with existing notification laws when so informed. Follow up with law enforcement in order to find out when it is safe to notify the affected individuals. When possible, get such confirmation in writing.			

3.0	Content of breach notice communication.	Required	Optional	N/A
3.1	Consider carefully the content of any breach notice communications, and focus on providing the most useful information possible.			
3.2	In the case of consumer breach, notification should include: <ul style="list-style-type: none"> ○ The date of the breach ○ The information accessed ○ Description of the incident in general terms ○ Contact information ○ Contact information for national consumer reporting agencies ○ Advice to the consumer to report suspected identity theft to law enforcement, including the Federal Trade Commission. 			
3.3	Consider available options, should you not have complete contact information for all impacted individuals:			
3.4	Consider providing further information that might be helpful for those who believe that they maybe a victim of identity theft. For example, including a brochure about how to set up credit monitoring or how to read a credit report could be helpful. Information available from the Federal Trade Commission (www.ftc.gov/bcp/menus/consumer/data/idt.shtm).			
3.5	Consider offering free credit monitoring services for one year to affected individuals, particularly if the incident involved Social Security or Driver’s License numbers. (When considering making such an offer, note that often only about 25% of consumers will accept such an offer.)			
3.6	Consider providing links on your Web site to resources such as the following: <ul style="list-style-type: none"> ○ The three major credit reporting agencies (available at the Federal Trade Commission Web site www.ftc.gov/bcp/online/edcams/gettingcredit/faqs.html) ○ Government agency resources such as this Federal Trade Commission identity theft consumer alert (www.ftc.gov/bcp/online/pubs/alerts/infocompartr.htm) ○ Identity Theft Resource Center (www.idtheftcenter.org) ○ Privacy Rights Clearinghouse (www.privacyrights.org) 			

4.0	Educate and coordinate with your own and other potential resources	Required	Optional	N/A
4.1	Educate your staff or other customer service employees about the breach so they can provide knowledgeable assistance. Consider having assistance available evenings and weekends.			
4.2	If the breach involves financial information, consider notifying credit reporting agencies before sending out notice of a breach to a large number of individuals, so they can prepare for the consequent inquiries. (You will find information about the major Credit Reporting Agencies at www.ftc.gov/bcp/online/edcams/gettingcredit/faqs.html) However, do not delay notice to individuals because of cooperation with credit reporting agencies.			

5.0	Follow Up	Required	Optional	N/A
5.1	Track phone calls received from those who were notified			
5.2	Track those who are registering for credit monitoring (if offered)			
5.3	De-brief with those involved in coordinating/managing the incident			
5.4	Document lessons learned			
5.5	Address security issues causing the incident			
5.6	Update the agency information security plan			

ID Theft Sample Notification Letter

DATE

Important information about your confidential information

On (date), computer security staff at the (Agency Name) found that software from outside our agency attacked an individual machine on our computer network via the Internet. This software was designed to record information and send it back to a Web site outside of our agency. According to the best information available from our staff and computer experts at the Oregon State Police, we believe that your Social Security number and possibly other information such as your name and address may have been sent to the receiving site outside our agency. We do not know whether the site received the information, or whether any use has been or could be made of it. We have identified (number of citizens) whose information is affected and we are researching information from (number) additional citizens to see if their information is affected.

A former employee enabled this intrusion by visiting a Web site in violation of our policies. This employee is no longer working for the (Agency Name). We are diligent about protecting confidential citizen information and deeply regret that our safeguards did not work in this instance. We are reviewing our security practices and procedures to further strengthen our protection for all confidential citizen information.

I am enclosing information about identity theft written by the Federal Trade Commission. I encourage you to monitor your personal information relating to recent financial transactions. If you notice any suspicious activity on your statements, you should report it immediately to the financial institution involved and contact the Federal Trade Commission at www.consumer.gov/idtheft or at 1-877-ID-THEFT (438-4338).

For more information, please call 1-800-xxx-xxxx toll-free from an Oregon prefix or 503-xxx-xxxx (outside Oregon). Choose the language option, then choose option "5" to speak with a representative. If you get a busy signal, please call our message line at 503-xxx-xxxx and leave your name and phone number and we will return your call within four hours. You may also e-mail us at questions. (agency initials)@state.or.us.

TTY (hearing or speech impaired; machine only): 503-xxx-xxxx (Salem) or 1-800-xxx-xxxx (toll-free from Oregon prefix). **Americans with Disabilities Act (ADA):** This information is available in alternative formats. Call 503-xxx-xxxx (Salem) or 1-800-xxx-xxxx (toll-free from Oregon prefix). **Asistencia en español.** Llame al 503-xxx-xxxx en Salem o llame gratis de prefijo de Oregon al 1-800-xxx-xxxx.

Thank you.

(Agency Director Name), Director
(Agency Name)

ID Theft Credit Monitoring Template Letter

DATE

Free Credit Monitoring for Citizens Affected by Illegal Software Intrusion

Recently, the (Agency Name) experienced its worst nightmare—some citizen personal information was recorded by an illegal software program and sent outside our secure computer network. Your personal information was included. Earlier this month, we sent you a letter explaining what happened. We also posted Frequently Asked Questions (FAQs) on our Web site, [www.oregon.gov/\(agency initials\)](http://www.oregon.gov/(agency initials)). To date, we have had no reports of identity theft as a result of this incident. However, to protect your information from possible fraud, we are offering credit monitoring and restoration services at no charge to affected taxpayers.

We have contracted with Identity Safeguards, an Oregon company specializing in protecting and restoring identities. The company offers safe, secure help to affected individuals.

Here's how it works:

- If you choose to enroll, you must contact Identity Safeguards directly.
- ***We will not provide Identity Safeguards with any information about you*** other than to confirm that you are eligible to receive this free service.
- Once you enroll, you will receive a copy of your credit report, regular updates on credit activity, and credit restoration if your information is used fraudulently.

Please see the enrollment instructions on the back of this letter so you can begin your protection with Identity Safeguards. If you have questions about the incident or want more information, please call the (Agency Name and 1-800 number) (toll-free from an Oregon prefix) or 503-xxx-xxxx (Salem area and outside Oregon). If you get a busy signal, please call (503-xxx-xxxx) and leave your name and phone number—we will return your call within four hours.

Since this incident, we have taken further steps to protect all confidential citizen information. I regret this security intrusion. I encourage you to enroll in Identity Safeguards' program to protect your information. Please don't hesitate to call us at one of the numbers above if you have questions. Thank you.

Sincerely,

(Agency Director Name), Director
Name of Agency

Take These Steps to Protect Your Identity and Credit

By taking the following three steps **right now**, you can help protect your identity and credit from fraud. It will take 20 to 30 minutes to complete this process.

Step 1: Enroll in Identity Safeguards' protection services for 12 months. The (Name of Agency) is paying for this service so there is no cost to you. *To enroll in this pre-paid service, visit Identity Safeguards' secure Web site: [www.identitysafeguards.com/\(agency initials\)](http://www.identitysafeguards.com/(agency%20initials)). Instructions will guide you through the enrollment process.*

If you have any questions, please contact Identity Safeguards, [www.identitysafeguards.com/\(agency initials\)](http://www.identitysafeguards.com/(agency%20initials)), or call the (Agency Name), 1-800-xxx-xxxx (toll-free from an Oregon prefix) or 503-xxx-xxxx (Salem area and outside Oregon). If you get a busy signal, please call 503-xxx-xxxx and leave your name and phone number—we will return your call within four hours.

After you enroll, you will receive an information packet, either by e-mail or by regular mail from Identity Safeguards. The information describes its services and the next steps you'll need to take to help protect your good name.

Step 2: Activate the credit monitoring service provided.

You will receive instructions on the credit monitoring service when you enroll (Step 1). Once you start this service, you will receive weekly credit reports that will alert you to any unauthorized changes to your credit. This service is included with your pre-paid membership, *but you must activate it.*

If you notice any suspicious activity on your weekly credit report, immediately report it to Identity Safeguards. An Identity Safeguards recovery advocate will work with you to assess, stop, and reverse any damage to your identity. The (Agency Name) is also paying for this service.

Step 3. Place a fraud alert at one of the three major credit bureaus via the internet or by phone. We encourage you to do this even if you are not aware of any suspicious activity. You do not need to enroll with Identity Safeguards to place this alert yourself.

A fraud alert will prevent someone from opening new financial or credit accounts in your name. As soon as one credit bureau confirms your fraud alert, the others are notified and will also place fraud alerts.

To contact any of the credit bureaus via the internet, visit www.Experian.com. Under the heading, "Identity theft & fraud protection," at the bottom of the page, click on "Steps to take if you are a victim." You will answer some questions to confirm your identity, and a 90-day security alert will be added to your credit file. Experian will allow you to view your report online. Examine it carefully for accuracy. Experian will also share this information with Equifax and TransUnion. All three companies will mail you free copies of your credit reports.

If you prefer, you may contact each credit bureau by phone:

Equifax: 1-800-525-6285

Experian: 1-888-397-3742

TransUnionCorp: 1-800-680-7289

If you choose to enroll in the Identity Safeguards' program and need help contacting the credit bureaus, Identity Safeguards can help you do that at no charge.

Sample FAQ

Frequently Asked Questions

- I received your letter but I am not sure exactly what it means?
- How do I know whether I am affected?
- Why did you even have my personal information?
- Does this mean I am the victim of identify theft?
- What are you going to do about this?
- How can I protect myself from identity theft?
- Why can't I get through to the credit bureau to place my fraud alert?
- What should I look for in my credit report?
- What if there's a problem on my credit report?
- What do I do if I am a victim of identity theft?
- Will a fraud alert prevent me from using my credit cards or getting new ones?
- Can I put a freeze on my credit report so that it is not sent to other people?
- Will the State pay for credit monitoring?
- Is it OK to give my Social Security number to the credit bureau fraud line?
- Should I change my Social Security number?
- Will the state contact me to ask for personal information because of this event?