

ODOT Information Security Incident Management Plan

The Oregon Consumer Identity Theft Protection Act – ORS 646A.600 to 646A.628 (“the Act”), provides consumers with more tools to protect themselves against identity theft. The Act issues clear direction and expectations to Oregon businesses and government to ensure the safety of the personal identity information they maintain. Personal information includes a consumer's name in combination with a: Social Security number; Oregon Department of Transportation issued driver license or identification card number; or a financial, credit or debit card number along with a security or access code or password that would allow someone access to a consumer's financial account.

Information security breaches can be caused by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms.

Given this context, it is clear that there is no single way of responding to an information security breach. Each incident will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved, and using that incident assessment as the basis for deciding what actions to take in the circumstances.

These are the key steps to consider when responding to a breach or suspected breach:

- Step 1: Contain the breach and do an incident assessment**
- Step 2: Evaluate the risks associated with the breach**
- Step 3: Evaluate notification requirements**
- Step 4: Prepare incident report**
- Step 5: Prevent future breaches**

Each of the steps is set out in further detail below.

General tips:

- Be sure to take each situation seriously and move immediately to contain and assess the suspected breach. Breaches that may initially seem immaterial may be significant when their full implications are assessed.
- Steps 1, 2 and 3 should be undertaken either simultaneously or in quick succession. Step 4 documents the investigation process and findings of the specific incident. Step 5 provides recommendations for longer-term solutions and prevention strategies.
- The decision on how to respond should be made on a case-by-case basis. Depending on the incident, not all steps may be necessary, or some steps may be combined.

ODOT Information Security Incident Management Plan

Section 1: Initial Reporting and Investigation of a Security Breach

There are many ways that security breaches could be reported. Some examples are as follows:

Externally

- A suspected security breach is reported to the Director's Office, Ask ODOT, or the Secretary of State Fraud Alert Program.
- The Department could learn of a potential breach through a news investigation, a contractor, or a third-party service provider.

Internally

- An employee suspects a security breach and communicates their concern to their manager.
- A member of the ODOT Computer Support Desk or DMV Help Desk discovers a potential breach while working with a customer or on a computer system.
- A Technician discovers a potential breach while working with a customer or on a computer system.
- An employee reports a potential security breach to the ODOT Information Security Unit.

Whether a suspected breach is reported by either an external source or an internal source the following protocol should be followed:

- ODOT Information Security Unit staff (ISU) or the Division Administrator or designee, using the ODOT Information Security Incident Report Form (Appendix A), will work with the reporter to collect the information needed to initiate an investigation. The Division Administrator or designee must immediately notify ISU of any reported information security incidents. ISU or the Division Administrator or designee will immediately notify the Central Services Deputy Director of the breach report.
- The Central Services Deputy Director will designate an Incident Response Commander to coordinate the activities related to the information security event.
- The Incident Response Commander, in coordination with the affected Division Administrator(s), will establish a Core Incident Response Team (CIRT). Based on the circumstances related to an information security event, the IRC may wish to select representatives from the following areas to participate as a CIRT member:
 - Human Resources
 - Financial Services
 - Communications
 - Risk Management

ODOT Information Security Incident Management Plan

- Information Security Unit
- Customer Relationship Manager of the affected Division
- ISB Technology Management
- Additional members of the affected Division
- Members from other Department Divisions
- DAS Enterprise Security Office
- Oregon Department of Consumer and Business Services

Once the CIRT has been established and all members notified, the team will:

- Conduct a preliminary investigation to determine whether a security breach has occurred; and
- Document the preliminary investigation results in an Incident Report.

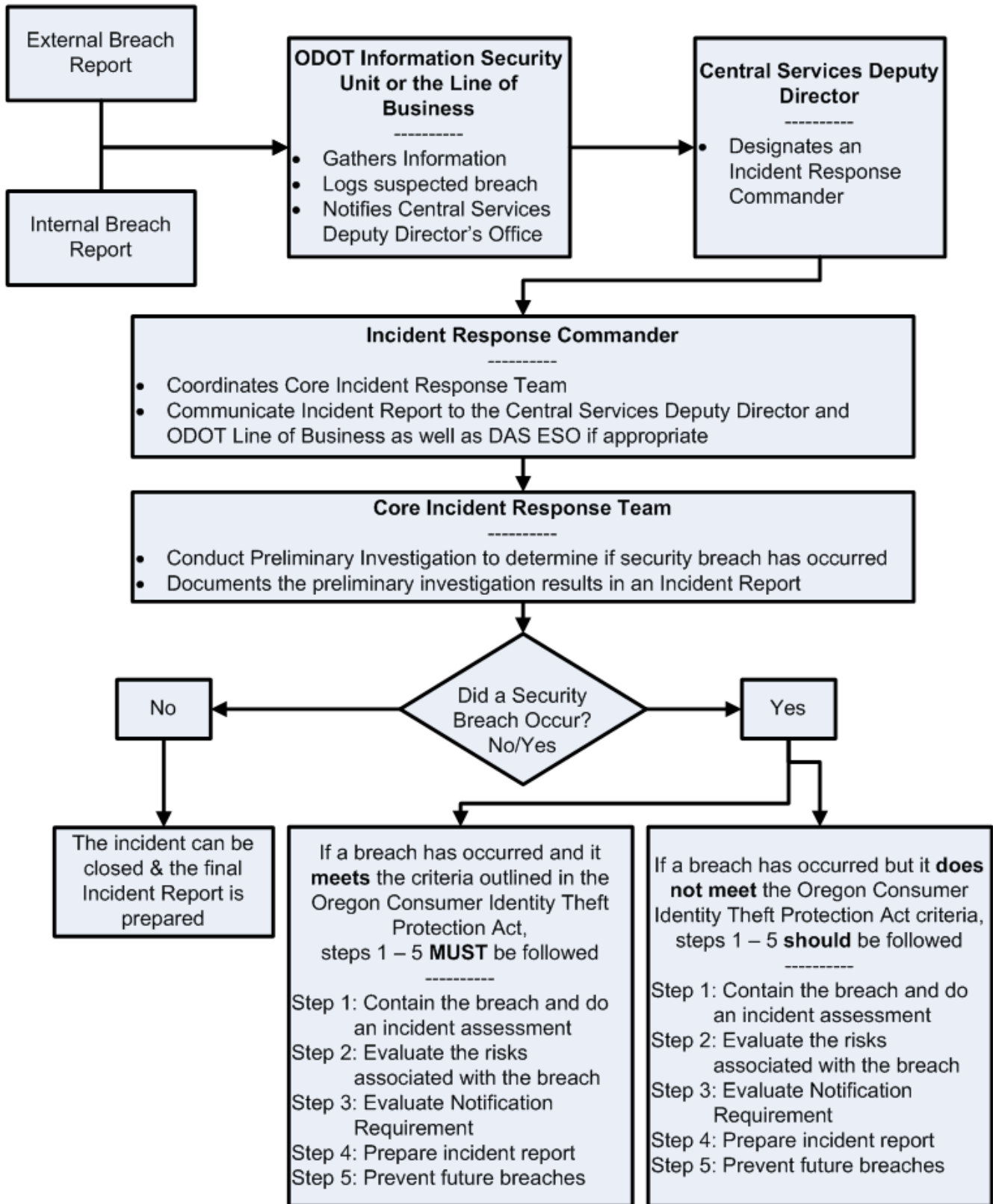
When a security breach as defined in the Oregon Consumer Identity Theft Protection Act (ORS 646A.600 to 646A.628) is confirmed, the CIRT must follow the Response Protocol for a Confirmed Security Breach (see Section 2).

When a security breach has occurred but it does not meet the criteria of the Act, the CIRT must determine which steps of the Response Protocol for a Confirmed Security Breach will be conducted to ensure the Department has responded with due diligence.

If it is determined in the preliminary investigation that no breach occurred, the incident must be closed. A final Incident Report is prepared to document the findings of the preliminary investigation. The Incident Commander will communicate the findings to the Central Services Deputy Director, the appropriate representative from the affected ODOT Division, and, when appropriate, DAS Enterprise Security Office (ESO).

ODOT Information Security Incident Management Plan

ODOT Information Security Incident Handling Flow Chart



ODOT Information Security Incident Management Plan

Section 2: Response Protocol for a Confirmed Security Breach

STEP 1: Contain the breach and do an incident assessment

The Incident Response Commander will lead the initial assessment and coordinate the activities of the Core Incident Response Team. This individual has the authority to conduct the initial investigation, gather any necessary information, document the investigation results in an Incident Report, and make initial recommendations. If necessary, a more detailed evaluation may subsequently be required.

The Incident Response Commander will:

- a) **Immediately contain the breach** by preventing unauthorized practice, recovering records, shutting down the breached system, revoking or changing computer access codes, or correcting weaknesses in physical or electronic security. Any action taken to contain the breach should also take into consideration the affect those actions may have on the ability to investigate, analyse or respond to the incident as well as the ability of the Department to take any further legal action should it become necessary.
- b) **Assemble a Core Incident Response Team** which must include representatives from appropriate parts of the Department and affected ODOT Division.
- c) **Determine who needs to be made aware of the incident**, both internally and externally, at the preliminary stage. Escalate communication internally as appropriate including informing the person(s) within the Department and the Division Administrator of the affected Division responsible for privacy compliance.
- d) **If the breach appears to involve theft or other criminal activity**, consult with the Central Services Deputy Director to coordinate the task of notifying law enforcement. Do not take action that may compromise the ability of law enforcement to investigate the breach.
- e) **Be careful not to destroy evidence** that may be valuable in determining the cause of the breach or would allow the Department to take appropriate corrective action.

STEP 2: Evaluate the risks associated with the breach

The Incident Response Commander, along with the CIRT, will determine what other steps are immediately necessary by evaluating the risks to the individual or group of individuals associated with the breach.

The following factors must be considered when assessing associated risks:

- What personal information is involved?
- What is the cause and extent of the breach?

ODOT Information Security Incident Management Plan

- Who is affected by the breach?
- What is the risk of harm that could result from the breach?

These factors are further expanded in the table provided in Appendix B.

STEP 3: Evaluate Notification Requirements

Notification is an important part of the mitigation strategy and has the potential to benefit both the Department and the individuals affected by a breach. The CIRT must determine when notification of individuals is appropriate. Each incident must be considered on a case-by-case basis to determine whether breach notification is required. The Act provides specific guidance on steps to take when there is a security breach of personal information.

(a) When to notify

In general, if an information security breach creates a real risk of serious personal or financial harm to the individual, the affected individual must be notified. Notification of individuals affected by the breach should occur within 10 calendar days following assessment and evaluation of the breach.

If the breach involves government-authorized credit cards, notify ODOT Financial Services Branch who will take appropriate steps to notify the issuing bank (example, SPOTS Card Administrator). If the breach involves an individual's bank account numbers used for direct deposit of credit card reimbursements, employee salary, or any benefit payment, the Department will notify, in addition to the individual as referenced above, the bank and any other entity that handles that particular transaction immediately.

Prompt notification provides affected individuals the opportunity to quickly mitigate personal and financial harm. When determining whether notification of individuals is appropriate, the CIRT must consider:

- Whether it is appropriate to inform anyone else, such as the law enforcement, other regulators or professional organizations, of the breach. If law enforcement authorities are involved, check with those authorities to see whether notification should be delayed to ensure that the investigation is not compromised. The timing of notification to parties other than the affected consumers must be carefully considered so that consumers are not inappropriately inconvenienced by actions of law enforcement, regulators, or professional organizations who may take actions on the consumers' behalf.
- Whether delaying the disclosure of details relating to a security breach of a security or information system may be appropriate until that system has been repaired and tested or the breach contained in some other way.
- The risk of serious personal or financial harm to the individual as determined in step 2.
- The ability of the individual to avoid or mitigate possible personal or financial harm if notified of a breach (in addition to steps taken by the Department). For example, would an individual be able to have a new bank account number issued to avoid potential financial harm resulting from a breach?

ODOT Information Security Incident Management Plan

- Any legal and contractual obligations that exist between the Department and the affected individuals.
- The consequences of failing to notify affected individuals. If individuals subsequently find out about the breach through the media for example, what could be the associated loss of trust that your agency or division sustains?

(b) How to notify

Once the CIRT has determined that notice to affected individuals is appropriate, the method of notification must be selected using the following guidelines.

Direct Notice: The preferred method of notification is direct to affected individuals either in writing (letter) or electronically (email), telephone, or in person.

Substitute (Indirect) Notice: Affected individuals are notified either by conspicuous posting of the notice or a link to the notice on your Web site, and/or notification to major state wide Oregon television and newspaper media. Substitute Notice should only occur where

- direct notification could cause further harm to the affected individuals,
- direct notification is prohibitive in cost (exceeding \$250,000),
- the number of those who need to be contacted is more than 350,000 or the contact information for affected individuals is not known.

Other Considerations:

- Preferably notification should 'stand-alone' and should not be 'bundled' with other material unrelated to the breach, as it may confuse recipients and affect the impact of the breach notification.
- Using multiple methods of notification in certain cases may be appropriate.
- You should also consider whether the method of notification might increase the risk of harm. For example, by alerting the person who stole the laptop of the value of the information on the computer if it would not otherwise be apparent.
- To avoid being confused with "phishing" emails, email notifications may require special care. For example, only communicate basic information about the breach, leaving more detailed advice to other forms of communication.

Sample notification decision scenarios are provided in Appendix C

(c) Who should notify

The CIRT must determine who is responsible for the notification to affected individuals.

Typically, the Department or a specific ODOT Division that has a direct relationship with the customer, client or employee should notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information.

ODOT Information Security Incident Management Plan

There may be circumstances where notification by a third party is more appropriate. For example, in the event of a breach of credit card information, the credit card issuer may be involved in providing the notice since the Department or third party provider may not have the necessary contact information.

(d) What should be included in the notification?

The content of notifications will vary depending on the particular breach and the method of notification chosen. In general, the information in the notice should help the individual reduce or prevent the harm that could be caused by the breach.

The Attorney General’s office has advised that the Department is prohibited from using Highway Funds to pay for credit-monitoring services for affected parties where there is no statutory requirement to do so. However, if as part of the settlement of a tort claim ODOT is required to pay for credit monitoring, then Highway Funds can be used and would be treated as an administrative expense.

Notifications should include, but are not limited to, the types of information detailed in the table below. A sample notification letter is provided as Appendix D.

Incident Description	Information about the incident and its timing in general terms.
Type of personal information involved	A description of the personal information involved in the breach. Be careful not to include personal information in the notification to avoid possible further unauthorized disclosure.
Response to the breach	A general account of what the Department or ODOT Division has done to control or reduce the harm, and proposed future steps that are planned.
Assistance offered to affected individuals	What the Department or ODOT Division will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves. Possible actions include: offering information on resources that perform credit monitoring or offer other fraud prevention tools; and, providing information on how to change a government issued identification number, personal health card or driver license number.
Other information sources	Sources of information designed to assist individuals in protecting against identity theft or interferences with privacy.
Agency/ Organization contact details	Contact information for the Department or ODOT Division that can answer questions, provide further information or address specific privacy concerns.
Whether breach notified to regulator	If applicable, indicate whether the Department or ODOT Division has notified any regulators or governing body.
How individuals can lodge a complaint	Explain that if individuals are not satisfied with the Department’s or ODOT Division’ efforts to resolve the issue, that they can file a complaint with the Oregon Department of Consumer and Business Services.

ODOT Information Security Incident Management Plan

(e) Others to Contact

The CIRT must determine whether it is appropriate to provide additional notification to third parties using the following guidelines.

Police	If theft or other crime is suspected (coordinate with Deputy Director, Central Services Division for notification of law enforcement).
Insurers or others	The State of Oregon is self-insured however other notification may be required by contractual obligations.
Credit card companies or financial institutions	If their assistance is necessary for contacting individuals or assisting with mitigating harm.
Credit reporting agencies	If the security breach affects more than 1,000 consumers, the Department must report to all nationwide credit-reporting agencies, without reasonable delay, the timing, distribution, and the content of the notice given to the affected consumers.
Professional or other regulatory bodies	When professional or regulatory standards require notification of these bodies. State of Oregon specific regulatory bodies include DOJ and the DAS Enterprise Security Office.
Other internal or external parties not already notified	<p>The Department should consider the potential impact that the breach and notification to individuals may have on third parties and take actions accordingly. For example, third parties may be affected if individuals cancel their credit cards or if financial institutions issue new cards.</p> <p>Consider:</p> <ul style="list-style-type: none">• third party contractors or other parties who may be impacted;• ODOT Divisions not previously advised of the breach, (communications and media relations, senior management); or• union or other employee representatives• managers and/or direct supervisors of affected employees

STEP 4: Prepare Incident Report

The Incident Response Commander will compile all of the information gathered during the course of the investigation into an Incident Report. This report will document the investigation process and must:

- Contain all information discovered that is relative to the handling and response by the CIRT.
- List investigation findings.

ODOT Information Security Incident Management Plan

- Document the process for determining inclusion in the notification group.
- Contain all information considered to determine the notification date.
- Include a copy of the official notification to affected individuals.
- List the names and other appropriate information of notified affected individuals (the mailing list used may be attached).

The final Incident Report is used by the Incident Commander to communicate the management of the incident to the Central Services Deputy Director, affected ODOT Division Administrator, and, when appropriate, DAS ESO.

The retention period for Information Security Breach Incident Reports is 10 years.

STEP 5: Prevent future breaches

Once the Incident Response Commander and the CIRT take the immediate steps necessary to mitigate the risks associated with the breach, the CIRT must investigate the cause of the breach and develop an appropriate prevention plan.

The prevention plan will identify action items for the Department or ODOT Division which are proportionate to the significance of the breach and whether it was a systemic breach or an isolated instance.

This prevention plan may include the following:

- a security audit of both physical and technical security;
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (for example, security, record retention and collection policies);
- a review of employee training practices; and
- a review of service delivery partners, for example internal and/or external business partners with whom information is regularly shared.

The resulting plan may include a requirement for a compliance audit at the end of the process to ensure that the prevention plan has been fully implemented.

ODOT Information Security Incident Management Plan

Appendix A

ODOT Information Security Incident Report Form

ODOT Tracking Number
(for internal use only)

If you suspect a breach or receive information suggesting a breach may have occurred, notify your supervisor immediately. Your supervisor must report the incident to ODOT Information Security Unit and the Division Administrator. Complete the attached Suspected Information Security Breach Incident Report form to collect initial details about the incident to assist in determining whether a breach has occurred and if so, the extent of the breach.

It is essential that if the information comes from an external source, that you not engage them in discussion suggesting that a breach has occurred. Their information needs to be forwarded to the ODOT Information Security Unit or the Division Administrator, who will initiate action according to the Information Security Incident Management Guidelines.

1. Date and Time of Incident:

2. Date and Time of Discovery:

3. Contact information of person reporting breach:

Name

Phone

Email

External party

ODOT Employee

Position:

Unit/Section/Office:

4. List additional employees with knowledge of incident:

5. Detailed description of incident:

6. What customer information was involved?

7. How many customers are potentially affected?

8. Additional pertinent information:

9. If breach was reported to you by a third party, provide your contact information below.

Name

Phone

Email

ODOT Information Security Incident Management Plan

Appendix B

Evaluating Risk Factors

(a) Consider what personal information is involved	
Considerations	Comments and examples
How sensitive is the information?	<p>Generally, the more sensitive the information the higher the risk of harm to individuals.</p> <p>Some personal information is more sensitive than others (for example, government-issued identifiers such as Social Security numbers, driver license numbers, and financial account numbers such as credit or debit card numbers that could be used in combination for identity theft).</p> <p>A combination of personal information is typically more sensitive than a single piece of personal information.</p> <p>However, sensitivity alone is not the only criteria in assessing the risk, as foreseeable harm to the individual is also important.</p>
What is the context of the personal information involved?	<p>For example, a list of customers on a newspaper carrier's route may not be sensitive. However, the same information about customers who have requested service interruption while on vacation may be more sensitive.</p> <p>While publicly available information such as that found in a public telephone directory may be less sensitive, this also depends on context. For example, what might be the implications of someone's name and phone number being associated with the services you offer?</p>
How can the personal information be used?	<p>Can the information be used for fraudulent or otherwise harmful purposes?</p> <p>The combination of certain types of sensitive personal information along with name, address and date of birth suggest a higher risk due to the potential for identity theft.</p>
(b) Establish the cause and extent of the breach	
Considerations	Comments and examples
Is there a risk of ongoing breaches or further exposure of the information?	What was the extent of the unauthorized access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?
Was the information lost or was it stolen?	If it was stolen, can it be determined whether the information was the target of the theft or not?

ODOT Information Security Incident Management Plan

Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?	For example, if a laptop containing adequately encrypted information is stolen, subsequently recovered and investigations show that the information was not tampered with, notification to individuals may not be necessary.
What was the source of the breach?	For example, did it involve external malicious behaviour, or was it an internal processing error?
Has the personal information been recovered?	For example, has a lost laptop been found or returned? If the information has been recovered, are there any signs that it has been tampered with?
What steps have already been taken to mitigate the harm?	How have you contained the breach? Are further steps required?
Is this a systemic problem or an isolated incident?	When checking the source of the breach, it is important to check whether any similar breaches could have occurred in the past. Sometimes, a breach can signal a deeper problem with system security.

(c) Consider who is affected by the breach

Considerations	Comments and examples
How many individuals' personal information is affected by the breach?	Remember, if this is a systemic problem, there may be more people affected than first anticipated. While numbers can help gauge the severity of the problem it is important to remember that even a breach involving the personal information of one or two people can be serious, depending on the circumstances.
Who is affected by the breach: employees, contractors, the public, clients, service providers, other agencies or organizations?	Remember that certain people may be particularly at risk of harm. For example, a security breach involving name and address of a person might not always be considered high risk. However, a breach to a women's refuge database containing name and address information may expose women who attend the refuge to a violent family member.

(d) Identify what is the risk of harm that could result from the breach

Considerations	Comments and examples
Who is the recipient of the information?	Is there any relationship between the unauthorized recipients and the affected individuals? For example, was the disclosure to an unknown party or to a party suspected of being involved in criminal activity where there is a potential risk of misuse? Or was the disclosure to a party to which the individual would object or is the subject of a restraining order. Or was the recipient a trusted, known entity or person that would reasonably be expected to return the information without disclosing or using it?

ODOT Information Security Incident Management Plan

What harm to the individuals could result from the breach?	<p>Examples include:</p> <ul style="list-style-type: none"> - threat to physical safety - identity theft - financial loss - loss of business or employment opportunities - humiliation, damage to reputation or relationships
What harm to the Department or ODOT Division could result from the breach?	<p>Examples include:</p> <ul style="list-style-type: none"> - loss of trust in the agency or division - loss of assets - financial exposure - legal proceedings

Examples of Risk and Notification Evaluation

An example of evaluating the risks and notification requirements associated with a breach.

An ODOT employee tells a manager that he viewed a document containing Social Security numbers and names on the Department's public file transfer protocol site (FTP). The manager notifies the Division Administrator and the Information Security Unit (ISU).

Following a preliminary investigation, ISU and a designee of the Division Administrator confirm that some current and previous employee information, including last names and Social Security Numbers (SSN), is contained in the document once located on the FTP site. ISU reviews access logs maintained for the FTP site and determines that no external party outside of the Department's firewall accessed the document. However, ISU is unable to determine if the document was viewed by Department employees or contractors who have access to the FTP site behind the firewall.

As a first step to contain the breach, ISU removes the document from the FTP site immediately upon notice of the potential breach and notifies the Deputy Director, Central Services Division, who, after consultation with the affected Division Administrator, names an Incident Response Commander (IRC).

With these initial steps completed, the IRC begins to evaluate the risks associated with the potential breach.

The information that was involved in the breach was a report prepared to comply with SAIF/Workers Compensation Claims and contained the last name and SSN of current and previous Department employees. While only the last name was available in association with the SSN, authorized users of the Department network could have viewed the document while it was posted on the FTP site. These same authorized users would have access to Department phone directories. Because the personal information was limited to Department employees, the IRC determined that an individual's personally identifiable information could easily be determined due to the limited number of employees with the same last name. The IRC concludes that the exposure of this information could likely result in financial harm to those current and former employees listed in the document. Based on the inability to determine if the information was accessed by current employees or contractors, the IRC chooses to notify current and former employees whose names and SSN were contained in the document of the breach. The IRC chooses to notify the current and former employees by sending a letter to each of the individuals listed in the document.

ODOT Information Security Incident Management Plan

An example of notification to affected individuals and Regulatory Body.

An employee reports to her supervising manager that a memory stick containing the employee records of 200 employees of the Department is missing. The manager immediately notifies the Division Administrator and the Information Security Unit (ISU) of the loss. ISU and the Division Administrator inform the Deputy Director of Central Services Division, who, after consultation with the affected Division Administrator, names an Incident Response Commander (IRC). The IRC's extensive searches fail to locate the whereabouts of the memory stick. The information contained in the employee records includes the names, salary information, Social Security Numbers, home addresses, phone numbers, birth dates and in some cases health information (including disability information) of current staff. Information on the memory stick is not encrypted.

Due to the sensitivity of the unencrypted information – not only the extent and variety of the information, but also the existence of health and disability information in the records – the Department decides to notify employees of the breach. It also notifies the Department of Consumer and Business Services (DCBS) of the breach and explains to DCBS what steps it is taking to resolve the situation.

A senior staff member emails affected staff to notify them of the breach. In the notification she offers staff an apology for the breach, explains what types of information were breached, notes that the DCBS has been informed of the breach, and explains what steps have been put in place to prevent this type of a breach occurring in the future. In the notification to staff, the senior staff member also provides staff with details about how they can issue a security freeze and informs staff that if they are unhappy with the steps the Department has taken they can make a complaint to the DCBS.

An example when no notification is required.

A staff member of the Department takes a Department laptop on an overnight business trip in order to work away from the office. The laptop is inadvertently left in the hotel room upon check out. At some point between leaving the hotel and arriving at home, the staff member realizes that the laptop has been left at the hotel. The staff member reports the incident to his manager the next day.

The manager immediately reports the loss of the laptop to the Division Administrator and the Information Security Unit (ISU). ISU notifies the Deputy Director of Central Services Division who appoints an Incident Response Commander (IRC).

The IRC confirms that the laptop is at the hotel, appropriately secured, and arranges for return of the laptop to the Department through a secured courier service. The IRC, after extensive investigation prior to receiving delivery of the laptop, determines that the laptop was normally used for training purposes and unlikely to have sensitive information stored on it. Upon return of the laptop, the IRC consults with the Department's Technology Management Unit. A scan is performed on the laptop and no sensitive information is discovered.

The IRC determines that no sensitive information has been breached and closes the incident.

ODOT Information Security Incident Management Plan

Appendix D

Sample Notification Letter – Security Breach

Dear :

We are contacting you because we have learned of a serious data security incident that involved some of your personal information.

[Describe what happened and what type of information was breached]

We have notified law enforcement and have advised the three major U.S. credit bureaus about this incident. We also have given them a general report, alerting them to the fact that the incident occurred. However, we have not notified them about the presence of your specific information in the data breach. Because this is a serious incident, we strongly encourage you to take preventative measures now to help prevent and detect any misuse of your information.

- As a first step, we recommend you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution.
- You also may want to consider requesting a free credit report from each of the three companies. To order your free credit report, visit www.annualcreditreport.com or call toll free 1-877-322-8228.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. A victim's personal information is sometimes held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

- To protect yourself from the possibility of identity theft, Oregon law allows you to place a security freeze on your credit files. By placing a freeze, someone who fraudulently acquires your personal identify information will not be able to use that information to open new accounts or borrow money in your name.

You will need to contact the three national credit reporting agencies (TransUnion, Equifax and Experian) in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze is no more than \$10 for each credit reporting agency for a total of \$30. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the Federal Trade Commission, there is no charge to place the freeze. For detailed procedures, go to the Oregon Department of Consumer and Business Services at www.dfcs.oregon.gov/id_theft.html and click on Security Freeze.

If you have further questions or concerns, contact us at this special telephone number: 000-000-0000. You can also check our Web site at www.ourwebsite.org for updated information.

We apologize for any distress this situation has caused you. We are ready to assist you in any way.

[Insert closing]

Your Name