

Oregon Public Employees Retirement System	Posted date November 24, 2009	Number 1.10.01.01.001.PRO
Signature <i>Paul Cleary</i>	Approval date November 13, 2009	Page 1 of 5
Policy/Procedure: Security Breach Response		
Objective:	Establishes a process to effectively handle an information security incident.	
References:	Information Security Incident Response Plan, Oregon Revised Statutes (ORS) 182.122, and ORS 646A.600	

Statement

ORS 182.122 requires agencies to develop the capacity to respond to incidents that involve the security of information. Agencies must implement forensic techniques and remedies and consider lessons learned. The statute also requires reporting incidents and plans to the enterprise security office. The Oregon Consumer Identity Theft Protection Act (ORS 646A.600) requires agencies to take specific actions in cases where personally identifiable information has been compromised.

Used with the [Information Security Incident Response Plan](#), this procedure addresses these requirements.

Responsibility	Procedure
Employee/Contractor	<ol style="list-style-type: none"> 1. Employees report events to manager; contractors report events to contract administrator. 2. When an information security event occurs, immediately complete and submit a PERS Information Security Incident form to the section manager or any executive. <ul style="list-style-type: none"> • Submit form in person (preferred method of notification). • Submit form by e-mail (least preferred method of notification) and then place a phone call to any executive. <p><i>Note: For staff at Salem office, an e-mail followed by a phone call to an executive is preferred.</i></p> <p><i>Note: Employees could receive incidents reported from third parties such as DAS/SDC, employers, members, TPAs, etc.</i></p>

Origination date: November 21, 2007

Last revision date: November 6, 2009

Last review date: November 6, 2009

SL2

Responsibility	Procedure
Manager/Contract Administrator	<p>3. Conduct a brief investigation.</p> <p>4. After receiving the PERS Information Security Incident form, immediately submit the form to the executive management team with a confirmation of the following information:</p> <ul style="list-style-type: none"> • what happened, • the date and time the incident occurred, • the type of data compromised, • where the incident took place, and • who reported or contracted PERS about the incident. <p>5. Report incident to the division executive and information security officer or backup.</p> <p>6. Submit the incident form to the information security officer in person (most preferred method of notification) or by e-mail (least preferred method of notification).</p>
Information Security Officer InSIRT	<p>7. Notify executive director and InSIRT of incident.</p> <p>The InSIRT core members consist of:</p> <ul style="list-style-type: none"> • agency information security officer (ISO), • agency chief information officer (CIO), • division administrator or designee who owns compromised data, • agency communications officer, and • agency risk manager. <p>8. Begin preliminary investigation with risk assessment.</p>

Origination date: November 21, 2007

Last revision date: November 6, 2009

Last review date: November 6, 2009

SL2

Responsibility	Procedure
Information Security Officer	9. Review preliminary investigation results with information security officer.
	10. Determine if there was a potential PII breach. If not, go to step 11 below; if so, go to step 12 below.
	11. If not a breach of PII, document incident, report to the Information Security Board (ISB) at the next scheduled meeting, and close incident. Notify division executive, InSIRT, and executive director.
Executive Director	12. Present investigation results to the executive director and division executive.
	13. Call an executive management team meeting to discuss the incident.
Executive Management Team	14. Review investigation results.
	15. Determine if there was a potential PII breach. If not, go to step 11; if so, go to step 16.
InSIRT	16. Notify InSIRT to continue the investigation.
	17. Conduct an investigation and perform a detailed review of the incident information, formulate a response plan, take corrective action, and document the incident.
	18. Develop draft materials for the announcement of a security breach to agency employees and other individuals involved.
	19. Develop draft scripting to educate agency employees about the security breach so they can provide knowledgeable assistance to the affected individuals when they contact PERS. Send a copy of the draft to the executive management team for approval.

Origination date: November 21, 2007

Last revision date: November 6, 2009

Last review date: November 6, 2009

SL2

Responsibility	Procedure
Executive Management Team	<p>20. Review and approve the content of any breach notification or communication before sending the notification to the affected individuals.</p> <p>21. If the announcement is not approved, go to step 19; if the announcement is approved, go to step 22.</p> <p>22. Implement plan of action. Report incident to DAS and law enforcement if needed.</p>
InSIRT	<p>23. Contact the business unit manager and notify him or her of any necessary action needed to respond to a security breach. Train business unit employees, set up hot topic, and provide follow up.</p>
CSD Administrator	<p>24. Set up the Customer Call Center service line to respond to the questions pertaining to the security breach.</p> <p>25. Use the existing 800 line and the current process to handle the security breach. Establish a hot topic on the Customer Call Center line to inform members of the incident. When calls come in, assign an appropriate number of Customer Service representatives to address the incoming calls.</p> <p>26. Use the Security Breach Notification letter to develop scripting and fact sheets and train staff regarding the appropriate response to calls regarding the breach.</p>
InSIRT	<p><i>Note: If possible, avoid putting a general notification regarding the breach on the PERS website as this can create a lot of phone calls.</i></p> <p>27. Conduct retrospectives or lessons learned with those who coordinated and managed the incident.</p> <p>28. Notify the executive management team of any issues that came up during the incident that need to be addressed and resolved.</p>

Origination date: November 21, 2007

Last revision date: November 6, 2009

Last review date: November 6, 2009

SL2

Responsibility	Procedure
IIM	<ol style="list-style-type: none"><li data-bbox="553 348 1398 411">29. Send all documents to Image and Information Management (IIM) for scanning into the FileNet system.<li data-bbox="553 453 1398 516">30. Update the Information Security Incident Response Plan if needed.<li data-bbox="553 558 1398 590">31. Report to ISB at the next scheduled meeting.<li data-bbox="553 621 1398 653">32. Close the security breach incident.<li data-bbox="553 684 1398 726">33. Archive security breach incident documents.

Attachments:

[PERS Security Breach Notification Letter Draft](#)

[PERS Security Breach Flow Chart](#)

[PERS Information Security Incident Form \(459-557\)](#)

Origination date: November 21, 2007

Last revision date: November 6, 2009

Last review date: November 6, 2009

SL2