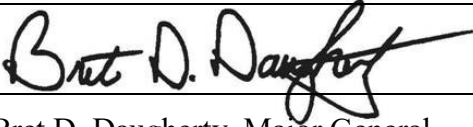




Department Policy No. SAF-609-17

Title:	Serious Incident Reporting
Former Number:	New
Authorizing Source:	RCW 43.41.370(4)
References:	Office of Risk Management Reporting Procedure
Information Contact:	Risk Manager Building #33 (253) 512-7940
Effective Date:	September 8, 2017
Mandatory Review Date:	September 8, 2021
Revised:	New
Approved By:	 Bret D. Daugherty, Major General The Adjutant General Washington Military Department Director

Purpose

This policy establishes a uniform system for reporting serious incidents within the Washington Military Department (WMD).

Scope

This policy applies to all state employees and supervisors of state employees within the WMD. It does not apply to guardsmen on state active duty or to federal personnel to include Active Guard Reserves (AGRs), traditional guardsmen in a federal military status, or military technicians.

Policy

To safeguard the health and safety of employees and to protect the interests of the WMD, incidents that meet the definitions in this policy must be fully and rapidly reported. State agencies are required to report the following incidents to the Office of Financial Management (OFM) through the Agency Risk Manager:

1. Death (WAC 296-27-031 requires employers to report worker fatalities to Labor and Industries - 1-800-4BE-SAFE - within 8 hours).
2. Significant bodily injury (WAC 296-27-031 requires employers to report a work-related employee hospitalization to Labor and Industries within 8 hours. OSHA requires employers to report an employee amputation or loss of an eye within 24 hours - 1-800-4BE-SAFE.)
3. Substantial property loss (in excess of \$100,000).
4. Substantial loss related to agency policies, procedures, or management practices, particularly where it appears there is a risk the event may recur.
5. Substantial loss related to litigation or defense practices.
6. Any breach (incident) of Information Technology (IT) Security. Refer to IT Division Policy.

Procedure for Reporting an Incident

Actor	Action
Employee	<ul style="list-style-type: none"> • Report incident as soon as possible but no later than the following work day, to supervisor, Risk Manager, and/or Chief Information Security Officer (CISO) depending on nature of incident. Refer to IT Division Policy. • Report must include information about what, when and where the incident occurred.
Supervisor	<ul style="list-style-type: none"> • Provide assistance to ensure the person or area is safe. • Stay with the person (if appropriate). • Apply interim controls if needed. • Gather information. • Conduct an internal review process.
Risk Manager and/or CISO	<ul style="list-style-type: none"> • Complete an Office of Risk Management (ORM) Loss History Incident Report Form found at: http://des.wa.gov/sites/default/files/public/documents/RiskManagement/incidentform.pdf and send to ORM along with supporting documents (if applicable). • If the person wants to file a claim against the state, direct them to the ORM Tort Claim at: http://des.wa.gov/sites/default/files/public/documents/RiskManagement/allforms.pdf. • Ensure all reports and responses are in accordance with agency policy.

<p>Department of Enterprise Services (DES) ORM</p>	<ul style="list-style-type: none"> • Receive ORM Loss History Incident Report Form. • Request additional information if needed. • Review each reported incident. • Per the ORM Incident Reporting Procedure (found at http://des.wa.gov/sites/default/files/public/documents/RiskManagement/guidelines.pdf), the Director of DES will decide if a special review team should be convened to review the incident (or incident trend) in depth. If so, a loss prevention review team (LPRT) will be assigned. • When the review is complete, the LPRT will provide a written report to the involved agency and the DES Director. The report and the agency response will be on the DES Web site at LPRT Reports. (Most reviews of reported incidents will not result in an LPRT. For these incidents, the agency is notified that a review will not take place.)
<p>Agency Director, Risk Manager and/or CIO</p>	<ul style="list-style-type: none"> • Review written report from LRPT (if applicable). • Determine appropriate mitigation or corrective action measures. • Notify manager about status of incident and if mitigation and/or corrective action is recommended. • Work with Risk Manager and/or CISO on mitigation measures. • Work with Human Resource Director on disciplinary action.

Definitions

Confidential Data Loss. The action or state of not maintaining or having control over confidential records in either paper or electronic form.

Incident. An event that may result in harm or loss and poses a risk to an agency goal, become litigious, result in external complaints;

Information Technology Security Incident. Any unplanned or suspected event that could pose a threat to the integrity or availability of confidential data or systems.

Potential Compromise of Agency Reputation. Incident or situation that could cause damage to the agency's reputation or credibility.

Significant Bodily Injury. Injury which creates a temporary loss of the function of any bodily member or organ or temporary loss of any one of the five senses.

Substantial Property Loss (in excess of \$100,000). Loss that is large in size, value, or importance.