

1. Purpose

To ensure the effective and appropriate reporting of known or suspected security incidents related to State of Alaska (SOA) information assets, system and/or services. All SOA employees have a duty to report all information security violation and problems to the State Security Office (SSO) on a timely basis.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to all SOA branches, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates the process for:

- Incident reporting.

5.1. Incident Reporting

5.1.1 Requirement to Report

Personnel must promptly report any known or suspected security incident to the SSO. The initial information to have available is listed on the incident response card found in section 5.1.2 of this policy. Personnel must create an SSO help desk ticket, an example shown in section 5.1.3 of this document, and contact the SSO at 907-269-5000. If electronics are not available, a manual report must be created; an example shown in section 5.1.4 of this document and contact the SSO at 907-269-5000.

Examples of security incidents include:

- Loss or unauthorized disclosure of confidential information;

State of Alaska

Office of Information Technology

Information Security Policies

Title: Incident Reporting



Number: ISP-152

- Serious misuse of assets (e.g., ethics violations, adult material, copyright infringement, misuse of email such as spamming or threatening, criminal activity, theft of equipment or media and unauthorized access to systems or facilities);
- Infection from a virus, worm, Trojan, botnet, spyware and adware;
- Use of a prohibited peer-to-peer network (e.g., KaZaA, Gnutella, or Limewire);
- Any direct human controlled compromise that has occurred on any device, system, network or service;
- Any other unusual or suspicious activity or event that could potentially affect the confidentiality, integrity and availability of SOA telecommunications or information technology services, systems, information or assets, including natural disasters; and
- The possible accumulation of security events that may escalate to the level of a security incident.

The SSO representative will complete an Incident Notification Report (INR) or Enterprise Service Desk System (USD) by using the appropriate template and will take the necessary steps to ensure proper notification or escalation occurs.

Serious misuse of assets must further be reported to the SSO or the Director of Personnel and Labor Relations.

5.1.2 Example of Incident Response Card

	State of Alaska Cyber Incident Reporting Procedure Call 907-269-5000	
Please have the following information available prior to your call:		
<ul style="list-style-type: none">• Agency Name• Point of Contact<ul style="list-style-type: none">• Name• Telephone/Pager/Cell• Email address• Characteristics of Incident• How the Incident was Identified• Date and Time Incident was Detected• Scope of Impact	<ul style="list-style-type: none">• Name of Incident<ul style="list-style-type: none">• Denial of Service• Malicious Code• Recon and scams• Unauthorized access• Other• What immediate assistance can the Security Office offer your agency?	

5.1.3 Example of SSC Help Desk Ticket

Security Incident Request Template (req33999)

req33999 Request Template security incident Detail - Unicenter Service Desk - Mozilla Firefox

state.ak.us https://helpdesk.state.ak.us/CAisd/html/popup_frames.html?POPUP_URLID=0&popupType=1

State of Alaska
Service Center

Logged in as: Wolf, Daniel (Log Out)

Request
Go

(Close Window)

File View Activities Actions Search Reports Window Help

req33999 Request Template security incident Detail
Edit Create Service Order Profile Browser

Affected End User	Request Area	Status	Active?
customer	Services.Security.Incident Infection	Closed	NO
Created By	Asset	Priority	Severity
Maki, Edward W		2	2
Assignee	Group	Urgency	Impact
	security.investigations		
Attached Change	Charge Back ID	Call Back Date/Time	Root Cause
Summary			Security Related
security incident			No
Description			Total Activity Time
this template is used to report security incidents. select properties tab and complete as many properties as possible. note that some properties are required. for large scale incidents (see scope property), set priority level to 1. for serious incidents, notify darrell davis by phone at 269-6733 or 244-4742. for definition of serious incidents, please see sp-004 at: http://www.state.ak.us/local/akpages/ADMIN/info/security/auth/Enterprise_Security_Policies_Final.pdf enter additional information as log comments. provide initial summary details on the security incident here:			00:19:14
Open Date/Time	Last Modified	Resolve Date/Time	Close Date/Time
08/03/2005 09:26 am	04/09/2007 03:58 pm	04/09/2007 03:58 pm	04/09/2007 03:58 pm

1. Activities2. Service Type3. Related Requests4. Knowledge5. Attachments6. Properties7. Template

Search Logs

History

Analyst	Date	Time Spent	Type	Summary

5.1.4 Example of Incident Notification Report Form

State of Alaska

Office of Information Technology

Information Security Policies

Title: Incident Reporting

Number: ISP-152



State of Alaska State Security Office

Providing Leadership in Security, Telecommunications Infrastructure and Information Technology

Incident Notification Report

Call the State Security Office (907) 269-5000


Security Event Name:

Date:

Security Event Number:

✓	Question	Response
1	Name (of reporting individual)	
	Other point of contact	
	Agency or organization	
	Phone number (primary)	
	Phone number (alternate)	
	E-mail address	
	Source & Destination IP, Port, Protocol?	
	Physical Location of the System involved?	
	Who has been notified?	
	What actions have been taken?	
✓	Question	Response
2	Date and time of event	
	Date and time event was detected	
	Impact (i.e., who/what was affected and what was the impact?)	
	Type of incident:	
	Denial of service	
	Malicious code	
	Scans or information gathering	
	Unauthorized access	
	Loss or theft	
	Destruction of assets or data	
	Other (describe to best of ability)	
✓	Question	Response
3	Attacking IP address(s) (if known)	
	Type of access gained	
	Network	
	Logged-on to device/computer	
	Use of resources	
	Access to information (if yes, type):	
	Personal/PII	
	Financial	
	Health	
	Insurance	
	Public	
	Other	

Example of Incident Notification Report (Page 2)

 State of Alaska State Security Office			
Incident Notification Report Page 2 of 2 Call the State Security Office (907) 269-5000			
✓	Question	Response	
4	Indicate Severity Level (if known)	Use Appendix C for event evaluation in to determine Level classification	
	LEVEL 1 Critical – Highest Level of Severity		
	LEVEL 2 Moderate – Medium Level of Severity		
	LEVEL 3 Minor – Lowest Level of Severity		
✓	Additional Details of the Security Event	Date	Time
5			
✓	SSO “On Call” Personnel Notification See: Appendix D and Appendix E	Date	Time
6			