

ALEISS

Alaska Law Enforcement Information Sharing System


Security Directives

02/03/2005
V. 002

Note: Current ALEISS Directives are posted on: <https://www.aleiss.org/>. ALEISS users are responsible for verifying the most current document version prior to performing tasks involving ALEISS. Please destroy printouts of outdated directives. (For reference, the ALEISS System Administrator maintains an archive of historical directives which are no longer in effect.)

TABLE OF CONTENTS

Directive 1. Governance.....	1-1
1.1. Authority	1-1
1.2. ALEISS Consortium Responsibilities	1-1
1.3. ALEISS System Administrator Responsibilities	1-2
1.4. ALEISS Officer Responsibilities	1-2
1.5. ALEISS User Responsibilities	1-3
Directive 2. Change Management.....	2-1
2.1. ALEISS Systems Documentation.....	2-1
2.2. ALEISS Software Documentation	2-1
2.3. Authorized User Documentation	2-1
2.4. Security Directives.....	2-1
2.5. ALEISS Website/Portal	2-2
Directive 3. Separation of Duties	3-1
3.1. Employee and Contractor Assignments.....	3-1
Directive 4. Physical Security	4-1
4.1. ALEISS Servers.....	4-1
4.2. ALEISS Workstations	4-1
4.3. Storage and Disposal of Printed Materials.....	4-1
Directive 5. Personnel Security Clearance	5-1
5.1. Eligibility.....	5-1
5.2. Application Process.....	5-1
5.3. Periodic Validation.....	5-2
5.4. Denial and Revocation; Appeals	5-2
Directive 6. User Identification and Authentication	6-1
6.1. User Access Codes.....	6-1
Directive 7. Authorization and Access Controls.....	7-1
7.1. "Read Only" Access Levels	7-1
Directive 8. Data Integrity	8-1
8.1. Data Sources.....	8-1
8.2. Data Transfer and Refresh.....	8-1
8.3. Data Consolidation	8-2
8.4. Data Backup	8-2
8.5. Virus Protection	8-2
Directive 9. Data Confidentiality and Classification	9-1
9.1. Confidentiality of ALEISS Information	9-1
9.2. Source Agency Restrictions on Confidential Data	9-1
Directive 10. Network Safeguards.....	10-1
10.1. Network Access.....	10-1
Directive 11. Audits and Sanctions for Noncompliance.....	11-1
11.1. Audit Schedule	11-1
11.2. Internal Audits.....	11-1
11.3. Independent Audits.....	11-1
11.4. Audit Reports.....	11-1
11.5. Sanctions for Noncompliance.....	11-2
Appendix A. Glossary.....	i
Appendix B. Revision Log	1

Directive 1. Governance			Page 1-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

Directive 1. Governance

This directive outlines the authority and responsibilities for various parties to establish, implement and enforce ALEISS policies.


1.1. Authority

- 1.1.1. ALEISS is established by the Memorandum of Understanding (MOU) signed by participating agencies in accordance with federal, state and local laws governing law enforcement information and information systems.

1.2. ALEISS Consortium Responsibilities

- 1.2.1. The head of each agency shall represent that agency as the voting member of the ALEISS Consortium or delegate this authority to an employee, in writing to the System Administrator.
- 1.2.2. By majority vote of command representatives present at a meeting during which a quorum of at least 50% exists, the ALEISS Consortium shall elect a chair and a vice chair. The term of each officer shall be twenty-four (24) consecutive months or until the next meeting after twenty-four (24) consecutive months at which new officers can be elected. Officers shall be elected from the names of those active command representatives in good standing after nominations from the floor. A representative elected to office may retain that office only so long as he remains a member in good standing. In the case of vacancy, an election will be held at the next scheduled meeting and the new officer will hold office for the remainder of the unexpired term.
- 1.2.3. The ALEISS Consortium shall approve the creation, change and rescission of security directives as needed to ensure that the system protects the confidentiality of information in compliance with state and federal laws and the provisions of the MOU.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	
Contract/Agreement:	ALEISS MOU 5. Governance
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 1-1. Governance.

Directive 1. Governance			Page 1-2
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

- 1.2.3.1. The Consortium may create, change or rescind a security directive after reviewing and approving a written draft submitted to it by the System Administrator.
- 1.2.3.2. The Consortium may not approve a directive that conflicts with state or federal law, the MOU, or another approved directive.
- 1.2.3.3. A Consortium member shall ensure that his/her agency does not adopt a local directive that conflicts with an ALEISS security directive.

- 1.2.4. The Consortium may impose sanctions against an ALEISS user or an ALEISS agency for noncompliance with a directive.

- 1.2.5. A Consortium member shall direct his/her staff and vendors to make available to the System Administrator agency information system documentation, records, and staff resources as needed for the agency to make its law enforcement records available to ALEISS.

- 1.2.6. A Consortium member shall appoint an ALEISS Officer to serve as the agency's operational and administrative contact with the System Administrator.


1.3. ALEISS System Administrator Responsibilities

- 1.3.1. Under the direction of the ALEISS Consortium, the System Administrator shall
 - 1.3.1.1. maintain control of the ALEISS program and network;
 - 1.3.1.2. maintain the security directive system;
 - 1.3.1.3. facilitate and maintain records of Consortium meetings, votes and other official actions;

- 1.3.2. Under the direction of the Consortium, the System Administrator may contract with another entity to provide these services, subject to **Directive 5. Personnel Security Clearance.**

1.4. ALEISS Officer Responsibilities

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	
Contract/Agreement:	ALEISS MOU 5. Governance
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 1-1. Governance.

Directive 1. Governance			Page 1-3
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature


1.4.1. An agency's ALEISS Officer shall serve as the liaison between the agency's users and the System Administrator for ALEISS operational and administrative matters.

1.5. ALEISS User Responsibilities

1.5.1. An ALEISS user shall comply with the MOU and ALEISS security directives. It is the user's responsibility to read and understand the current MOU and directives.

1.5.2. An ALEISS user who needs assistance to access or use ALEISS or to comply with an ALEISS directive shall contact the agency's ALEISS Officer, who may contact the System Administrator if necessary.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	
Contract/Agreement:	<i>ALEISS MOU 5. Governance</i>
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 1-1. Governance.

Directive 2. Change Management			Page 2-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

Directive 2. Change Management

This directive describes how system configuration and changes in policies and procedures are controlled to ensure appropriate documentation.

2.1. ALEISS Systems Documentation

2.1.1. The System Administrator shall develop and maintain documentation for ALEISS, including

- 2.1.1.1. a narrative description of the programs, files, and procedures used by the system;
- 2.1.1.2. system or program requests and appropriate responses;
- 2.1.1.3. program source code listings;
- 2.1.1.4. record formats showing sequence of data elements and character length of all files accessed;
- 2.1.1.5. samples of source documents, displays and reports;
- 2.1.1.6. description of backup procedures and frequency;
- 2.1.1.7. list of authorized administrators and users;
- 2.1.1.8. user access logs and periodic audit reports;
- 2.1.1.9. agency data refresh schedules;
- 2.1.1.10. any other special requirements an individual system may require.

2.2. ALEISS Software Documentation

2.2.1. ALEISS software documentation shall be maintained by the ALEISS System Administrator.

2.3. Authorized User Documentation


2.3.1. The System Administrator shall maintain a table of additions, changes, and deletions of user access codes.

2.3.2. The System Administrator shall retain information about a user access code in the table for at least three years from the date that the code was added, changed or deleted.

2.4. Security Directives

2.4.1. The System Administrator shall

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	
Contract/Agreement:	ALEISS MOU 5. Governance
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 2-5. Change Management.


Directive 2. Change Management			Page 2-2
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

- 2.4.1.1. submit to the Consortium draft proposals to create, change and rescind security directives, including proposed effective dates;
 - 2.4.1.2. notify system users in writing of the creation, change or rescission of a security directive, and make the directives available to users in an electronic format that protects the documents from being altered.
- 2.4.2. A security directive must include
- 2.4.2.1. a brief statement of purpose;
 - 2.4.2.2. after approval by the Consortium, the signature of the System Administrator and the effective date;
 - 2.4.2.3. if revised, the revision number; and
 - 2.4.2.4. citation of the state or federal law, MOU provision, standard, or other source of authority that the directive is intended to implement, clarify or make more specific.
- 2.4.3. A word or term used in a directive has the meaning commonly given in a dictionary unless a different definition is provided in *Appendix A. Glossary*.
- 2.4.4. Unless otherwise approved by the ALEISS Consortium, a directive, change, or rescission is effective five working days after it is approved by the ALEISS Consortium.
- 2.4.5. The System Administrator shall retain a rescinded or outdated version of a directive in an archive for at least ten years from the date the directive was rescinded or changed.
- 2.4.6. The System Administrator shall permanently maintain a record of changes to security directives in *Appendix B. Revision Log*.

2.5. ALEISS Website/Portal

- 2.5.1. The System Administrator shall maintain an ALEISS website, providing portals for access to ALEISS data and information about ALEISS.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	
Contract/Agreement:	ALEISS MOU 5. Governance
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 2-5. Change Management.

Directive 3. Separation of Duties			Page 3-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

Directive 3. Separation of Duties


This directive requires segregation of critical, operational functions into distinct jobs to prevent a single person from harming the system through an accidental or intentional act or omission.

3.1. Employee and Contractor Assignments

3.1.1. The System Administrator shall assign employees and administer contracts to ensure that the following critical tasks are not all assigned to a single person:

- 3.1.1.1. programming;
- 3.1.1.2. database administration;
- 3.1.1.3. system security;
- 3.1.1.4. user functions
- 3.1.1.5. source code access.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	
Contract/Agreement:	ALEISS MOU 5. Governance
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 1-4. Separation of Duties.

Directive 4. Physical Security			Page 4-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

Directive 4. Physical Security

This directive explains physical restrictions intended to prevent deliberate or accidental damage to ALEISS facilities, hardware, software, and data.

4.1. ALEISS Servers

- 4.1.1. ALEISS servers and related equipment may be placed only in an area that is restricted to law enforcement agency employees. This restriction must be enforced at all times by locked doors and windows or a receptionist/screener so that persons must prove their identity as law enforcement agency employees before entering the area.
- 4.1.2. Unattended ALEISS servers and related equipment must be stored in an area that is protected by a security/alarm system to reduce the risk of theft, fire or other damage.
- 4.1.3. A person who is not a law enforcement employee may enter a room where ALEISS servers and related equipment are placed only if the person is under constant escort by a law enforcement employee.


4.2. ALEISS Workstations

- 4.2.1. An ALEISS workstation or computer must be located so that only a law enforcement employee can view the screen or keyboard when ALEISS is in use.
- 4.2.2. An ALEISS user shall exit ALEISS before leaving an ALEISS workstation or computer unattended.

4.3. Storage and Disposal of Printed Materials


- 4.3.1. Printed ALEISS records and documentation must be stored in a locked location when not in use.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 1-2. Physical Security.

Directive 4. Physical Security			Page 4-2
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

4.3.2. When ALEISS records and documentation are no longer needed an ALEISS user shall destroy them in a manner that prevents an unauthorized person from reading them. Shredding and burning are examples of acceptable methods.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 1-2. Physical Security.

Directive 5. Personnel Security Clearance			Page 5-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

Directive 5. Personnel Security Clearance

This directive describes minimum criteria for granting user access to ALEISS.

5.1. Eligibility

5.1.1. A law enforcement agency may apply for an ALEISS security clearance for an employee who

- 5.1.1.1. is not currently under arrest or charged with a crime;
- 5.1.1.2. has not been convicted of a felony;
- 5.1.1.3. has not been convicted of a misdemeanor involving moral turpitude;
- 5.1.1.4. performs law enforcement duties, such as criminal investigations, which may be facilitated by using ALEISS, or supports and maintains the ALEISS system.

5.2. Application Process

5.2.1. An ALEISS Officer may submit an application to the System Administrator that contains:

- 5.2.1.1. the name of the employee for whom ALEISS access is requested;
- 5.2.1.2. the employee's job title and a description of the level of ALEISS access desired to assist the employee in performing law enforcement duties;
- 5.2.1.3. certification that the employee meets the qualifications described in this directive, based on the ALEISS Officer's personal review of one of the following:
 - 5.2.1.3.1. a state and national criminal history record based on fingerprint identification of the employee within the past 30 days;

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 1-3. Personnel Security Screening.

Directive 5. Personnel Security Clearance			Page 5-2
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

5.2.1.3.2. a current Alaska Public Safety Information Network (APSIN) security clearance issued to the employee under 13 AAC 68.215;

5.2.1.3.3. a current security clearance issued to the employee by the United States Department of Justice, Defense, or Homeland Security;

5.2.1.3.4. a current certificate issued to the employee by the Alaska Police Standards Council for employment as a police officer under 13 AAC 85.040 or a probation, parole or correctional officer under 13 AAC 85.22

5.2.2. The System Administrator may grant a security clearance upon receipt of a properly completed application, by sending written notice to the ALEISS Officer.

5.3. Periodic Validation

5.3.1. The System Administrator shall periodically request the ALEISS Officer to validate the eligibility of an ALEISS user to retain a security clearance, at the direction of the ALEISS Consortium.

5.3.2. The ALEISS Officer shall immediately notify the System Administrator in writing if the Officer becomes aware that an ALEISS user no longer meets the requirements for a security clearance.


5.4. Denial and Revocation; Appeals

5.4.1. The System Administrator will deny or revoke a security clearance for an person who does not meet the requirements in this directive.

5.4.2. The System Administrator may deny or revoke a security clearance based on evidence system access would pose a threat to the security of the system.

5.4.3. The System Administrator will notify the appropriate ALEISS Officer of the denial or revocation of a security clearance.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 1-3. Personnel Security Screening.

Directive 5. Personnel Security Clearance			Page 5-3
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

- 5.4.4. If the System Administrator denies or revokes a security clearance for failure to submit a properly completed application or validation, the System Administrator will notify the ALEISS Officer of what action is required to change the decision.

- 5.4.5. If the System Administrator denies or revokes a security clearance due to evidence that an employee poses or would pose a threat to system security, the System Administrator will notify the ALEISS Officer that only the agency's Consortium member has the right to appeal the decision. If the Consortium member wishes to appeal, the Consortium member and the System Administrator may present their reasons orally or in writing to the Consortium. The decision of the Consortium is final.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 1-3. Personnel Security Screening.

Directive 6. User Identification & Authentication			Page 6-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature


Directive 6. User Identification and Authentication

This directive describes how the system identifies users to reduce the risk of unauthorized access.

6.1. User Access Codes

- 6.1.1. After granting a security clearance, the System Administrator shall assign a unique user name and default complex alphanumeric password to an ALEISS user.
- 6.1.2. Upon logging on to ALEISS for the first time, the user shall change the default password to another complex alphanumeric password.
- 6.1.3. A user may not access ALEISS by using a name or password assigned to another user. A user may not give his or her password to another person, including another user, to access ALEISS.
- 6.1.4. The System Administrator may suspend a user's access code if the user does not follow correct login procedures. Upon request from the user's ALEISS Officer, the System Administrator may reset suspended access.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6.3.1. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 2-1. Identification and Authentication.

Directive 7. Authorization and Access Control			Page 7-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature


Directive 7. Authorization and Access Controls

This directive defines the levels of system access and criteria for assigning them based on user roles.

7.1. "Read Only" Access Levels

- 7.1.1. Except as provided in 7.1.2, the System Administrator shall assign Level 1, 2, or 3 "read only" access to a user, based on the user's job duties, as follows:
- 7.1.1.1. for the System Administrator only, Level 1, which allows access to all information maintained in ALEISS;
 - 7.1.1.2. for users who are peace officers, Level 2, which allows access only to unrestricted information, but includes notice of the existence of restricted information. The notice informs the user that information exists relating to the user's query but cannot be displayed and advises the user to contact the originating agency for assistance.
 - 7.1.1.3. for all other users, Level 3 allows access only to unrestricted information, and does not indicate the existence of restricted information.
- 7.1.2. Upon request by an agency, the System Administrator may grant a user an access level other than described in 7.1.1 after presenting the request to the Consortium and determining that no Consortium member objects.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6.3.1. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 2-3. Authorization and Access Control.

Directive 8. Data Integrity			Page 8-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

Directive 8. Data Integrity

This directive describes how data is protected against accidental or malicious alteration or destruction during transfer, storage and retrieval.


8.1. Data Sources

- 8.1.1. ALEISS contains a subset of records currently maintained in each member agency's record management system or database.
- 8.1.2. Each agency is responsible for creating, updating and deleting law enforcement records in its own records management system or database, according to its own policies. The agency is solely responsible for the completeness and accuracy of its source data.

8.2. Data Transfer and Refresh

- 8.2.1. After law enforcement agency enters law enforcement information into its own records management system, a subset of the data is extracted and transferred to ALEISS according to criteria approved by the agency.
- 8.2.2. An agency shall notify the System Administrator prior to changing its computer configurations or modifying its software in order to ensure that the agency maintains data refresh connectivity.
- 8.2.3. Each agency shall propose, and the System Administrator may approve, the frequency with which the agency's data will be refreshed in ALEISS. The System Administrator will not approve a refresh schedule less frequent than once per week.
- 8.2.4. The System Administrator shall publish a data refresh schedule that enables a user to determine the potential timeliness of each agency's data in ALEISS.
- 8.2.5. Modified law enforcement information or information that is removed from an agency's records management system will be updated or removed from ALEISS at the next scheduled refresh cycle.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6.3.1. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 2-3. Data Integrity.

Directive 8. Data Integrity			Page 8-2
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

8.3. Data Consolidation

8.3.1. The System Administrator will consolidate records in the ALEISS database according to the following standards:

- 8.3.1.1. Phone numbers are consolidated only if there is an exact match of all digits, including the area code.
- 8.3.1.2. Person records are consolidated only if there is an exact match of name plus FBI number, State Identification Number or Alaska Driver’s License Number.
- 8.3.1.3. Property is consolidated only if there is a match on NCIC type, model and serial number (or serial number range).
- 8.3.1.4. Vehicles are consolidated only if there is an exact match of the Vehicle Identification Number (VIN).

8.4. Data Backup


8.4.1. The System Administrator shall ensure reliability and fault tolerance of the ALEISS database by

- 8.4.1.1. storing ALEISS data in a redundant array of independent disks (RAID);
- 8.4.1.2. daily backing up the data;
- 8.4.1.3. storing the data in a secure location;
- 8.4.1.4. storing a copy of system administration records in a secure, off-site location.

8.5. Virus Protection

8.5.1. Each agency is responsible for installing and maintaining virus protection software on its own workstations that are used to access ALEISS.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6.3.1. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 2-3. Data Integrity.

Directive 9. Data Confidentiality and Classification			Page 9-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

Directive 9. Data Confidentiality and Classification

This directive describes restrictions on the use and dissemination of ALEISS data.


9.1. Confidentiality of ALEISS Information

- 9.1.1. ALEISS information is confidential and is not subject to public disclosure.
- 9.1.2. An ALEISS user who receives a request for ALEISS information may not release that information, but may refer the requester to the agency that is the source of the information.
- 9.1.3. An ALEISS user who receives a court order to release ALEISS information shall not release the information but shall immediately provide a copy of the court order to the agency that is the source of the ALEISS information (“owner agency”) and to the System Administrator. The owner agency is responsible for responding to the court order. The System Administrator shall refer the matter to the Consortium for possible action if referral to the owner agency does not satisfy the court that issued the order.

9.2. Source Agency Restrictions on Confidential Data

- 9.2.1. An agency that does not want data made available from its records management system to any ALEISS user is responsible for ensuring that the data is not included in a data transfer to ALEISS.
- 9.2.2. An agency that does not want data made available from its records management system to ALEISS users with Level 2 or Level 3 access is responsible for placing the appropriate restriction indicator on the underlying data in the agency’s internal records management system or database.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.160. Release and use of criminal justice information; fees and AS 40.25.120. Public Records; Exceptions.
Contract/Agreement:	ALEISS MOU 6.3.1. Data Access and Security Requirements; 7.1. Ownership and Release Constraints.
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 2-4. Data Classification, and 2-6. Privacy and Confidentiality.

Directive 10. Network Safeguards			Page 10-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature


Directive 10. Network Safeguards

This directive explains how public and private information is kept separate.

10.1. Network Access

- 10.1.1. An ALEISS user may access ALEISS through a secure, encrypted web-site through the user's computer.
- 10.1.2. An ALEISS workstation requires 128 bit encryption web browser software such as Internet Explorer, version 5.5 or higher. ALEISS is not fully compatible with Netscape Navigator and will not provide full functionality to a user using this web-browser.
- 10.1.3. The System Administrator shall ensure that the system prevents a user from storing and re-using a user's access codes from one session to another. Once a user logs off the system, the system shall require the user to manually re-enter the user's access codes in order to initiate a new session.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6.3.1. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 2-7. Firewalls, VPNs, and Other Network Safeguards; 3-1 Intrusion Detection Systems; 3-2. Critical Incident Response; 3-4. Disaster Recovery and Business Continuity.

Directive 14. Disaster Recovery			Page 11-1
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

Directive 11. Audits and Sanctions for Noncompliance

This directive explains how compliance is measured and sanctions imposed to ensure that ALEISS security directives are properly implemented and maintained.

11.1. Audit Schedule

- 11.1.1. The System Administrator shall develop and implement an audit schedule, to include periodic, random audits of a sample of ALEISS record queries to determine whether a query was made for a legitimate law enforcement purpose.

11.2. Internal Audits

- 11.2.1. The ALEISS Officer shall conduct administrative audits of users within the Officer's agency, as needed, to investigate suspected noncompliance with the MOU or a Security Directive, e.g., suspicion that a user has queried ALEISS for an unauthorized purpose.
- 11.2.2. The ALEISS officer shall report any findings of noncompliance to the System Administrator, including a report of any internal agency administrative action taken or under consideration as a result of the noncompliance.


11.3. Independent Audits

- 11.3.1. Any Consortium member may propose a methodology, and upon approval of that methodology by the Consortium, perform an audit of the System Administrator to determine compliance with the MOU and Security Directives.

11.4. Audit Reports

- 11.4.1. An ALEISS Officer shall report the findings of any internal agency audit involving ALEISS to the System Administrator. If the audit findings show noncompliance, the System Administrator shall forward the findings to the Consortium.
- 11.4.2. Any Consortium member that audits the System Administrator shall make a copy of the audit findings available to the other Consortium members.

AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6.3.1. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 3-4. Disaster Recovery and Business Continuity.

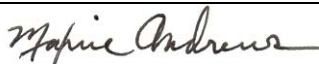
Directive 8. Data Integrity			Page 11-2
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

11.5. Sanctions for Noncompliance

11.5.1. Upon receipt of an audit report showing noncompliance with the MOU or a Security Directive, the Consortium shall take or approve any of the following actions necessary to ensure system security and deter future noncompliance:

- 11.5.1.1. Issuance of a letter of instruction;
- 11.5.1.2. Suspension or revocation of user access;
- 11.5.1.3. Suspension or revocation of ALEISS membership.


AUTHORITY/SOURCE	CITATION/DESCRIPTION
Federal Law:	
Alaska Law:	AS 12.62.150. Completeness, accuracy and security of criminal justice information.
Contract/Agreement:	ALEISS MOU 6.3.1. Data Access and Security Requirements
Policy/Standard	Global September 2003 (Draft), <i>Applying Security Practices Justice Information Sharing</i> , 2-3. Data Integrity.

Appendix A. Glossary			Appendix A. Page i
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

Appendix A. Glossary

Term	Definition
agency	ALEISS agency
agency representative	the head of an agency or an employee whom the head of the agency has designated to represent that agency in the consortium
ALEISS agency	law enforcement agency [MOU, 3. <i>Definitions</i>]
ALEISS	Alaska Law Enforcement Information Sharing System [MOU]
ALEISS Consortium	Agencies that have signed the MOU [MOU, 1. <i>Agreement...</i>]
ALEISS MOU	Memorandum of Understanding for Sharing Law Enforcement Information [MOU]
ALEISS node	Shall refer to a complete ALEISS system that will be housed at the National Law Enforcement and Corrections Technology Center - Northwest (NLECTC-NW) in Anchorage, Alaska, that receives law enforcement information from all of the AGENCIES and makes it available to authorized users. [MOU, 3. <i>Definitions</i>]
ALEISS Officer	An agency representative, appointed by the ALEISS Consortium member, to serve as a liaison between agency users and the System Administrator. [Directive 1. <i>Governance</i>]
ALEISS user	A person who is authorized to have direct access to ALEISS as a condition of employment by a law enforcement agency and who has an ALEISS security clearance.
Consortium	ALEISS Consortium
criminal intelligence data	Non verified or anonymous information or reports of criminal activity or association. [MOU, 3. <i>Definitions</i>]
data repository	Shall refer to the web servers, database servers, and backend databases maintained by the AGENCIES to facilitate the sharing of law enforcement information between the AGENCIES and other law enforcement agencies that may enter into subsequent agreements with the AGENCIES. [MOU, 3. <i>Definitions</i>]
employee	A person who performs a service for a law enforcement agency full time or part time for pay, according to a written contract.
law enforcement agency	A federal, state, or municipal agency that employs a peace officer. For the purposes of this agreement, NLECTC-NW shall be included as a Law Enforcement Agency. [MOU, 3. <i>Definitions</i>]

ALEISS Security Directives

Appendix A. Glossary			Appendix A. Page ii
03/16/2004	002		
Effective	Revision #	Rescinded	System Administrator Signature

- law enforcement information Shall include AGENCY records collected for the purpose of conducting criminal investigations and law enforcement activities. Information regarded as "criminal intelligence data" shall not be regarded as Law Enforcement Information for the purposes of this agreement and will not be included in the ALEISS data repository. [MOU, 3. *Definitions*]
- MOU ALEISS MOU
- peace officer has the meaning given in AS 11.81.900 ("a public servant vested by law with a duty to maintain public order or to make arrests, whether the duty extends to all offenses or is limited to a specific class of offenses or offenders".) [MOU, 3. *Definitions*]
- representative agency representative
- System Administrator the ALEISS Consortium facilitator, the Director of the National Law Enforcement and Corrections Technology Center, Northwest or the Director's designated employee. [MOU, 1.3. *Facilitator*]
- User ALEISS user

Appendix B. Revision Log			Appendix B. Page 2
Effective	Revision #	Rescinded	System Administrator Signature
3/16/2004	002		