DATA SECURITY and CONFIDENTIALITY HANDBOOK
for
NATIONAL MARINE FISHERIES SERVICE
ALASKA REGION

A. PURPOSE

This handbook contains the National Marine Fisheries Service Alaska Region (Region) policy for the maintenance, access, handling, and disposition of confidential data as required under NOAA Administrative Order (NAO) 216-100 titled "Protection of Confidential Fisheries Statistics." This handbook will be reviewed annually by staff from the Region for consistency with regional policy and NAO 216-100 for the maintenance and handling of confidential data. Future revisions to this handbook will be summarized in an addendum.

B. SCOPE

1. The operational responsibilities and procedures contained in this handbook apply to all administrative and statutory confidential data including Personally Identifiable Information and Business Identifiable Information. This includes information in any format (electronic, paper, etc.) from any source, that is received, stored, handled, or released by any employee in the Region or by any authorized Federal employee, state employee, grantee, or contract employee.

2. Information Technology (IT) security controls are not described in this handbook since they are covered in "NOAA Information Technology (IT) Security Policy" (NAO 212-1302) which describes the security controls that must be implemented on all NOAA IT systems. Those controls follow the National Institute of Standards and Technology (NIST) Special Publication 800-53 standards and the Department of Commerce (DOC) Information Technology Security Program Policy and Minimum Implementation Standards.

C. DEFINITIONS

1. **Personally Identifiable Information (PII)** means information about an individual maintained by an agency, including, but not limited to (1) information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, and biometric information (e.g., fingerprints); and (2) financial information (e.g., credit card numbers, bank accounts), medical history, and criminal or employment history.
2. **Business Identifiable Information (BII)** means confidential trade secrets and commercial or financial information obtained from a person. These records are protected under 5 U.S.C. 552 (b)(3) and 5 U.S.C. 552(b)(4) confidentiality provisions which protect commercial fishery statistics, data, and specifically any observer information collected for agency business processes and transactions and mandated by the Secretary of Commerce.
3. **Confidential Data** means information that is identifiable with any person and prohibited by law from being disclosed to the public. This definition is similar to "Controlled Information," as defined in the Department of Commerce Handbook of Security Regulations and Procedures (DOA 207-2). Confidential data include fisheries data such as landings and port sampling information.
4. **Aggregated or Summary Form Data** are structured so that the identity of the submitter cannot be determined either from the present release of the data or in combination with other releases. Specific criteria for aggregating information collected by the Alaska Department of Fish and Game (ADF&G) are outlined in the memorandum of understanding between NMFS and ADF&G titled "Reciprocal Data Access Agreement (1999)."
5. **Records** (as defined under 44 U.S.C. 3101) include confidential data and/or sensitive data or

information collected by the agency. The level of physical protection and security afforded to confidential data require a higher level of protection than common program or case files.

D. RESPONSIBILITIES

1. **Individual**.

Each individual having custody or control over confidential data (regardless of media format or information system in which these records or data may reside) shall provide appropriate physical protection and security from inappropriate use, access, distribution, or destruction. Appropriate measures for physical protection and security include, but are not limited to the following: locks, mandatory password requirements, and adherence to security software policy, procedures, and the NOAA disposition handbook for data under the direction of the responsible program manager or division head. All individuals handling confidential data are responsible for the following:

a. Knowing what constitutes confidential data;
b. Correctly handling and protecting confidential information as outlined in this handbook and other applicable laws;
c. Reporting unauthorized data access or data release as outlined in this handbook and according to policy outlined by NOAA Computer Incident Response Team (https://www.csp.noaa.gov/noaa/ncirt/itsecreport.html).

2. **Program Administrators and Managers**.

Supervisors and managers are responsible for (1) ensuring that persons under their supervision have read this handbook and conform to regulatory and policy requirements dealing with confidential data; and (2) determining staff access needs to confidential data and communicating those needs to the Regional Database Administrator.

3. **Regional Database Administrator** (RDBA)

The RDBA is responsible for assigning database roles and granting database privileges based on job descriptions and access needs as determined by Program Administrators and Managers.

E. PROCEDURES

1. Access. Any confidential information submitted to NMFS (including data provided to NMFS by a State agency, the International Pacific Halibut Commission, regional fishery management councils, or marine fisheries commissions), by any person in compliance with Federal data collection requirements, including cooperative research, fishery monitoring and management, and enforcement shall not be disclosed. Exceptions are allowed for disclosure under the following circumstances:

a. to Federal employees and fishery management council employees who are responsible for fishery management plan development, monitoring, and enforcement;
b. to State or Marine Fisheries Commission employees as necessary to further the Department of Commerce's mission, subject to a confidentiality agreement that prohibits public disclosure of the identity of business or a person;
c. to recipients of a grant, contract, or other financial assistance from a State, fishery management council, or Marine Fisheries Commission for the purpose of information collection or other programs if the recipient of such a grant, contract, or other financial assistance has specific signed and is authorized by an effective Confidentiality Agreement, Data Access Sharing Agreement, Memorandum of Understanding, Standard Statement of Nondisclosure, or similar agreement;
d. to State employees who are responsible for fishery enforcement if the States employing those employees have entered into a fishery enforcement agreement with NMFS and the agreement is in effect;
e. when required by court order;
f. when such information is used by Federal, State, fishery management council, or Marine

Fisheries Commission employees, and contracted employees thereof to verify catch or fishing effort under a limited access program, but only to the extent that such use is consistent with this handbook;

g. when NMFS has obtained written authorization from a person authorizing the release of their confidential information to persons for reasons not otherwise provided for in this subsection and is otherwise consistent with Federal law and state law;
h. when confidential data are required by Federal law or policy to be submitted to the Secretary of Commerce for any determination under a limited access program;
i. in support of homeland and national security activities, including the Coast Guard's homeland security missions as defined in section 888(a)(2) of the Homeland Security Act of 2002 (6 U.S.C. 468(a)(2));
j. No observer information shall be disclosed, except in accordance with the requirements of subparagraphs (a) through (i), or as authorized by a fishery management plan or regulations under the authority of the North Pacific Fishery Management Council to allow disclosure to the public of weekly summary bycatch information identified by vessel or for haul-specific bycatch information without vessel identification, or as authorized by the Magnuson Stevens Fishery Conservation and Management Act at 16 U.S.C. 1881(a)(2);

Access to confidential data shall never be granted to an office or other organization or group; access to confidential data shall only be granted to an individual that meets the criteria outlined in Section E1 a-j above. Access can only be granted to an individual if a signed and effective Confidentiality Agreement, Data Access Sharing Agreement, Memorandum of Understanding, Standard Statement of Nondisclosure, or similar agreement is in place. These signed agreements shall indicate that individuals have reviewed and understand the provisions in this manual governing the legal use of confidential data. The signed agreements are maintained by the Alaska Regional Records office. The name of each individual that has signed a statement of nondisclosure for using confidential data will be added to the Alaska Region list of authorized confidential data users.

2. Aggregation or Summarization of Confidential Data

Direct access to confidential data is prohibited except as outlined in Section E1. However, Federal law and regulations under which data are collected do permit the release of information derived from confidential data that is structured to prevent identification of individual submitters or the information submitted by them. The procedures set forth in NOA 216-100 for structuring the data are not described in detail and merely define aggregate or summary data as "data structured so that the identity of the submitter cannot be determined either from the present release of the data or in combination with other releases."

A general rule that is applied in the Alaska Region for aggregation is that any unit (e.g., fishery, fleet, or sector) for which statistical information is reported must include at least three entities (i.e., individuals, vessels, corporations, associations, or whatever form the data takes). Under the data sharing agreement between ADF&G and NMFS, fisheries data supplied by ADF&G are to be aggregated over units of at least four entities.

3. Maintenance and Safeguards

Safeguards. NMFS safeguards of confidential data include the following:

a. Physical and electronic data or documents containing confidential information must be stored in areas with no uncontrolled public access.
b. Only individuals outlined in Section E.1 may be given access to confidential data and each individual must enter into a confidentiality agreement with NMFS through a signed Confidentiality Agreement, Data Access Sharing Agreement, Memorandum of Understanding, Standard Statement of Nondisclosure, or similar agreement. The name of each individual that has

signed confidentiality agreement will be added to the Alaska Region list of authorized confidential data users.

c. Each confidentiality agreement shall continue in force for the duration of the individual's relationship with NMFS, so long as the individual requires access to confidential data. Upon termination of the relationship or when access to confidential data is no longer required, NMFS shall terminate the person's access to confidential data and require that all confidential data be destroyed or returned to NMFS. Within 30 days of the termination, the individual must provide to NMFS a signed statement that the confidential data were destroyed or returned to NMFS.

Unauthorized access or release of confidential data. All incidents involving unauthorized access to confidential data must be reported to the NOAA Computer Incident Response Team (CIRT) by calling the office at (301) 713-9111 and completing an incident report within 24 hours. The report consists of NOAA Form 47-43 (https://www.csp.noaa.gov/V3_Form/index.php). The form will be sent to the NOAA CIRT and appropriate IT Security Officer. If the incident involves PII, NOAA CIRT must be notified within *one hour* of discovering the problem. This requirement applies to incidents involving PII in electronic or physical form.
For more information about steps to follow see: https://www.csp.noaa.gov/noaa/ncirt/itsecreport.html

Shipping, Mailing, and Electronic Mail. Before shipping, mailing or emailing confidential data, a Statement of Non-Disclosure (Appendix 1) must be completed by the recipient. Confidential data, except PII, may be hand delivered or shipped or mailed by ordinary U.S. mail, Parcel Post, Air Express, United Parcel Service, Fed Ex and other conventional carriers. Couriers who are not authorized access to the material may be used if the confidential information is securely sealed in such a manner as to make undiscovered tampering unlikely. All confidential data shall be double-wrapped or double-enveloped, with the full address of the recipient on the inner and outer wrapping or envelope. The inner wrapping or envelope will be clearly marked as confidential data. These procedures also apply to interoffice delivery of confidential data. Confidential data may be sent via email, but it must be clearly marked as "Confidential Fisheries Data."

PII data may only be shipped or mailed in encrypted electronic files. An accepted encryption method must be used. PII data may not be sent via email. The following procedures must be followed when shipping or mailing PII data:

a. Export the data to a file in a secure disk location.
b. WinZip the file using 256-bit AES encryption and a strong password in a secure disk location.
c. Clearly label a CD-ROM as "Privacy Act Data" and include the date, our agency name, our phone number, and the originator's name and address.
d. Copy the encrypted Winzip file to the labeled CD-ROM, *not* a thumb drive. Use the WRITE-ONCE format.
e. Delete the unencrypted and encrypted files from the secure location and empty the computer recycle bin.
f. Have a second party check the CD-ROM on another workstation to make sure that only the encrypted WinZip file is on the CD-ROM and that the file is really encrypted.
g. Mail the CD-ROM via certified U.S. mail, UPS, FedEx or other conventional carrier that allows tracking. Mail it to a physical address, not a post office box.
h. Obtain a signed receipt from the recipient.
i. Contact the recipient by phone to communicate the strong password to them and request that they destroy the CD-ROM.
j. Record the data transfer in a log book, which will be maintained for this purpose. Retain the receipt in your files, or in a shared file area until a record of the transfer has been made in the log book.

k. In case of hand-delivery, follow the above steps to create an encrypted file and store it to CD-ROM. Hand-deliver the CD-ROM and obtain a receipt from the recipient.

Disposition/Destruction. Confidential data, including PII and BII have applicable file and/or record disposition (lifecycle of information) authorized under the NOAA File Plan Disposition Handbook (http://www.corporateservices.noaa.gov/~ames/Records_Management/disposition_handbook.html).

Destruction occurs only when disposition of the data reaches disposal stage. Disposal may occur under any appropriate means that will insure complete destruction, such as cross cut shredding or burning of physical or electronic information. Recycling documents or storage media (including computer hard drives) containing confidential data or re-writing electronic media formats is prohibited.

F. PENALTIES

1. Civil and Criminal.

Persons who disclose unauthorized confidential data are subject to civil penalties or criminal prosecution under the following laws:

a. Trade Secrets Act (18 U.S.C. 1905)
b. Privacy Act of 1972, 5 U.S.C. 552a (2000), as amended
c. Magnuson Stevens Fishery Conservation and Management Reauthorization Act (16 U.S.C. 1858), December 8, 2006
d. Marine Mamma Protection Act (16 U.S.C. 1375)
e. NOAA Directive, NOA 216-100 - Section 7 (July 1994)
f. OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information," (July 12, 2006).
g. OMB Memorandum M-06-16, “Protection of Sensitive Agency Information,” (June 23, 2006)

2. Conflict of Interest.

Employees are prohibited and shall not engage in financial transactions using nonpublic information, nor allow the improper use of nonpublic information to further his/her own private interest or that of another, whether through advice or recommendation, or by knowing unauthorized disclosure (DOC Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR 2635.703 (October 10,2002)).

3. Disciplinary Action. Persons may be subject to disciplinary action, including removal, for failure to comply with policy outlined in NOAA Directive NAO 216-100. Prohibited activities include, but are not limited to, unlawful disclosure or use of the data, and failure to comply with implementing regulations or statutory prohibitions relating to the collection, access, use, and disclosure of data covered by the NOAA Directive NAO-210-100 and this handbook.

APPENDIX 1
Statement of Non-Disclosure
For Using Confidential Fisheries Data

(CHECK THE BOX THAT APPLIES)

☐ **FEDERAL CONFIDENTIAL DATA**

I have read the NOAA Administrative order 216-100 on Protection of Confidential Fisheries Statistics and the Alaska Region's Data Security and Confidentiality Handbook and I understand the contents of both these documents.

I will not disclose any data identified as confidential to any unauthorized person(s), except as directed by the Assistant Administrator for Fisheries. I am fully aware of the civil and criminal penalties for unauthorized disclosure, misuse, or other violation of the confidentiality of such data.

I understand that I may be subject to criminal and civil penalties under provisions of Titles 5 U.S.C. 552 and 18 U.S.C. 1905, which are the primary Federal statutes prohibiting unauthorized disclosure of confidential data. I may also be subject to civil penalties for improper disclosure of data collected under the Magnuson Stevens Fishery Conservation and Management Act or the Marine Mammal Protection Act.

☐ **STATE CONFIDENTIAL DATA**

Specifically for State of Alaska confidential data, I have read the RECIPROCAL DATA ACCESS AGREEMENT and I am aware of the provisions of 18 U.S.C. 1905, 18 U.S.C. 201-209, and Alaska Statute 16.05.815.

_____	_____
Typed Name	Name of Witness
_____	_____
Signature	Signature of Witness
_____	_____
Date	Date

Affiliation:

NMFS Employee	_____
Other Federal Employee	_____
Council Member or Staff	_____
Contractor	_____
Grantee	_____