SIS Data Services' Confidential/Sensitive Data Request Procedure:

1. Acknowledge receipt of the data request within 5 business days.

2. Ask the requester to complete the SIS Data Services' Data Request Form (request.doc), with the "need to know" clearly defined. Submission of a project proposal may be substituted for the data request document.

3. Forward the request document to the Data Steward for the data. Each request for confidential/sensitive data that comes to SIS Data Services (SDS) is reviewed by the Data Steward.

4. If the request is denied, the Data Steward should notify the requester and provide the reason(s) for the denial. The requester should be informed that an appeal can be sent to the Pacific Islands Fisheries Science Center (PIFSC) Science Director.

5. If the request is approved, determine the requester's affiliation, e.g., NMFS, JIMAR, Aquatic Farms, NOAA, UH, or other.

6. If the requester is a NMFS, JIMAR, Aquatic Farms, or NOAA employee, check for the data requester's signed non-disclosure form filed with SDS. In most cases, these employees are asked to submit the signed non-disclosure form once during their employment. Each confidential/sensitive dataset that the requester receives is added to a list that is maintained by the SDS staff.

7. Ask all other requesters to submit a signed non-disclosure form for every request of confidential/sensitive data, including the access period for the data. At the end of the access period, the requester should destroy the data.

8. Include the document, "Suggestions on Handling Confidential/Sensitive Data," when sending the non-disclosure form.

9. A FAX copy of the signed non-disclosure form can serve as a proxy until the original signed non-disclosure form reaches SDS. Notify the requester when the original form is received.

10. Extract the data as fixed length or comma-delimited ASCII, depending on the requester's preference.

11. Zip and encrypt the data using WINZIP or other appropriate compression/encryption software. The password should be compliant with the Department of Commerce's Password Policy.

12. Send the password protected file by email, secure ftp site or on an electronic transfer medium (CD or DVD). The electronic transfer medium should be clearly labeled CONFIDENTIAL.

13. Provide the password directly to the requester. Avoid using email or voice mail to provide the password.