Marine Resource s Commission
Employee Sensitive Data Handling Acknowledgement

The State defines sensitive data as personal or medical information as described below:

a. Personal information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements *that relate to a resident of the Commonwealth*, when the data elements are neither encrypted nor redacted:

1) Social security number;

2) Drivers license number or state identification card number issued in lieu of a driver's license number; or

3) Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;

b. *Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted*:

1) *Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional*; or

2) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Please check each of the statements below to acknowledge that you fully understand your responsibilities for handling sensitive data as defined above, including possible penalties for improper handling of sensitive data.

[ ] I understand the definition of sensitive data as described above

[ ] I understand that sensitive data must never be electronically transmitted by email, ftp or any other means unless it has been encrypted.

[ ] I understand that I may be required to use the following sensitive data stored on a network location and I understand that I will do so only for legitimate business purposes and will never copy the sensitive information to non-network locations unless properly authorized. Signature of my supervisor on this form indicates that they agree with the business need for me to access this sensitive data:

[ ] I understand that sensitive data should not be collected and electronically stored unless absolutely necessary for business purposes and properly authorized.

[ ] I understand what is meant by network and non-network locations as it applies to Marine Resources Commission electronic file storage and I am able to distinguish where my files are stored electronically. I understand that files stored on my PC "desktop" and in my local "my documents" are non-network locations (as well as any other file stored on my C: drive).

[ ] I understand that my failure to properly handle sensitive data as described in this document, or otherwise directed by my supervisor can result in personnel action under the State Standards of Conduct. Other penalties may apply and be determined by other applicable state and federal statutes.

[ ] If I am a Marine Police Officer, I understand that if I have been assigned a STARS laptop for law enforcement purposes that I cannot store sensitive data of any type on the STARS laptop hard drive (C: drive). Furthermore, if I am not a Captain or First Sergeant, I understand that I am not authorized to put any sensitive data, particularly SSN or Driver's License number, in any electronic file anywhere (if sensitive data is needed, a MPO can keep that information in their personal physical notes or relay the information verbally to a Captain or First Sergeant or to Operations staff for inclusion in the encrypted Complaint Incident system (part of TES).

[ ] I understand that any malware event or unusual behavior of my computer should be reported immediately, and that I should make my computer available for malware scanning as soon as can be arranged with agency IT staff.

[ ] I am NOT authorized by the Commissioner to store sensitive data on a non-network location. **If not authorized please skip to end of form and sign this acknowledgement form.**

[ ] I am authorized by the Commissioner to store the following types of sensitive data on a non-network location:

[ ] I understand that all sensitive data stored on a non-network location must be encrypted.

[ ] I understand that I must only use encryption software provided by the agency.

[ ] I understand that it is my responsibility to ensure that agency IT staff have installed encryption software and it operates properly on the computer(s) that has been authorized for that purpose as specified below.

[ ] I understand how to encrypt and decrypt sensitive data files using the software I have been provided.

[ ] I understand that encryption should not be used for computer operating system or other application software files necessary for proper operation of the computer.

[ ] I understand that I must use the following encryption passphrase for all files I encrypt and if this passphrase is ever compromised I must report it to my supervisor and agency IT staff immediately.

[ ] I understand how to correctly delete sensitive data files stored on non-network devices or media (encrypt the file, then delete it; never delete an unencrypted sensitive data file that has been stored in a non-network location).

[ ] I understand that sensitive data can only be stored on external media (CD, Flash, external hard drive, etc) in an encrypted form and that such storage should only be for as short a time as absolutely necessary for business purposes and should be properly secured when not in use; I understand when the encrypted sensitive data on external portable media is no longer needed, the encrypted files will either be deleted or media will be physically destroyed or returned to the agency IT staff for physical destruction.

Identification Number(s) of computers I am authorized to store encrypted sensitive data:

By signing below, I am agreeing that I fully understand all requirements regarding proper sensitive data handling as indicated in the boxes checked above, as well as, the penalties for improper handling of sensitive data.

Employee Signature Printed Name
Date

Supervisor Signature Printed Name
Date

ISO/backup ISO Signature Printed Name
Date