Policy Number: 2007-001 **Effective Date: 2/1/2020**

Policy Title: Information Security User Policy

Purpose: To establish a MRC policy that will protect and safeguard information resources residing within the MRC environment in conjunction with COV ITRM Policy SEC500 *Information Technology Security Policy,* COV ITRM Standard SEC501 *Information Technology Security Standard,* DHRM Policy 1.75 *Use of Internet and Electronic Communication Systems, MRC Information Security Program and MRC Continuity Plan.* This Policy replaces and supercedes Policy Number 1-97, *MRC PC and LAN Policy*. Policy Number 2-97, Internet Usage Policy, is hereby rescinded (appropriate computer usage requirements are now found in DHRM Policy 1.75).

Scope: All Marine Resources Commission employees, whether classified, hourly, or contractual, have the responsibility for safeguarding information resources from unauthorized use, destruction or theft. This policy not only includes data, but also the personal computer systems, software, and hardware resources used to process the electronic information.

Definitions: "IT systems users" are MRC personnel or contractors who have been assigned job responsibilities that require the access to and use of PC resources for the purpose of creating, updating, deleting, or reading PC based information.

"PC" is defined broadly within this policy. "PC" refers to both networked, standalone, and file server workstations and the data stored on those workstations or computer media.

"Sensitive Data" is any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled. Commercial fisheries harvest data is statutorily protected sensitive data, and the State further 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.

Guiding Principles: Commonwealth of Virginia (COV) Data is:

- A critical asset that shall be protected;
- Restricted to authorized personnel for official use.

Information security must be:

- A cornerstone of maintaining public trust;
- Managed to address both business and technology requirements;
- Risk-based and cost-effective;
- Aligned with COV priorities, industry-prudent practices, and government requirements;
- Directed by policy but implemented by business owners;
- The responsibility of all users of COV IT systems and data.

Key IT Security Roles and Responsibilities: IT security roles and responsibilities are assigned to individuals, and may differ from the COV role title or working title of the individual's position. Consult your supervisor about the personnel changes related to these roles. All users should remain aware of the key security roles and responsibilities, and the system users assigned to those roles by the Agency.

- The Agency Head is responsible for the security of the Agency's IT systems and data.

- The Information Security Officer (ISO) is responsible for developing

and managing the Agency's IT security program.

- The Privacy Officer provides guidance on the requirements of state and federal Privacy laws, disclosure of and access to sensitive data, and security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

- The System Owner is the Agency manager responsible for operation and maintenance of an Agency IT system.

- The Data Owner is the Agency manager responsible for the policy and practice decisions regarding data; they evaluate and classify sensitivity of the data, define protection requirements for the data based on the sensitivity of the data and any legal or regulatory requirements, and business needs; they also communicate data protection requirements to the System Owner and define requirements for access to the data.

  Division Heads are the Data Owners of their divisional PC data and PC data application systems, and software and hardware resources. The Division Heads may further assign trustee rights to Department Managers, Technical Administrators or to the PC information users in their Division.

- The System Administrator assists Agency management in the day-to-day administration of Agency IT systems and implements security controls and other requirements of the Agency IT security program on IT systems for which the System Administrator has been assigned responsibility.

- Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners; they protect the data in their possession from unauthorized access, alteration, destruction, or usage; they establish, monitor, and operate IT systems in a manner consistent with COV IT security policies and standards; and they provide Data Owners with reports, when necessary and applicable.

- Any employee or contractor with any of the security roles listed above should also read and comply with requirements documented in the *MRC Information Security Program*.

- System users include all employees and contractors that have access to Agency PC resources; they are required to read and comply with this Policy (Policy Number 2007-001 *Information Security User Policy*) and DHRM Policy 1.75 *Use of Internet and Electronic Communication*

Systems. All system users should report breaches of IT security, actual or suspected, to their agency management and/or the ISO; and they are required to take reasonable and prudent steps to protect the security of IT systems and data to which they have access.

The Commonwealth's Information Security Program, the Commission's Information Security Program and this Information Security User Policy are based on the following nine fundamental security functions. All Commission employees and contractors must read and comply with the basic system user security requirements listed in the following sections.

Risk Management

This policy and related Commonwealth standards are based on protecting COV IT systems and data based on sensitivity and risk, including system availability needs. Accordingly, Risk Management is a central component of an Agency IT security program and allows each Agency to determine how these factors apply to its IT systems. The Commission will conduct Business Impact Analyses and Risk Assessments as necessary, but at least every three years.

- System users must report to their supervisor any activity or situation that they perceive may pose a short term or long term risk to the security of information managed and accessed by Commission systems; supervisors shall report in writing any credible risks to the Data Custodian of the affected system and the ISO.

IT Contingency Planning

IT Contingency Planning defines processes and procedures that plan for and execute recovery and restoration of IT systems and data that support essential business functions if an event occurs that renders the IT systems and data unavailable. IT Contingency Planning includes Continuity of Operations Planning, Disaster Recovery Planning, and IT System Backup and Restoration. The *MRC IT Business Impact Analysis, Risk Assessment, Contingency Management, Disaster Recovery and System Security Plan* and the *MRC Continuity Plan* document the Agency's contingency planning and disaster recovery procedures.

- System users that have been assigned a role in contingency planning must read and comply with requirements described by applicable Agency contingency plans (*MRC IT Business Impact Analysis, Risk Assessment, Contingency Management, Disaster Recovery and System Security Plan* and *MRC Continuity Plan).*

- Agency contingency plans should be protected as sensitive data and stored at a secure off-site location.

IT Systems Security

The purpose of IT systems security is to define the steps necessary to provide adequate and effective protection for Agency IT systems in the areas of IT System Hardening, IT Systems Interoperability Security, Malicious Code Protection, and IT Systems Development Life Cycle Security.

- All IT systems users must know and comply with all relevant security and usage standards.

- Use MRC PC resources for State business purposes.

- Use virus and malware protection/detection software when provided. Report to technical support personnel when anti-virus and anti-malware software is not properly functioning or not using up to date signature files.

- Prevent the use of computer games on all state owned PC resources. If current or newly purchased PC workstations have computer games installed, the user will delete or ask for assistance in deleting computer game software.

- All IT system users are prohibited from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.). The installation or use of unauthorized monitoring devices is prohibited.

- All IT system users are prohibited from knowingly propagating malicious programs including opening attachments from unknown sources.

- Any employee or contractor involved in systems development or systems installation for the Commission must read and comply with all requirements for systems development life cycle security identified in the *MRC Information Security Program*.

Logical Access Control

Logical Access Control requirements define the steps necessary to protect the confidentiality, integrity, and availability of COV IT systems and data against compromise. Logical Access Control requirements identify the measures needed to verify that all IT system users are who they say they are and that they are permitted to use the systems and data they are attempting to access. Logical Access Control defines requirements in the areas of Account Management, Password Management, and Remote Access.

- Supervisors are required to ensure that all requests to create accounts for the internal network, remote access, sensitive systems, and data applications are submitted via the

agency portal account request process. All system access shall be consistent with the concept of "least privilege".

- Commission employees and contractors are prohibited from accessing data or systems for which they have not been explicitly been granted access authorization via their assigned user ID or other written authorization.

- The use of guest and shared accounts is prohibited. Please report any existing guest or shared accounts to the Agency ISO. Shared passwords shall not be used on any IT system.

- Supervisors, in conjunction with Human Resources, shall notify the ISO in a timely manner about termination, transfer, or changes in access level requirements of IT system users.

- IT system users are required to immediately change their passwords and notify the ISO if they suspect their passwords have been compromised.

- IT system users are required to obtain formal authorization and a unique user ID and password prior to using the Agency's remote access capabilities.

- IT system users are required to prevent unauthorized use of unattended PC workstations. This would imply the use of screen saver passwords or automatic Windows workstation locking (automatic locking time should not exceed ten minutes).

- IT system users are required to keep all passwords confidential. Passwords should not be posted or displayed or stored in a manner that risks unauthorized use. In addition, passwords are not to be included in any type of script, batch login file or procedure. Passwords shall not be transmitted electronically in conjunction with username without use of industry accepted encryption standards.

- System Administrators should have both an administrative account and at least one user account and administrators are required to use their administrative accounts only when performing tasks that require administrative privileges. At least two individuals should have administrative accounts to each IT system, to provide for continuity of operations.

Data Protection

Data Protection provides security safeguards for the processing and storing of data. Data Protection includes requirements in the areas of Media Protection and Encryption.

- Protection and identification of stored sensitive data is the responsibility of the dataset creator or Data Custodian.

- Sensitive data may not be stored on mobile data storage media, local desktop or laptop computers unless properly encrypted and physically and logically secured in a reasonable manner and authorized in writing by Agency Head. The pickup, receipt, transfer, and delivery of all data storage media containing sensitive data is restricted to authorized personnel only. Sensitive data may not be transmitted without proper encryption.

  All agency personnel shall have on file with the agency ISO a signed acknowledgement of their individual responsibility and authorization for handling sensitive data.

  Data Custodians shall be responsible for submitting the names to the ISO of all personnel requiring authorization to transport sensitive data on mobile electronic storage media, or store sensitive data on local desktop or laptop computers. The ISO shall request Agency Head written authorization for all personnel transporting sensitive data on mobile storage media or storing sensitive data on local desktop or laptop computers and maintain written records of those authorizations.

- Data storage media must be sanitized prior to disposal or reuse. Either Commission personnel or authorized State Contractors, shall be used for data destruction. All data destruction shall be done in accordance with ITRM *Removal of Commonwealth Data from Electronic Media Standard* (ITRM Standard SEC514). With the exception of agency server and PC hard drives managed by VITA, any data media containing sensitive data shall be destroyed or sanitized by Agency personnel only. Data Custodians shall be responsible for requesting in writing from the ISO the destruction or sanitization of data storage media with sensitive data. The ISO or his designee shall be responsible for data destruction or sanitization, and the documentation of the data destruction.

- All personnel with access to agency owned data systems shall agree to terms of use upon initial login, and where necessary, must sign additional non-disclosure and security agreements; for VITA personnel and contractors the Agency will accept non-disclosure and security agreements signed as a condition of their employment with VITA or its contractors. The agreements shall make clear that it is Agency policy that unauthorized disclosure of any sensitive data is prohibited, and violators will be subject to disciplinary action under the State Standards of Conduct and prosecution under any applicable State and Federal laws.

- The posting of any data classified as sensitive with respect to confidentiality on a public web site, ftp server, drive share, bulletin board or any other publicly accessible medium is prohibited unless a written exception is approved by the Commissioner identifying the business case, risks, mitigating logical and physical controls, and all residual risks

- IT system users are required to regularly back up user created data files that have been stored on the PC local hard drives. If the user created data files are considered critical, the user is responsible for storing the backup copy offsite for disaster recovery purposes. Any user PC files stored on network directories will be backed up each business day by VITA contractors.

- Store magnetic media (diskettes, tapes, CD-ROM) in a secure container away from extreme temperature and sunlight.

- The auto forwarding of emails to external accounts is prohibited to prevent data leakage unless there is a documented business case disclosing residual risk approved in writing by the Commissioner.

- All system users should report breaches of IT security, actual or suspected, immediately to their agency management and/or the ISO; and they are required to take reasonable and prudent steps to protect the security of IT systems and data to which they have access. Employees or contractors handling credit card information must report any suspected breach of credit card data in the same manner.

Facilities Security

Facilities Security safeguards require planning and application of facilities security practices to provide a first line of defense for IT systems against damage, theft, unauthorized disclosure of data, loss of control over system integrity, and interruption to computer services.

- All employees should strive to maintain an office environment that employs practical, cost efficient safeguards to protect against human, natural and environmental risks to Agency information resources. Personnel are instructed to report immediately any suspicious situations or problems related to facilities such as heating, cooling, water, electrical, fire suppression, security access systems and door locks.

- Visitors to areas of the Agency that house sensitive data, particularly the First Floor Network Room, must be accompanied by Agency personnel or must have proper authorization by the ISO or VITA to be working in those areas. ISO shall maintain a log of individuals with permission to access the Network Room.

- Employees and contractors using the Commission main office suites and the small field offices of the Commission must lock office areas if departing when the office is unattended. Secure, locked vault rooms should be used to protect sensitive data as necessary.

- Employees or contractors transporting or using computer equipment in vehicles, boats or planes are expected to take normal security precautions to protect their equipment and

data from theft or loss, eg. locking vehicle, removing equipment and data from vehicle/boat when not in use.

Personnel Security

Personnel Security controls reduce risk to COV IT systems and data by specifying Access Determination and Control requirements that restrict access to these systems and data to those individuals who require such access as part of their job duties. Personnel Security also includes Security Awareness and Training requirements to provide all IT system users with appropriate understanding regarding COV IT security policies and Acceptable Use requirements for COV IT systems and data.

- All personnel and contractors shall complete Agency specific information security training at least annually. New users should complete the mandatory information security training as soon as practical after starting work for the Commission.

- Adherence to DHRM *Policy 1.75 – Use of Internet and Electronic Communication Systems* is a requirement for Agency employees and contractors; all personnel are required to have signed acknowledgement forms on file with the Human Resources Department. Note that system users have no expectation of privacy and that the Agency and the COV reserve the right (with or without cause) to monitor, access, and disclose all data created, sent, received, processed, or stored on COV systems.

- Background checks will be required of all new Business Application Department employees of the Agency at the time they are hired. Individual Agency divisions shall determine the need for background checks for personnel with user access to sensitive systems within their area of responsibility.

- It is the policy of the Commission to remove physical and logical access rights upon personnel transfer or termination. It shall be the responsibility of the Human Resources Officer to report, in writing, to the ISO all employee terminations. The ISO shall maintain a file documenting terminations and associated removal of physical and logical access rights. Agency supervisors shall report in writing transfers and requests for associated modification of user access rights.

Threat Management

Threat Management addresses protection of COV IT systems and data by preparing for and responding to IT security incidents. This component of the COV IT Security Program includes Threat Detection, Incident Handling, and IT Security Monitoring and Logging.

- All system users must report immediately to their supervisors any unauthorized disclosure of data or incidents that potentially could compromise data, eg. loss of media

or laptops with stored sensitive data. Supervisors must report such incidents immediately to the ISO.

IT Asset Management

IT Asset Management concerns protection of the components that comprise COV IT systems by managing them in a planned, organized, and secure fashion. Asset Management includes IT Asset Control, Software License Management, and Configuration Management and Change Control.

- Installation of software on Agency IT systems is prohibited until the software is approved by the Information Security Officer (ISO) or VITA. Only new media (e.g. diskettes, CD-ROM) or sanitized media may be used for making copies of software for distribution.

- All system users should understand that the unauthorized installation and duplication and/or violation of the software license agreement of copyrighted software is illegal and subject to a Group II Offense under the State Employee Standards of Conduct, "Unauthorized use or misuse of state property or records".

- Only authorized personnel in the Business Applications Department or VITA may procure or dispose of Agency hardware and software assets. Upon employee termination assets return should be coordinated with the Agency Inventory Coordinator. Return of surplus hardware and software assets should be made to the Supervisor or ISO, or when available the appropriate VITA personnel, with the appropriate property transfer documentation. All transfers of hardware and software assets must be made with the appropriate property transfer documentation and thereby coordinated with the Agency Inventory Coordinator.

- Static COV IT assets, such as desktop PCs and printers, may only be removed from Agency facilities with the written authorization of an employee's supervisor with notification to the Agency Inventory Coordinator. The Agency Inventory Coordinator shall maintain the records of those authorizations.

- Mobile COV IT assets such as laptops, mobile phones and tablets, portable printers are intended to be used regularly away from Agency premises and when assigned to an individual employee or contractor shall not require any additional authorization to be used offsite.

- Annually, the Agency Inventory Coordinator shall conduct a paper inventory audit of all IT assets, supplemented with a random physical audit to ascertain the location of all COV IT assets.

- Personal IT assets, such as laptop or desktop computers and associated peripherals, and media like personal flash drives or usb hard drives, are not allowed on State owned or leased facilities used by the Agency and cannot be attached to COV devices.

Mobile Device Management

Mobile device management concerns protection and management of COV hardware, software and data related to mobile devices like wireless phones, tablets and laptops.

- The Agency will apply commonwealth governance and security guidelines to mobile devices and data stored on mobile devices. As such, other policies and procedures described by this policy also apply to mobile devices unless indicated otherwise below.

- The Agency will maintain cost-effective mobile device plans, an inventory of mobile devices, and track usage.

- Employees should not store sensitive data on mobile devices unless authorized in writing by the Commissioner, and if so, the data must be properly encrypted. Lost, stolen or damaged devices containing sensitive data should be reported immediately to the employee's supervisor, Agency ISO and the telecommunications coordinator, and all lost, stolen or damaged devices should be reported within 72 hours.

- In general, when advised by the manufacturer, mobile device users may upgrade their COV device operating system software. Users should only install business related apps on their COV mobile phones and tablets. Users should also stay aware of any COV or Agency ISO advisories to delay software upgrades or installs to maintain compatibility with COV software.

Credit Card Information Management

- The Commission intends to process its electronic payment processes through Elavon, the Commonwealth of Virginia's contractor for electronic payment services. Commission data systems will not collect or store confidential credit card information. If through some electronic payment transactional activity, a Commission employee gains knowledge of confidential credit card information they are expected to not store the data electronically, and are required to destroy any hard copy data immediately following the transaction, unless otherwise authorized. Acceptable destruction methods include cross-cut shredding, incineration, or pulping so that cardholder data cannot be reconstructed.

- Employees or contractors handling credit card information must report any suspected breach of confidential credit card data immediately to their agency management and/or the ISO.

7/1/10 Revision: clauses added to prohibit posting of sensitive data on publicly accessible media, require clean media for software distribution, requirements for system administrator accounts, shared passwords shall not be used on any IT system, no auto-forwarding of emails to external accounts, and no monitoring devices allowed.
6/1/11 Revision: removed requirement for background checks every two years for Agency IT personnel.
10/5/15 Revision: minor procedural changes primarily related to use of agency portal for electronic account requests.
10/1/18 Revision: minor procedural changes primarily related to use of mobile devices, updating of sensitive data definition, and reporting of possible credit card data breach.
2/1/2020 User Policy reviewed, minor editorial changes added, policy approved by Agency Head and made effective 2/1/2020.