



VIRGINIA MARINE RESOURCES COMMISSION

External User System Access Request Form

Instructions: Please include all signatures on page 1 of this form and use system acronyms listed at bottom of page to describe needed systems. If system requested is sensitive, Page 4, Statement of Non-Disclosure must also be signed. Return signed form(s) to Linda Farris, 2600 Washington Avenue, Newport News, Virginia, 23607; fax# 757-247-2020; Linda.Farris@mrc.virginia.gov; 757-247-2280 (phone).

EXTERNAL USER INFORMATION			
External User Name:	MRC Sponsor:		
Company:	Address:		
Phone:	Email:		
MRC ID:	Vessel Name and USCG Document Number or State Registration Number:		
Agency Network	Add Access	Change Access	Delete Access
Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Remote Access (Citrix/VPN)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Non-Sensitive Systems			
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive Systems			
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other Systems (Please fill in the name of additional systems you are requesting access for or already have access to that are not listed above)			
System:			
VERIFICATION OF SYSTEM ACCESS REVIEW			
By signing this form, you confirm that you have discussed your system access in detail with MRC staff and have read and agree to abide by the PC safeguards outlined on Page 2 of this document.			
External User Signature	Date		
Data Custodian Signature	Date		
System Owner Signature	Date		

Non-Sensitive Systems	
Charter Boat Online Reporting (CBOR)	Gamefish Tagging Online System (GFTOS)
Habitat Management Permit Tracking System (HMPTS)	Outstanding Angler Awards Online System (OAAOS)
Oyster Ground Billing & Leasing System (OGLS)	Time & Effort System (TES)
Biological Sampling Program (BSP)	
Sensitive Systems	
Commercial Fishing License System (CFLS)	Fisheries Statistics Systems (FSS)
Fisheries Tracking System (FTS)	Summons Management System (SMS)



VIRGINIA MARINE RESOURCES COMMISSION

External User System Access Request Form

PC Safeguards to protect both your personal data and MRC data

Computers and the Internet have become an important part of our daily life, enabling a wide range of services to home users such as communicating with friends and family, shopping, paying bills, storing personal photos and music. This convenience and inter-connectivity does not come without risk however. Potential threats include viruses that could erase your entire system or hackers stealing your credit card information.

By understanding the risks and combining some common sense rules with a little bit of technology, home users can safeguard their data from these threats and understand the needs for security controls at work. The following tips will help protect your data.

BACK UP YOUR DATA

Your hard drive may crash or you may find that an infection has affected your computer so much that the operating system and applications need to be reinstalled. In cases like this it is best to have your important data backed up so you can restore your system without fear of losing your data. Below are some important steps you can follow:

- Use your computer's backup tools. Most operating systems provide backup software designed to make the process easier. External hard drives and online backup services are two popular vehicles for backing up files.
- Back up data at regular intervals. Weekly backups are recommended.
- Verify the data has been backed up. Backup media needs to be reviewed periodically to determine if all of the data has been backed up accurately.
- Verify the ability to restore. It is a best practice to periodically test that your backup data can be restored if loss occurs.

USE STRONG PASSWORDS

Passwords help protect your data. It is important to have a strong password for your computer, mobile device, and any other media used to store important and/or sensitive data. A strong password is at least eight characters that use a mix of upper case, lower case, and numeric or special characters. Each device should have its own strong password so that if one is compromised your others will stay secure.

BE SAFE ONLINE

Below are a few helpful tips on how to keep safe on the Internet:

- Keep your operating system updated/patched. Set it to "auto update."
- Use anti-virus and anti-spyware software and keep them updated.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Secure your transactions. Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the communication with the Web page is encrypted.
- Keep your applications (programs) updated and patched, particularly if they work with your browser to run multi-media programs used for viewing videos. Set these programs to "auto update."
- Block pop-up windows, some of which may be malicious and hide attacks. This may prevent malicious software from being downloaded to your computer.



VIRGINIA MARINE RESOURCES COMMISSION

External User System Access Request Form

ENCRYPTION

Encryption is a process whereby the data is scrambled and can only be read by someone with the "encryption key" to unscramble the data. Users should consider encrypting sensitive information. Some new operating systems include tools to encrypt data while others require the installation of encryption software.

Important Note: Your authorization to use a MRC sensitive data systems such as CFLS or FSS may enable you to view sensitive or confidential data. With the exception of your personal data, such data may be only viewed via the MRC data application and may not be extracted or stored on your hard drive without permission of the MRC staff that serves as data custodian for the data. If such permission is granted encryption must be used to protect the confidentiality of the sensitive data.

DISPOSE OF INFORMATION PROPERLY

It is important to properly handle data erasure and disposal of electronic media (e.g. PCs, CDs, thumb drives) in order to protect confidential and sensitive data from accidental disclosure. Become familiar with the proper methods of sanitizing, destroying, or disposing of media containing sensitive information.

Before discarding your computer or portable storage devices, you need to be sure that data has been erased or "wiped." Below are a few tips to assist in disposing your data:

- Read/writable media (including your hard drive) should be "wiped" using Commonwealth of Virginia Information Security Standard (SEC514) compliant software. Software that meets compliance standards can be downloaded from the Internet <http://www.vita.virginia.gov/library/default.aspx?id=5046> at no cost.
- Shred CDs and DVDs. This type of media should be physically destroyed.
- Media that does not have a need to be re-used or contains sensitive or private data that cannot be "wiped" should be physically destroyed.

FOR MORE INFORMATION:

- US-CERT Tips for Safeguarding Your Data:
<http://www.us-cert.gov/cas/tips/ST06-008.html>
- MS-ISAC Guidelines for Backing Up Information:
<http://www.msisac.org/awareness/>
- MS-ISAC Newsletter – Backing Up Your Files:
<http://www.msisac.org/awareness/news/2010-02.cfm>
- MS-ISAC Newsletter – Using Encryption to Protect Data:
<http://www.msisac.org/awareness/news/2008-05.cfm>
- MS-ISAC Newsletter – Erasing Information and Disposal of Media:
<http://www.msisac.org/awareness/news/2006-08.cfm/>

Important Note: as indicated above computer virus or malware infections are commonplace. Please keep your anti-virus software up to date and learn to recognize the symptoms of an infected PC such as slower performance than normal, freezeups, unsolicited popup windows. Unfortunately MRC staff can not commit to helping our external users with malware problems, but if you have a problem you can contact Linda Farris at 757-247-2280 or Linda.Farris@marc.virginia.gov for help on how to approach a malware problem.



VIRGINIA MARINE RESOURCES COMMISSION

External User System Access Request Form

Sensitive Systems Individual Statement of Non-Disclosure

This is to certify that:

1. I am a non-MRC employee working with the Marine Resources Commission; it has been determined to be acceptable by an Agency Data Custodian to allow my access to the following state computer systems and/or VMRC data files that may contain information declared to be sensitive and are to be held confidential by the VMRC and all authorized users:

2. In using VMRC computers, data systems, and data I agree to uphold the state's security safeguards outlined on Page 2 of this document to preserve the safety and integrity of the systems accessed and protecting against misuse or destruction of the computer systems and data being accessed.

3. If I require access to the Commercial Fishing Licensing System, the Fisheries Statistics System, or Fisherman Tracking System, I have read Section 28.2-204 of the "Laws of Virginia Relating to the Marine Resources of the Commonwealth," on Page 5 of this document which pertains to the collection and confidentiality of fisheries data.

4. I am fully aware of the civil and criminal penalties for unauthorized disclosure, misuse or other violation of the confidentiality of such data.

5. I will not knowingly disclose any data, statistics, or files identified as confidential under this agreement to any person or persons, except as authorized by the VMRC Data Supervisor, or the Supervisor's designee, in accordance with the law, as authorized by the Commonwealth of Virginia Attorney General.

External User Signature	Date
Data Custodian Signature	Date
System Owner Signature	Date



VIRGINIA MARINE RESOURCES COMMISSION

External User System Access Request Form

Virginia Code: 28.2-204. Authority to collect fisheries statistics –

A. The Commission may collect from any source any fisheries data and information necessary to develop fishery management plans and to evaluate management options.

This information shall include, but not be limited to:

1. Statistics for catch and fishing efforts by species from commercial and recreational fishermen;
2. Statistics from fish processors and dealers;
3. Types of gear and equipment used;
4. Areas in which fishing has been conducted;
5. Landing places; and
6. The estimated capacity of fish processing facilities and the actual amount of fish processed at these facilities.

B. The Commission may enter into cooperative agreements with any other entity for the collection of statistics.

C. The information collected or reported shall not be disclosed in any manner, which would permit identification of any person, firm, corporation or vessel, except when required by court order. The Commission may prescribe the form and manner in which this information is reported (1986, c.273, 28.1-23.2; 1992, c.836)