iet Information & Educational Technologies

VIRGINIA WESTERN
WE'LL TAKE YOU THERE

Dual Enrollment Security Access Request Form

First Name:		Middle Initial:		Last Name:	
Date:				Department:	Dual Enrollment
Title/Position:	Dual Enrollment Faculty			Location:	Off Campus
Empl ID:				Phone:	
School:				Business E-mail:	
SIS (Student Information System): □Faculty Access: Print Class Rosters, Enter Grades, etc.					

I agree to comply with the attached Virginia Western Community College's Security Awareness Tips.			
Employee's Signature:		Date:	
VWCC Authorizing Signature:		Date:	

SIS Data Owner's Signature:		Date:	

VP of Academic and Student Affairs Use Only

SIS Set to active by:		Date:	

Information and Educational Technologies (IET) Use Only

Copyid:	AAS	**WWEB / Instructor**	Date:	
SIS Processed by:	AAS		Date:	
SARF Database Updated:	HD		Date:	
System Owner's Signature: Dir. of IET			Date:	

Security Awareness Tips

2021

10 Basic Tips for Security Awareness

For questions, please contact the VWCC Help Desk at 540-857-7354 or helpdesk@virginiawestern.edu

1. Never respond to email or telephone requests for passwords, account numbers, or any confidential or sensitive information no matter who makes the request.
2. Never leave your computer logged on unattended, even for a minute. Remember, you are responsible for any activity performed under your assigned user id. Always take care to log off from each application when the work is completed or when you are leaving your work area for an extended period of time. It is highly recommended that you power off the desktop at the end of your business day.
3. Create a strong password. A non-word with one or more numbers inserted in the middle (not on the ends) is the best choice. To make a memorable and secure password use the letters from a phrase/song, add digits, and use upper and lower case letters (ex. I Love Paris In The Spring – IL2piTS4).
4. Do not give your password to anyone for any reason or type your password when someone is watching. Don't write down your password, include it in automated scripts, store it on your hard drive/PDA, and don't ask the system to remember your id and password. Employees should never log on with their user id/password and then permit another user to have access to the device.
5. Never send confidential or personal information (e.g., password, credit card or account information, social security number, driver's license number, etc.) through the network. E-mail, chat, instant messaging, are all equally unsafe. Do not download files from an unknown source or **open emails or attachments from unknown sources.**
6. Sensitive or personal information should be encrypted if saved on any portable device or sent via e-mail. This prevents unauthorized people from viewing the information.
7. To protect your computer against viruses and other security exploits, install and routinely run anti-virus software. Update your anti-virus software regularly to ensure new virus signatures will be detected.
8. Never make or use on any notebook or desktop computers illegal or unlicensed copies of software, manuals, images, music, video, etc.
9. Dispose of personal or confidential information in a secure manner (e.g., shred, wipe, incinerate).
10. Maintain the confidentiality of all data, keeping in mind the privacy of all individuals and laws that apply to it.

(Provided courtesy of VCCS System Office and serves as Annual Security Awareness Training for Dual Enrollment faculty)

Last Updated: 02/10/2021