Virginia Western Community College

ONLY YOU CAN REPORT INFORMATION SECURITY INCIDENTS

How to report a VWCC information security incident:

- Contact a member of the VWCC IT team and inform your immediate supervisor about the incident.
- All incidents should be reported only through channels that have not been compromised.
- If you suspect reporting methods are compromised, verbal or face-to-face reporting should be used.

helpdesk@virginiawestern.edu
540-857-7354
Business Science M273

What is an Information Security Incident?

An information security incident is any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information. This includes interference with information technology operation and violation of VCCS policy, laws or regulations.

Examples of information security incidents include but are not limited to:

- Computer system breach
- Unauthorized access to, or use of, systems, software, or data
- Unauthorized changes to systems, software, or data
- Potential unauthorized disclosure of sensitive information, such as PII (Personally Identifiable Information} or FERPA protected student data
- Loss or theft of equipment storing institutional data
- Denial of service attack
- Interference with the intended use of IT resources
- Compromised user accounts
- Inappropriate use of computers and the System Office network

It is important that actual or suspected information security incidents are reported **as early as possible** so that VWCC can limit the damage and cost of recovery. Include specific details regarding the system breach, vulnerability, or compromise of your computer and we will respond with a plan for further containment and mitigation.

All users of VWCC information technology resources are responsible for being vigilant for unusual system behavior which may indicate a security incident in progress and for reporting computer incidents to include:

- Noting all important details (e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behavior, etc.) immediately and recording details of any suspicious activities.
- Not carrying out any own action, but immediately reporting the event as noted below.
- Do not turn off your computer but disconnect it from the network (including wireless networks) if you suspect it might have been compromised.