Southwest Virginia Community College
Standard Operating Procedure

Information Security Incident Management

16.1 Incident Response Plan

Version: 1.2
Status: Reviewed June 2024
Contact: Brenda Bowling, Information Security Officer, bbowling@vccs.edu

The purpose of the Incident Response Plan (IRP) is to provide technical and managerial guidance to enable a quick and efficient recovery from security incidents, perform the necessary steps to correctly handle an incident, prevent or minimize disruption of mission critical services, and minimize loss or destruction of confidential or sensitive information. Southwest Virginia Community College (SWCC) will also use the information gained during incident handling to better prepare for future incidents and provide for stronger protection for systems and data.

See also:

Appendix A - Security Event Prioritization Criteria

Appendix B – Information Security Incident Response Team (ISIRT) Contact Information

Appendix C – Additional Resources Contact Information

Attachment: Information Security Incident Reporting Form

Response Checklist & Communication Plan

Incident Response Steps	Responsibility

1)	**Report all suspicious events** involving information assets to the SWCC Help Desk, a Supervisor, or use automated reporting features (Outlook – Report Message)	All persons
2)	**Characterize the nature of the information security event** (See Appendix A) a. **High Priority** – Sensitive data loss involving student records or SSN, active threat to technology assets or infrastructure (Ransomware, computer virus), monetary loss via computer fraud in excess of $5,000. b. **Medium Priority** – Sensitive data loss involving PII (not including SSN), stolen laptop or other technology assets, monetary loss via computer fraud of less than $5,000, **c. Low Priority** – Phishing email, non-sensitive data loss	ISO, ISO point of contact, CIO
3)	**Report High and Medium Priority events** to the Chief Information Security Officer (CISO)	Information Security Officer (ISO)
4)	**Report Low Priority events** to the Application System Security Administrator. Low priority events are handled administratively by the Data Owner and the Application Security Administrator	ISO, ISO point of contact, CIO
5)	**Assess the High and Medium priority event and determine severity** a. Any event involving the actual loss of sensitive data or property must be classified as an Information Security Incident and prioritized as Medium or High Priority Incidents	ISO CISO
6)	**Secure information assets** to prevent further loss and to preserve evidence for investigation by appropriate authorities. Review plans with appropriate ISO(s) to mitigate risks and future occurrences	SWCC IT, ISO, ISO point of contact, CIO
7)	**Notify appropriate members of the Information Security Incident Response Team** (ISIRT) See Appendix B for Team Members	ISO
8)	**Document the Incident using the Incident Reporting Form**	ISO
9)	**Notify the SO Chief Information Officer** (CIO) of all High level events determined to be Security Incidents as well as any events which require public reporting. Further brief CIO on progress to mitigate current and future risks	CISO
10)	**Notify the VCCS Legal Counsel** of all Security Incidents involving the theft of sensitive data	CISO
11)	**Notify the State Police** of all Security Incidents involving the reported theft of sensitive data, COV property, or monetary losses	CIO SWCC Police
12)	**Notify the Chancellor** of all High level Security Incidents or incidents requiring public notice or reporting	CIO/CISO

13)	**Notify and Work With Impacted Individuals** who are affected by any compromise of sensitive data	VCCS Legal Counsel through VCCS Cyber Insurance Carrier

Reporting Information Security Events

The beginning of an Information Security Incident response warrants consideration of these actions:

- Preservation of evidence (ISO, SWCC IT Department, Data Owner, Application Technical Owner)
- Assessment (ISO)
- Containment and recovery actions (Application Technical Owner, System Admins)
- Damage determination (Data Custodian, System Admins, Data Owner)

Initial actions will be taken to determine the nature and severity of the information security event upon initial reporting to the Help Desk, ISO or ISO Point of Contact. Low priority events occur commonly and are normally mitigated without full involvement of the Information Security Incident Response Team (ISIRT). Individuals as designated in the elements of responsibility detailed in the Employee Work Profile are responsible for investigation and mitigation of low priority events. The Data Owner will normally handle events of this type in cooperation with the reporting individual and the Application Security Administrator.

If the incident type passes beyond the criteria for a low priority event, mitigation actions begin at the next level. At this point the Information Security Officer (ISO), delegate, or other appropriate representative of the ISIRT is notified of the event and briefed of the specific nature of the event as it is known. As the investigation begins, forensic preservation, logging and other actions are taken by the appropriate technical team members should the incident scope expand to the next level. If mitigation is successful and no data breach is suspected, the ISO, delegate, or other appropriate representative of the ISIRT will conclude the investigation and recommend remediation actions to prevent further occurrence.

If the scope expands to a medium or high priority event, the ISO, delegate, or other appropriate representative of the ISIRT will convene the ISIRT and begin operations necessary to address the event as an Information Security Incident. The ISO will manage the ensuing investigation. The operational aspects of the investigation and breach notifications will expand and contract with the incident scope. Appropriate notifications to authorities and other government entities with jurisdiction must be made. All suspected criminal activities are investigated by the Virginia State Police and they must be notified at the earliest opportunity once the initial facts of the incident are established.

The ISO will call on any necessary additional offices and System Office Information Technology Services (ITS) resources if needed to assist with carrying out the investigation and remediation of any breach. This expanded ISIRT will be responsible for the investigation of the incident and any technical support required. Incident team members will include representatives of affected data owners, any other units responsible for the devices or data involved, and any associated information technology or investigative resources. These additional personnel are identified in

the Information Technology Systems Inventory for each information system and include the Data Owner, Technical Owner, and System Administrators.

Forensics preservation will be elevated. The Cybersecurity Response Team and outside resources will be notified and assistance will be requested as needed to mitigate the incident and assess the possibility of data breach as well as other actions needed to address the nature of the incident.

The Information Security Incident Response Team (ISIRT) will provide an overview of the investigation and technical support associated with information security incidents and/or a suspected or actual breach of protected electronic data.

Incident Conclusion

Upon the conclusion of an Information Security Incident, the ISO, delegate, or other appropriate representative of the ISIRT will make an assessment and determine actions necessary to conclude the incident. These actions include but are not limited to:

- Report documentation
- Lessons learned
- Identification of corrective actions required by the organization's security programs
- Briefings for SWCC President and Executive Management as required

Information Security Incident Response Team (ISIRT) Composition

The SWCC ISIRT is established to provide the expertise and judgment for the discovery, response, and reporting of information security incidents. Various members may be needed based on the type of incident including:

- The Primary and Point of Contact Information Security Officers (ISO).
- The SWCC President, Executive Management and CIO who will make administrative decisions.
- Human Resources personnel who are authorized to assist in disciplinary or employee relations.
- Facilities manager who may be needed to access physical office locations during an incident (i.e., to obtain a workstation from a locked office).
- Emergency Preparedness & Safety Manager (Business Continuity Planning or Continuity of Operations Planning personnel) who may need to be aware of incidents that may require a review of risk assessments and continuity of operations plans.
- Public Relations personnel who are authorized to speak on behalf of the institution

System Office Resources:

- Management – ITS Managers, Enterprise System Owners, Chancellor's Cabinet
- System Engineers – ITS Operations staff
- System Administrators – ITS Application Development and Support staff
- Legal Counsel

State Legal Resources:

- Office of the Attorney General – All communications with the Office of the Attorney General will be managed by VCCS Legal Counsel.

This is not an all-inclusive list and different incidents may require different personnel. The ISIRT will remain active until the incident is closed.

Southwest Virginia Community College Employee Roles and Responsibilities

- All users of SWCC information technology resources are responsible for being vigilant for unusual system behavior which may indicate a security incident in progress and for reporting information security 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.
    - Not carrying out any own action, but immediately reporting to The SWCC Help Desk, the ISO or the ISO Point of Contact.

- Supervisors should ensure their employees are aware of reporting procedures and that employees complete security awareness and training appropriate to their EWP core duties.

- System administrators who are familiar with SWCC systems are responsible for reporting information security incidents. They may also be called upon to determine and implement a solution during an incident.

- Employees, contractors and third party users will not attempt to prove suspected security weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

Employees may be subject to Southwest Virginia Community College or Department of Human Resource Management (DHRM) disciplinary processes for failure to follow proper incident response procedures.

Confidentiality of IT Security Incident Reports

SWCC employees and ISIRT members will maintain the confidentiality of all IT security incidents.

Incident Reporting Forms

Southwest Virginia Community College will use the appropriate Incident Reporting Form when documenting and reporting incidents.

VCCS Reporting Information for IT Security Incidents

Colleges, the SSC and the System Office must report medium or high incidents to the VCCS Information Technology Services Office to comply with the Level II delegation. Specifically,

they should be reported to the Chief Information Security Officer, or in their absence, any other member of the Security, Risk and Compliance Office. The SWCC, colleges and the System Office must report these incidents via TeamDynamix (Issue Type: Network – Abuse) or Abuse@vccs.edu. At a minimum, the information below is required when reporting an incident:

- Date and time of the incident
- Incident description
- Impact of the Incident
- Severity of the attack (high, medium)
- Steps taken to respond to the attack
- Names of others who have been notified

Colleges, the SSC and the System Office must complete an *Incident Reporting Form* and include it as an attachment to the TeamDynamix ticket or Abuse@vccs.edu email. All incidents should be reported only through channels that have not been compromised. If either of the above reporting methods are compromised, verbal or face-to-face reporting may be used.

Appendix A

Security Event Classifications

When more than one condition applies, the most severe event determines the priority level for response.

Event Description	Severity	Priority	Public Reporting Requirement
Denial of Service – Distributed attack on Network	Loss of Network Services	High	No
Denial of Service – Distributed attack on Application Service	Loss of Network Services	High	No
Denial of Service – Single attack on Network	Loss of Network Services	High	No
Denial of Service – Single attack on Application Service	Loss of Single Application Services	Medium	No
Network Intrusion – Multiple Nodes	Any	High	No
Network Intrusion – Single Node	Depends on sensitivity of the accessed node	Medium	No
Sensitive Data Loss – Student Records	> 100 Records	High	Yes
Sensitive Data Loss – Student Records	< 100 Records	Medium	Yes
Sensitive Data Loss – PII including Social Security Numbers	Any quantity	High	Yes
Sensitive Data Loss – PII	> 100 Records	High	Yes
Sensitive Data Loss – PII	< 100 Records	Medium	Yes
Sensitive Data Loss – Financial data including	Any quantity	High	Yes

Social Security Numbers			
Sensitive Data Loss – Financial data	> 100 Records	High	No
Sensitive Data Loss – Financial data	< 100 Records	Medium	No
Theft of Equipment (Computers, Laptops, Mobile devices)	> $5,000 value	High	No
Theft of Equipment (Computers, Laptops, Mobile devices)	< $5,000 value	Medium	No
Theft of Payroll or other cash equivalent	> $5,000 value	High	No
Theft of Payroll or other cash equivalent	< $5,000 value	Medium	No
Ransomware Infection, Malware	Infection of 1 or more systems	High	No

Appendix B

Information Security Incident Response Team (ISIRT) Contact Information		
Role	**Name**	**Contact Information**
Information Security Officer	Primary: Brenda Bowling	P: 540-591-5868 Email: bbowling@vccs.edu
	Point of Contact: Greg Scala	P: 276-964-7776 C: Email: Greg.Scala@sw.edu
IT Manager	Charles Musick	P: 276-964-7647 C: Email: Charles.Musick@sw.edu
Network Administrator	Brandon Walls	P: 276-964-7547 C: Email: Brandon.Walls@sw.edu
Help Desk Manager	Josh Hess	P: 276-964-7767 C: Email: Josh.Hess@sw.edu
Web Developer	John Dezember	P: 276-964-7332 C: Email: John.Dezember@sw.edu
Security Administrator	Jennifer Hale	P: 276-964-7295 C: Email: Jennifer.Hale@sw.edu
Director of Strategic Communications	John Dezember	P: 276- 964-7332 C: Email: John.Dezember@sw.edu
Campus Police Chief	Millard McGhee	P: 276-964-7603 C:

Information Security Incident Response Team (ISIRT) Contact Information		
Role	**Name**	**Contact Information**
		Email: Millard.McGhee@sw.edu

Appendix C

Additional Resources Contact Information		
	Name	**Contact Information**
Abuse Email Reporting	Abuse Email	abuse@vccs.edu
Chief Information Security Officer	Jud Skinker	P: (804) 891-4994 C: (804 229-4391 jskinker@vccs.edu
AVC Infrastructure and Security	John Savage	P: (804) 819-4945 jsavage@vccs.edu
SO Chief Information Officer	Mike Russell	P: (804) 423-5635 mrussell@vccs.edu
SO IT Emergency Support Line	On Call Employee	P: (804) 819-4915 Option 4
Legal Counsel **Office of the Attorney General**	Greer Saunders	P: (804) 819-4906 gsaunders@vccs.edu
Virginia State Police **Division Four**	Bureau of Criminal Investigation	P: (276) 228-3131 P: (800) 542-8716 **BFO** **EMAIL:vspdiv4@vsp.virginia.gov** **BCI EMAIL: bci-wytheville@vsp.virginia.gov** https://www.vsp.virginia.gov/Div4.shtm
FBI Local Field Office	FBI	FBI – 1913 Lee Highway, Suite 301 Bristol, VA 24201 (276) 466-1913
U.S. Secret Service	US Secret Service	P: (804) 592-3086
Cybersecurity Response Team	Beazley's Breach Response Services	bbr.claims@beazley.com

REVISION HISTORY

Date	Version	Reviewer	List of Changes
4/27/2021	1.0	Brenda Bowling	Draft SWCC IRP SOP
4/27/2021	1.1	Brenda Bowling/Charles Musick	Reviewed and updated
5/12/2021	1.1	SWCC Senior Staff	Reviewed and approved
5/26/2023	1.1	Brenda Bowling	Updated personnel changes
6/18/2024	1.2	Brenda Bowling/Charles Musick	Updated personnel changes