WCC Vendor-Supported Systems
Minimum Security Standards

If a vendor will be supporting and administering a computer system at WCC, these are the controls that must be in place.

Please complete these items for our information:

Operating System: _____

Anti-Virus Package: _____

Operating system — Devices shall use an operating system which is still supported by the software company. If the operating system stops being supported (end of life) it must be upgraded to the current supported version.

Security updates — Devices shall be kept up-to-date with current operating system and third-party applications security patches and updates.

Anti-virus software — Anti-virus software shall be used and kept up-to-date.

Software firewall — Firewall software shall be used and kept up-to-date.

Backups — Systems will be backed up to a secure facility to minimize the impact of hardware failure or malware attacks.

Security incident plan — A plan must be in place for the system for detecting security incidents and notifying WCC employees and Chief Information Security Officer (infosec@wccnet.edu) when a security incident is discovered.

Protection against brute force login attacks — Controls shall be put in place to limit failed login attempts.

Session controls — Controls shall be put in place to ensure that inactive sessions shall expire after a defined period of inactivity.

Logging and monitoring — System administrator and user activities and system events shall be logged. Logs shall be retained for a period of at least one year.

Identification and management of vulnerabilities — Devices shall be hardened prior to implementation. Security updates shall be applied and unnecessary services disabled in order to minimize potential technical vulnerabilities.

Encrypted transmission of data — Encrypted protocols or secure channels shall be used to transmit sensitive data to and from the device.

Encrypted storage of data — Sensitive data should be stored in an encrypted state or have compensating controls to secure the data.

WCC Vendor Questionnaire: On-premises System

Minimum security standards for a vendor supporting and administering a computer system at WCC.

Do you run operating systems that are still supported by the software vendor?

Will you update the operating system when it becomes end-of-life and no longer receives security patches?

What is your standard procedure for installing security patches on operating systems?

What anti-malware programs are you running on your systems? Who is the manufacturer?

What software-based firewalls are used to defend the computer and data?

Describe the backup procedures of the system.

Do you have a documented security incident response plan? If so, please provide.

What controls are in place to detect breaches and notify clients?

Describe controls in place to restrict and monitor the installation of unauthorized software.

What controls are in place to prevent brute force login attacks?

Describe controls in place to ensure that inactive sessions shall expire after a defined period of inactivity.

Describe controls in place for systems to hardened prior to implementation. Security updates shall be applied and unnecessary services disabled in order to minimize potential technical vulnerabilities.

How do you enable encryption of data in-transit and at-rest?

WCC Vendor Questionnaire: Cloud-based System

Minimum security standards for a vendor supporting and administering a Cloud-based computer system for WCC.

Do you run operating systems that are still supported by the software vendor?

Will you update the operating system when it becomes end-of-life and no longer receives security patches?

What is your standard procedure for installing security patches on operating systems?

What anti-malware programs are running on your systems? Who is the manufacturer?

What firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) are used to defend networks and data?

How often are rules reviewed to ensure that appropriate threats are mitigated?

Describe the backup procedures of the system. Please provide the name of the backup solution and the location of the backups.

Do you have a documented security incident response plan? If so, please provide.

What controls are in place to detect breaches and notify clients?

Do you conduct network penetration tests of your cloud service?

Do you perform SAS70/SOC2/ISO 27001/SSAE16 or similar external reviews?

How do you enable encryption of data in-transit and at-rest?

Describe controls in place to restrict and monitor the installation of unauthorized software.

Do you review your source code (if applicable) to detect security issues in code prior to placing code into production?

Do you have a BYOD policy to defend against data exfiltration?

Do you perform background checks on your employees?
