Version: 1.1
Issued: 6/30/2019

Vulnerability Scanning and Penetration Testing Policy- BCC-29 - 1.0

PURPOSE

The purpose of this policy is to define the guidelines for conducting vulnerability testing and penetration testing of systems within Berkshire Community College.

SCOPE

The scope of this policy applies to all information technology assets owned or leased by Berkshire Community College.

POLICY

Vulnerability testing and penetration testing is required for restricted systems. Optionally, non-restricted systems may also apply these standards.

Vulnerability Testing

- I cooperation with the Department of Homeland Security Berkshire Community College will regularly conduct vulnerability testing on all public-facing systems and restricted systems with testing of restricted systems.
- External vulnerability testing (scans) of restricted systems must be conducted on a regularly scheduled basis.
- Upon configuration change to the system, an internal scan must be performed.
- Failed vulnerability scans must be addressed and followed by a retest, repeating these steps until the vulnerability testing completes successfully.
- Upon identification of new vulnerability issues, firewall configuration standards shall be updated accordingly.

Penetration testing

- External and internal penetration testing shall be performed at least once a year.
- External and internal penetration testing shall be performed after any significant infrastructure or application changes.
- Penetration testing shall minimally consist of network-layer and application-layer penetration tests.
- Exploitable vulnerabilities noted during penetration testing shall be corrected and an adequate retest performed to demonstrate that identified exploit is addressed.

RESPONSIBILITIES

Role	Responsibility
IT Staff	Perform the tasks outlined in this policy, adhere to the policy.
IT Management	Ensure scheduling of necessary tasks and vendors to perform tests, ensure budget is available, confirm remediation is completed in a timely fashion.
Information Security Officer	Oversee the Compliance of the Policy, review the policy periodically and update the policy as needed.

REFERENCES

Frameworks	**Name**	**Reference**
	SANS CSC V6	CSC 4: Continuous Vulnerability Assessment and Remediation CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs CSC 7: Email and Web Browser Protections CSC 16: Account Monitoring and Control CSC 20: Penetration Tests and Red Team Exercises
Regulations and Requirements	**Name**	**Reference**
	PCI DSS 3.1	Requirement 1 Requirement 2 Requirement 11
	HIPAA/HITECH	§ 164.308(a)(1)(i): Security Management Process § 164.308(a)(1)(ii)(A) Risk Analysis § 164.308(a)(1)(ii)(B) Risk Management § 164.308(a)(3)(i): Workforce Security § 164.308(a)(6)(i): Security Incident Procedures § 164.308(a)(6)(ii) Response and Reporting
Supporting Standards and Procedures		

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Revision Number	Date and Time	Name	Description
0.1	2/6/2017		Initial Version
1.0	6/30/2018	Arlen Rauschkolb	Update
1.1	6/30/2019	Arlen Rauschkolb	Update