BERKSHIRE
COMMUNITY COLLEGE

Version: 2.0

Issued: 6/28/2018

Data Breach Response Policy BCC30 – 1.1

PURPOSE

The purpose of this policy is to define the actions required for responding to security incidents involving Berkshire Community College information and/or information technology resources to ensure effective and consistent response and handling of such events.

SCOPE

The scope of this policy applies to all members of the Berkshire Community College community and any affiliates using Berkshire Community College's information technology resources or data.

POLICY

All members of Berkshire Community College are responsible for reporting known or suspected information security breaches. (See BCC Incident Response Policy - Policy # 4) Incident response will be handled appropriately based on the type and severity of the incident.

Incident severity-Incident response is based on the level of severity of the incident. The level of severity is based on its impact on or threat to the operation or integrity of Berkshire Community College.

High: (Immediate Response)

- Threatens to have a significant adverse impact on a large number of systems or people
- Poses a potential large financial risk or legal liability to Berkshire Community College
- Threatens confidential data
- Adversely impacts an enterprise system or service critical to the operation of a major portion of Berkshire Community College
- Poses a significant and immediate threat to human safety
- Has a high probability of propagating to other systems and causing significant damage or disruption

Medium: (Response within 4 hours)

- Adversely impacts a moderate number of systems or people (department, unit or building)
- Adversely impacts a non-critical enterprise system or service
- Adversely impacts a departmental system or service
- Disrupts a building or departmental network
- Has a moderate probability of propagating to other systems

Low: (Response within next business day)

- Adversely impacts a very small number of systems or individuals
- Disrupts a small number of network devices or segments
- Has little or no risk of propagation or causes only minimal disruption

RESPONSIBILITIES

Role	Responsibility
Staff and Management	Understand and adhere to this policy. Report incidents to the Information security Manager immediately.
Management	Assist with evaluation and mitigation of the incident in conjunction with IT and the Information Security Officer
Chief Information Security Officer	Reports the incidents to upper management and appropriate external entities. Determines if incident follow-up is needed. Ensures that all incidents and resolution activities are fully documented and tracked. Uses these incidents in training awareness as examples of what could happen, how to respond to such incidents, and how to avoid them in the future. Oversee the Compliance of the Policy, review the policy periodically and update the policy as needed.

REFERENCES

	Name	Reference
Frameworks	**SANS CSC V6**	CSC 9: Limitation and Control of Network Ports, Protocols, and Services CSC 10: Data Recovery Capability CSC 13: Data Protection CSC 19: Incident Response and Management
Regulations and Requirements	**Name**	**Reference**
	PCI DSS 3.1	Requirement 10 Requirement 11 Requirement 12
	HIPAA/HITECH	§ 164.308(a)(1)(i): Security Management Process § 164.308(a)(1)(ii)(C): Sanction Policy § 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
1.1	6/4/2018		Update