Data Breach Response Policy

Document Version: 2018-10-01

Copyright © 2018

This material is based upon work supported by the National Science Foundation under DUE #1501990. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

This work is licensed under the Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by/3.0/.

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the incident response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards, and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well-publicized and made easily available to all personnel whose duties involve data privacy and security protection.

XYZ College Information Security's intentions for publishing an incident response policy are to focus significant attention on data security and data security breaches and how XYZ College's established culture of openness, trust, and integrity should respond to such activity.

1.1 Background

This policy mandates that any individual who suspects that a theft, breach, or exposure of XYZ College or restricted data or XYZ College sensitive data has occurred must immediately provide a description of what occurred via e-mail to CIRT@XYZcollege.edu or through the use of the help desk reporting web page at http://XYZcollege.edu. This e-mail address and web page are monitored by the XYZ College information security administrator. This team will investigate all reported thefts, data breaches, and exposures to confirm if a theft, breach, or exposure has occurred. If a theft, breach, or exposure has occurred, the information security administrator will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information of XYZ College members. Any agreements with vendors will contain language similar.

3.0 Policy Confirmed theft, data breach or exposure of XYZ College Restricted or Protected

As soon as a theft, data breach, or exposure containing XYZ College protected data or XYZ College sensitive data is identified, the process of removing all access to that resource will begin.

The CISO will chair an incident response team to handle the breach or exposure. The team will include members from:

- IT infrastructure
- IT applications
- Finance (if applicable)
- Legal
- Communications

- Member services (if member data is affected)
- Human resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, additional individuals as deemed necessary by the executive director

The executive director will be notified of the theft, breach, or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

4.0 Enforcement

Any XYZ College personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have their network connection terminated.

5.0 Definitions

Data Breach – A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.
Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).
Information Resource – The data and information assets of an organization, department or unit.
Safeguards – Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

6.0 Revision History

Version	Date of Revision	Author	Description of Changes
1.0	August 17, 2016	SANS Institute	Initial version
1.0			