VISTA

Data Breach Response Plan

1.0 Purpose
The purpose of the plan is to establish the goals and the vision for the data breach response process. The plan shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Vista Information Security's intentions for publishing a Data Breach Response Plan are to focus significant attention on data security and data security breaches and how Vista's established culture of openness, trust and integrity should respond to such activity. Vista is committed to protecting Vista's students, employees, patrons and the school itself from illegal or damaging actions by individuals or organizations, either knowingly or unknowingly.

1.1 Background
This plan mandates that any individual who suspects that a theft, breach or exposure of Vista Protected data or Vista Sensitive data has occurred must immediately provide a description of what occurred via e-mail to tbradshaw@vistautah.com or bhatch@vistautah.com. In conjunction with the Director, the IT team members 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 IT Team and Director will follow the appropriate procedure in place.

2.0 Scope
This plan applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or any protected information of Vista students, employees, and/or other patrons.

3.0 Plan Confirmed theft, data breach or exposure of Vista Protected data or Vista Sensitive data

As soon as a theft, data breach or exposure containing Vista Protected data or Vista Sensitive data is identified, the process of removing all access to that resource will begin.

The Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- Director
- Members of school administration
- IT Data Team
- Finance (if applicable)
- Legal Counsel
- Communications
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- FBI & BCI (If CJIS Data is Involved)
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Director

Confirmed theft, breach or exposure of Vista data

The Director will be notified of the theft, breach or exposure. IT, along with the designated incident response team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

Vista will select forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan.

Work with Vista communications and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

Develop a remediation plan.
Work with Vista IT staff and other employees to develop a remediation plan to protect the network from subsequent breach and the provide necessary training to employees.

Edited 9/6/17
SG