Data Breach Response

Mayville State University's policy on data breach response.

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. Information Technology Services' intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how MSU's established culture of openness, trust, and integrity should respond to such activity. Information Technology Services is committed to protecting the MSU community from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.0 Background

This policy mandates that any individual who suspects that a theft, breach, or exposure of protected data or sensitive data has occurred must immediately provide a description of what occurred via e-mail to Service.Desk@mayvillestate.edu, by calling 701-788-4739, or through the use of a Service Desk ticket at http://mayvillestate.edu/to/its/ticket . ITS staff 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 Chief Information Officer will follow the appropriate procedure in place.

3.0 Scope

This policy applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle private or restricted data, as defined in NDUS Procedure 1901.2.1.

4.0 Confirmed theft, data breach or exposure of protected data or sensitive data

As soon as a theft, data breach, or exposure containing protected data or sensitive data is identified, the following process will go into effect:

1) ITS staff will begin disabling access to identified exposed protected data or sensitive data
2) The Chief Information Officer will notify
    a. the Vice President for Academic Affairs or Vice President for Business Affairs
    b. the NDUS Chief Security Information Officer
3) The President's Cabinet will form an Incident Response Committee to handle the breach or exposure. The Incident Response Committee will be chaired by a cabinet member, but may include members from NDUS CTS, legal counsel, and others as necessary.
4) ITS staff will work with forensic investigators if requested by NDUS CTS. ITS staff will provide any necessary access to best 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.
5) The Incident Response Committee will develop and execute an appropriate communication plan that will communicate the breach to appropriate parties, including students, employees, the public, and those directly affected.

Reference:
NDUS Procedure 1901.2.1

Established: December, 2016
Sponsor: Vice President for Academic Affairs and : Chief Information Officer