Data Breach Response Policy

Policy Title:
Data Breach Response Policy

Responsible Executive(s):
Jim Pardonek, Associate Director and Chief Information Security Officer

Responsible Office(s):
University Information Security Officer

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

....

I. Policy Statement

This policy covers all computer systems, network devices, and any additional systems and outputs containing or transmitting Loyola Protected data or Loyola Sensitive data. The purpose of this policy is to provide a process to report suspected thefts involving data, data breaches or exposures (including unauthorized access, use, or disclosure) to appropriate individuals; and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved.

II. Definitions

Not applicable.

III. Policy

Reporting of suspected thefts, data breaches or exposures

Any individual who suspects that a theft, breach or exposure of Loyola Protected data or Loyola Sensitive data has occurred must immediately provide a description of what occurred via email to DataSecurity@luc.edu, by calling 773-508-7373, or through the use of the anonymous reporting web page at https://www.luc.edu/its/uiso/contacttheuiso/report_anon.shtml. This email address, phone number, and web page are monitored by Loyola's Information Security team. 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 team will follow the appropriate procedure, utilizing the University Incident Response Plan, depending on the class of data involved.

If the incident is a suspected theft, Loyola's Department of Campus Safety shall also be contacted at 773-508-6039. They will determine whether a local law enforcement agency

should be contacted based on the location and details of the incident. If a local law enforcement agency is contacted, the name of the agency and the report number should be provided to Loyola via the methods of contact outlined above.

Confirmed theft, data breach or exposure of Loyola Protected data or Loyola Sensitive data

As soon as a theft, data breach or exposure containing Loyola Protected data or Loyola Sensitive data is identified, the process of removing all access to that resource will begin as soon as possible. If the information is available on a site outside of Loyola, that site will be contacted to have the information removed as soon as possible.

The CIO will chair a response team to handle the breach or exposure. The team will include members from:

- ITS
- University Marketing and Communications (UMC)
- The Office of the General Counsel, Risk Management
- 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, as listed in the appendix
- Additional individuals as deemed necessary by the CIO

If a theft of physical property occurred, the Department of Campus Safety will be notified by ITS. This team will provide information to UMC regarding how the breach or exposure occurred, the types of data involved, the Loyola classifications of those data types, any protective measures around the involved data (such as encryption), and the number of internal/external individuals and/or organizations impacted. UMC will handle all communications about the breach or exposure. ITS will work with the appropriate parties to remediate the root cause of the breach or exposure.

Confirmed theft, breach or exposure of Loyola Public data

The CIO will be notified of the theft, breach or exposure, and will inform UMC as soon as possible. ITS will analyze the breach or exposure to determine the root cause. ITS will work with the appropriate parties to remediate the root cause of the breach or exposure. ITS will also examine any involved systems to ensure that they did not house any Loyola Protected data or Loyola Sensitive data. If the systems are found to also contain Loyola Protected data or Loyola Sensitive data, the CIO will be notified and the "Confirmed data breach or exposure of Loyola Protected data or Loyola Sensitive data" section of this policy will be invoked. If a theft of physical property occurred, the Department of Campus Safety will be notified by ITS. The Department of Campus Safety will determine if it is also appropriate to necessary other law enforcement agencies based on where the theft occurred.

For any data breaches, exposures, or thefts involving information listed below, a representative from the listed areas will be included on the response team:

Checklist

This checklist covers items that the response team should consider while responding to a security incident.

- Materials that may need to be developed to handle the incident including:
- Web pages
- Notification letter
- Press release
- Q&A for media
- Q&A for call center and other responders
- Alert university leadership teams (President, Cabinet, Information Technology Executive Steering Committee, Deans) so they understand what is being done to address the incident and are apprised of status. The order and frequency of updates to these groups will be determined by the CIO depending on the incident.
- All available information about the incident, including both information that has been confirmed and information that is suspected, will be provided to the response team. As new information is discovered, it will be provided to the response team as quickly as possible.
- Daily conference calls to checkpoint progress and obstacles are tremendously helpful in keeping things moving and sharing information.
- Size and severity (likelihood of fraud) of the incident may warrant different actions, i.e. whether credit monitoring is affordable and/or appropriate.
- Track the amount of time that has passed between incident, discovery of incident, and notification of affected individuals. While none of these steps are necessarily long, each one of them adds to the number of days to notification.
- If contracts need to be negotiated to provide services to the affected individuals, those negotiations should begin immediately. Check to see if previously negotiated contracts can be applied to the situation (especially for credit monitoring).
- Depending on the number of individuals impacted, it can take some time to assemble mailing address information for large groups. Begin pulling this data immediately.
- Identify the best location for mail merge and volume printing, envelope stuffing and metering of the mail.
- Ensure that adequate letterhead and envelopes is available or ordered. Letter should come from the Vice President in charge of the area in which the incident occurred. Determine the type of envelopes (windowed vs. address labels) as this will affect printing and the speed of envelope stuffing.
- The cost of printing, letterhead, envelopes and credit monitoring will be covered by the area in which the incident occurred.
- A percentage of the initial mailings will be returned as undeliverable so the number of deliveries to attempt and methods to pull additional delivery information should be identified.

Data Type	Areas or individuals to be additionally included on response team
Financial information, including but not limited to credit card numbers, bank account numbers, investment information, grant information, and budget information	Finance, Director of Cash Management and/or Assistant Treasurer
Information about individual employees, including but not limited to social security numbers	Human Resources
Student financial information	Office of Student Financial Assistance, Bursar, Marketing Communication Services
Student information protected by FERPA	Student Affairs, Registrar, Provost, Marketing Communication Services
Student health information	Student Affairs, Marketing Communication Services
Student information not listed above	Student Affairs, Marketing Communication Services
Research data	Research Services, Provost
Information Containing PHI under HIPAA Privacy Rule	Provost
PII concerning faculty	Faculty Administration, Provost
PII concerning donors or unreleased information about gifts received	Advancement
Payroll information	Controller and/or Payroll

Please refer to the Incident Response Policy and the Incident Response Policy – Appendix for further information and guidance.

IV.   Related Documents and Forms

Not applicable.

V.   Roles and Responsibilities

Chief Information Security Officer	Enforcing the Policy at the University by setting the necessary requirements.

VI.   Related Policies

Please see below for additional related policies:

- Security Policy
- Data Classification Policy
- Incident Response Plan
- Incident Response Appendix
- Disaster Recovery Master ITS Plan

Approval Authority:	ITESC	Approval Date:	March 4th, 2008
Review Authority:	Jim Pardonek	Review Date:	March 7th, 2024
Responsible Office:	UISO	Contact:	datasecurity@luc.edu