

IMMACULATA UNIVERSITY IT SECURITY INCIDENT RESPONSE PLAN

Effective Date:

- Authority** This Program was approved by the President of Immaculata University (hereinafter "IU").
- Program Statement** This IU IT Security Incident Response Plan (the "Plan") defines standard methods for identifying, documenting and responding to Data Security Incidents.
- Program Purpose** The purpose of this Plan is to prevent damage and/or loss to Institutional Data, including Private Information, to prevent damage to IU Information Technology and to place IU in compliance with its legal obligations.

Section headings are:

1. DEFINITIONS
2. IDENTIFICATION OF INCIDENT
3. ESTABLISHMENT OF INCIDENT RESPONSE TEAM
4. CONTAINING DAMAGE AND PRESERVING EVIDENCE
5. INCIDENT RESPONSE REPORT
6. ADDITIONAL OBLIGATIONS OF INCIDENT RESPONSE TEAM
7. INCIDENT PREVENTION
8. MODIFICATIONS AND ADJUSTMENTS
9. SPECIAL SITUATIONS/EXCEPTIONS

I. DEFINITIONS

"Data Security Incident" occurs when there is a serious threat of or unauthorized access or acquisition to IU Information Technology or a User's computerized data that compromises the security, confidentiality, or integrity of the information, including Institutional Data and Private Information. A Data Security Incident also occurs where there has been unauthorized access or acquisition of encrypted data and the confidential process or key to the encryption is also compromised. Data Security Incidents can range from the unauthorized use of another User's account or system privileges to the execution of malicious code, viruses, worms, trojan horses, cracking utilities, or attacks by crackers or hackers. Data Security Incidents may also involve the physical theft of IU Information Technology or a User's technology, such as a computer or other electronic media, or may occur as the result of a weakness in information systems or components (e.g., hardware design or system security procedures). A non-exhaustive list of symptoms of incidents that qualify as Data Security Incidents include: a system alarm or similar indication from an intrusion detection tool; suspicious entries in a system or

network accounting; accounting discrepancies; unexplained new user accounts or file names; unexplained modification or deletion of data; system crashes or poor system performance; unusual time of usage; and unusual usage patterns. Good faith acquisition of Private Information by a User granted Administrative Access pursuant to the IU Administrative Data Security Policy does not constitute a Data Security Incident, provided that the Private Information is not used or subject to unauthorized disclosure.

“Identity Theft” means fraud committed or attempted using the identifying information of another person without authority.

“Incident Response Team” is a group of individuals who will provide a quick, effective, and orderly response to a Data Security Incident. The incident response team’s mission is to prevent the misappropriation of confidential information such as Private Information, damage to IU Information Technology, serious loss of profits, public confidence, or information assets by providing an immediate, effective, and skillful response to any unexpected event involving computer information systems, networks, or databases. Members of the Incident Response Team should include the Program Officer, IU’s general counsel and outside counsel (Duane Morris LLP), members of the Office of Technology Services (“OTS”), a forensic specialist outside of IU who will provide independent analysis of any Data Security Incident and any additional individuals deemed appropriate by IU.

“Institutional Data” is any information, including Private Information, that can be linked to any individual, including but not limited to, students, faculty, staff, patients or contractors. Such data resides in applications such as Banner. Institutional Data and all applications storing and transmitting such data are valuable assets which IU has an obligation to manage, secure and protect.

“IU Information Technology” means IU resources, information technologies, and networks, including but not limited to, computers, computing staff, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computing-related contracts, network bandwidth, usernames, passwords, documentation, disks, CD-ROMs, DVDs, magnetic tapes, and other electronic media or storage devices.

“Private Information” is any information, including Non-Public Confidential Customer Information as defined in the IU GLBA Required Information Security Policy, all information that is considered personally identifiable information, trade secrets or intellectual property such as research activities, home phone number and address, health information, location of assets, passwords, parking leases, identity of anonymous donors, gender, ethnicity, citizenship, citizen visa code and veteran and disability status. Private Information and all applications storing and transmitting such data are valuable assets which IU has an obligation to manage, secure and protect.

“Program Officer” is the person appointed by the President who is responsible for the management and administration of this Policy.

"User" includes any individuals, entities such as third party hosting contractors, staff, faculty, or employed students, given electronic access to IU's Institutional Data and/or using IU Information Technology.

II. IDENTIFICATION OF INCIDENT

Any User or individual or organization not affiliated with IU may refer a Data Security Incident to the Program Officer. The Program Officer and his or her personnel can identify a Data Security Incident through proactive monitoring of IU's network and information system activities.

III. ESTABLISHMENT OF INCIDENT RESPONSE TEAM

The Program Officer shall assemble, manage, maintain, train and lead the Incident Response Team.

IV. CONTAINING DAMAGE AND PRESERVING EVIDENCE

Following a Data Security Breach the Incident Response Team will:

- Review the circumstances and the actions taken;
- Assign roles;
- Create a plan of action to contain damage and gather evidence; and
- Ensure that wherever possible, a forensic copy of the affected computer hard drive or server database is created.

The Incident Response Team will work with the appropriate staff and OTS to take whatever actions are necessary to ensure that no additional Institutional Data is lost or taken and/or that no additional Information Technology is exploited.

V. INCIDENT RESPONSE REPORT

The Incident Response Team will ensure that Data Security Incidents are appropriately logged and archived. To that end, following any Data Security Incident, the Incident Response team must produce an Incident Response Report (a "Report") as outlined in this Section V of the Plan. Any Data Security Incidents involving Electronic Protected Health Information ("ePHI") pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") will be so identified in the Report.

The Incident Response Team will be responsible for communicating the Incident to appropriate IU personnel and maintaining contact, for the purpose of update and instruction, for the duration of the Incident.

Each Report should include at a minimum the following:

- A description of the Data Security Incident;
- Type of Institutional Data or other information exposed and/or potentially at risk of exposure from the Data Security Incident;
- Type of IU Information Technology damaged or potentially at risk of damage or loss due to the Data Security Incident;
- Steps taken for containment of the Data Security Incident;
- Steps taken for remediation of the Data Security Incident;
- Logging of all internal and external communications issued, including all emails and phone calls regarding the Data Security Incident;
- Interactions with law enforcement and disciplinary authorities regarding the Data Security Incident; and
- Legal obligations and actions taken to satisfy those legal obligations regarding the Data Security Incident.

VI. ADDITIONAL OBLIGATIONS OF INCIDENT RESPONSE TEAM

Simultaneous with the creation of the Report and containment of the Data Security Incident, the Incident Response team must:

- Determine how the Data Security Incident occurred and take immediate remedial action to prevent it from occurring again;
- If the breach involves a User, contact the appropriate disciplinary office, including the local police if appropriate;
- Collaborate with IU's outside counsel to determine and then perform IU's obligations to affected persons and parties;
- Collaborate with the President to manage public relations communications effectively regarding the Data Security Incident; and
- Rebuild all comprised IU Information Technology and closely monitor the rebuilt systems.

VII. INCIDENT PREVENTION

Wherever possible and in conjunction with the application of other IU policies relating to information security, IU will undertake to prevent Data Security Incidents by monitoring and scanning its own network for anomalies, and developing clear protection procedures for the configuration of its Information Technology and other related resources.

VIII. MODIFICATIONS AND ADJUSTMENTS

This Plan and its procedures will be reviewed periodically to adjust processes, identify new risks and remediations.

IX. SPECIAL SITUATIONS/EXCEPTIONS

Any personally-owned devices, such as PDAs, phones, wireless devices or other electronic transmitters which have been used to store Institutional Data and are determined to have contributed to a Data Security Incident, may be subject to seizure and retention by IU authorities until the Data Security Incident has been remediated, unless the custody of these devices is required as evidence for a court case. By using these devices within the IU network for business purposes, individuals are subject to IU policies restricting their use such as the IU Acceptable Use Policy.