Revision History

Version	Date
Electronic Data Security Breach Reporting and Response Policy, 1.0	30 July 2021

ELECTRONIC DATA SECURITY BREACH REPORTING AND RESPONSE POLICY

I. Introduction

USEIC is committed to compliance with all applicable federal and state laws and regulations relating to the compromise of Sensitive Data (as such term is defined in the USEIC Data Protection Charter (the "Charter")). This Policy establishes measures that must be taken to report and respond to a possible breach or compromise of Sensitive Data, including the determination of the Systems affected, whether any Sensitive Data have in fact been compromised, what specific Sensitive Data were compromised and what actions are required for forensic investigation and legal compliance.

Capitalized terms used in this Policy without definition are defined in the Charter.

II. Policy

A. Reporting

Any suspected or confirmed breach or compromise of Sensitive Data must be reported to the Data Protection Officer (DPO) as set forth in Section D below in a timely manner in order to mitigate the risk to Information Resources and protect the Organization's operations.

B. Organization Response Team

Upon receipt of such report, the DPO, Director, Owner, and the Legal Counsel or his or her delegate will convene the Organization Response Team ("ORT").

The following lists the general responsibilities of the members of the ORT:

1. The DPO will serve as Incident Lead for any actual or suspected compromise of Sensitive Data.
2. The Legal Counsel is responsible for all legal issues associated with an actual or suspected compromise of Sensitive Data.
3. The Owner is responsible for all contacts with law enforcement and for non-technical aspects of any investigation.
4. The Director is responsible for all internal and external communications and media relations.
5. The Director will advise on personnel issues and communications to staff.
6. The DPO will provide the support required to investigate and respond to the actual or suspected compromise of Sensitive Data.

C. Procedures

The DPO will establish detailed internal procedures for compliance, external and internal communications, oversight of the investigation and technical support associated with a suspected or actual breach of Sensitive Data.

The specific incident response procedures are set forth in the applicable Information Security and Privacy Incident Procedure and Checklist.

The general steps in a response include the following:

1. Incident Categorization

Incidents will be categorized based on the applicable Information Security Office's internal procedures. Based on the severity of the incident, an appropriate response action will be taken.

2. Response and Recovery

The ORT may call upon any necessary additional offices and resources required to carry out the investigation and remediation of any breach. This expanded ORT will be responsible for the investigation of the incident and any technical support required. Incident team members will include the DPO and any other staff responsible for the Information Resources involved.

Any individual responsible for an Information Resource containing Sensitive Data that may have been compromised must take immediate steps to secure that system and preserve it without change.

3. Lessons Learned

After an incident has been resolved, an incident report will be created and distributed to the ORT. The ORT will then convene to discuss the security controls that failed and establish the steps necessary to prevent or limit the risk of the incident recurring.

D. Contact Information

To report a possible breach of Sensitive Data at USEIC:

USEIC Data Protection Officer
Email: dpo@useic.org
Telephone: +65 6471 0804