ELECTRONIC DATA SECURITY BREACH AND RESPONSE POLICY

INTRODUCTION

Relay Graduate School of Education is committed to compliance with all applicable federal and state laws and regulations relating to the compromise of Sensitive Data. Sensitive Data is any information protected by federal, state, and local laws and regulations and industry standards, such as HIPAA, HITECH, the New York State Information Security Breach and Notification Act, similar state laws, and PCI-DSS. This Policy establishes measures that must be taken to report and respond to a possible breaches or compromises of Sensitive Data, including the determination of the affected systems, whether any Sensitive Data have in fact been compromised, what specific Data were compromised, and what actions are required for forensic investigation and legal compliance.

A data breach is any instance in which there is an unauthorized release or access of personal identifiable information or other information not suitable for public release. This definition applies regardless of whether an organization stores and manages its data directly or through a contractor, such as a cloud service provider. Data breaches can take many forms, including:

- third party gaining access to data through a malicious attack
- lost, stolen, or temporarily misplaced equipment (e.g., laptops, mobile phones, USB flash drives, external hard drives, etc.)
- employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, etc.)
- policy and/or system failure (e.g., a policy that doesn't require multiple overlapping security measures—if backup security measures are absent, failure of a single protective system can leave data vulnerable)

The Sensitive Data included in the scope of the Electronic Data Security Breach and Response Policy are:

- all data regardless of the storage medium (e.g., paper, memory cards, hard disks, CD, DVD, external drive, USB flash drives, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.);
- the computing hardware and software systems that process, transmit and store Data
- the networks that transport Data

The Electronic Data Security Breach and Response Policy applies to all individuals who access, use or control Sensitive Data at Relay Graduate School of Education, including faculty, staff and students, as well as contractors, consultants and other agents of the University and/or individuals authorized to access Sensitive Data by affiliated institutions and organizations. Our goal is to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information. This document provides an overview of the process.

POLICY

Reporting

Any suspected or confirmed breach or compromise of Sensitive Data must be reported to the Security Response Team (defined below) in a timely manner in order to mitigate the risk to Information Resources and protect the University's operations at incident@relay.edu.

Security Response Team

Upon receipt of such report, the Senior Director of Technology or his or her delegate will convene the Security Response Team (SRT).
The SRT consists of representatives of the following units:

- Human Resources
- Affected Department or System Owner
- System and/or Network Administrator
- Senior Director of Technology
- Chief Operating Officer

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

- Human Resources will advise on personnel issues and communications to University staff
- The affected department or system owner will provide the support required to investigate and respond to the actual or suspected compromise of Sensitive Data
- The Senior Director of Technology is responsible for all legal issues associated with an actual or suspected compromise of Sensitive Data
- The Senior Systems & Support Engineer will be responsible for serving as Incident Lead for any actual or suspected compromise of Sensitive Data
- The Chief Operating Officer in concert with the Office of External Affairs responsible for all internal and external communications and media relations

Reporting Loss or Theft

- When equipment or a device (laptop, desktop, smart phone, iPad, mifi, other) is lost or stolen on campus, immediately fill out this form.
- If a Relay-owned device or personal device containing Relay sensitive data or used to access Relay sensitive data is stolen while off campus, first file a police report with the appropriate local authorities. Then, also report the occurrence

using this form.

- If you do not hear back within 48 hours after filling out the form, please email incident@relay.edu.

SRT Procedures

The Senior Director of Technology and Senior Systems & Support Engineer will establish detailed internal procedures for compliance, external and internal communications, and 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 Electronic Data Security Breach and Response Policy Checklist.

The general steps in a response include the following:

1. Incident Categorization

Incidents will be categorized based on the applicable SRT internal procedures. Based on the severity of the incident, an appropriate response action will be taken.

2. Response and Recovery

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

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

In the case of a lost or stolen Relay owned device the SRT will gather initial details of the loss or theft from the individual responsible for Sensitive Data including whether or not the device was on, logged into the network when stolen, if it contained files with sensitive data, and if those files were encrypted and password-protected or not. The SRT will, among other things, reset the end user's password and block all access to network resources, including e-mail, until such a time that the end user can change their password.

If there was a potential compromise of sensitive information or exposure of network resources, the Chief Operating Officer may confer with appropriate College officials and/or legal counsel, coordinate notification to affected individuals, and report the incident to state or federal agencies and the media as required.

3. Lessons Learned

After an incident has been resolved, an incident report will be created and distributed to the SRT. The SRT 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.