

Data Incident Notification Toolkit

Added by Valerie Vogel, last edited by Valerie Vogel on Feb 06, 2009

Purpose

To provide a toolkit with templates, tips, and examples that can be referred to during the process of notifying potential victims of data compromise.

Introduction

The resources provided here cover a range of issues that commonly arise in the heat of the moment when responding to data incidents. If your institution has a data incident, you will find these templates helpful on topics such as building a press release, drafting a notification letter to potential victims, creating a website with information about the specific incident, preparing for the handling of hotline calls and frequently asked questions, and constructing a website with tips on preventing and dealing with identity theft. In addition, a selection of other resources have been gathered for your easy reference: federal and state legal requirements; sample college and university policies, procedures, and plans; suggestions for determining the threshold for notification (whether or not to notify); general resources on identity theft; and real-life accounts from colleges and universities who have completed one or more incident notification processes.

If you have suggestions for additional content, or materials you would like to add, please contact Security-Task-Force@educause.edu.

Notification Templates

These Data Incident Notification Templates provide sample materials for dealing with all aspects of a data incident.

- Building a Press Release (Section One)
- Notification Letter Components (Section Two)
- Incident-Specific Web Site Template (Section Three)
- Incident Response FAQ (Section Four)
- Generic Identity Theft Web Site (Section Five)

Other Resources

Federal and State Legal Requirements

Note that there are currently no federal requirements, but several bills are in varying stages of approval in Congress, so stay tuned.

- California SB 1386
- Data Security Breaches and Consumer Notification (BNA's Web Watch)
- Electronic Privacy Information Center (EPIC) Bill Track
- Security Breach Notification Laws (University of Georgia)
- State Security Breach Notification Legislation/Laws (National Conference of State Legislatures)
- Summary of State Security Freeze and Security Breach Notification Laws (State Public Interest Research Groups)

Sample University Policies, Procedures, and Plans

- Indiana University Protection of Sensitive Institutional and Personal Data
- Indiana University IT Incident Response Procedures
- Indiana University School of Medicine Incident Response Policy
- Miami University Critical Incident Response Plan
- Miami University Incident Response Policy (Draft)
- Purdue University Incident Response Policy
- University of Delaware Personal Non-Public Information (PNPI) Policy
- University of Delaware Guidelines for Protecting Personal Non-Public Information (PNPI)
- University of Delaware Breach Notification Procedures
- University of Minnesota Policy on Reporting and Notifying Individuals of Security Breaches
- The University of Texas at Austin Policy on Protecting the Confidentiality of Social Security Numbers
- The University of Texas at Austin SSN Remediation Project

Thresholds for Notification (some suggestions)

- Thresholds for Notification: Deciding Whether or Not to Notify
- Determining the Threshold for Security Breach Notification (University of California Office of the President)

Individual University Materials on Prevention and Responses to Actual Incidents

Sample University Resources on Identity Theft

- Binghamton University
- Carnegie Mellon University

- Eastern Kentucky University
- University of Delaware
- University of Kansas
- University of Oklahoma
- University of Pennsylvania
- University of Rhode Island
- Yale University

University Responses to Real Data Security Incidents

- Johns Hopkins Hospital
- Oklahoma State University
- San Diego State University
- University of California at Los Angeles
- University of California at Riverside
- University of Texas at Austin
- University of Washington

Articles

- "Security Breaches: Notification, Treatment, and Prevention", by Rodney Petersen, EDUCAUSE Review (Volume 40, Number 4, July/August 2005)

California Office of Privacy Protection

- Recommended Practices on Notice of Security Breach Involving Personal Information

Department of Education Resources

- Department of Education's Office of Inspector General Identity Theft Website
- What To Do If A Victim of Identity Theft

EDUCAUSE Effective Security Practices Guide

- Incident Handling and Forensics

EDUCAUSE Resource Center Pages

- Data Security
- Identity Theft
- Incident Handling/Incident Response

Federal Trade Commission (FTC) Resources

- FTC Brochure: Facts for Consumers
- FTC Identity Theft Web Site

Hearing Testimonies

- UCLA's written testimony provided during a hearing on "Identity Theft: Innovative Solutions for an Evolving Problem"

Presentations

- "Cyberprivacy, Cybersecurity, and Cyberliability: The Duty to Disclose Security Breaches Under California's SB 1386" (NACUA 45th Annual Conference)
- "Damage Control: When Your Security Incident Hits the 6 O'Clock News" (EDUCAUSE 2003)
- Handout for "Damage Control: When Your Security Incident Hits the 6 O'Clock News" (EDUCAUSE 2003)
- "When the Bits Hit the Fan: Managing Data Security and Privacy" (EDUCAUSE 2004)

VA (Department of Veterans Affairs) Data Theft Information

- VA Frequently Asked Questions
- VA Notification Letter to Veterans
- VA Statement