



## ELECTRONIC DATA SECURITY INCIDENT PLAN

April 25, 2007

This document, prepared by the Office of the Vice President for Information Technology and the Office of the Vice President for University Relations, outlines Purdue University's plan should the security of restricted electronic data become compromised on the West Lafayette campus. It reflects the work of many across campus, whose advice has been extensively relied upon in formulating this plan.

Restricted information is information protected because of applicable protective statutes, policies or regulations. This level also represents information that is not by default protected by legal statute or regulation, but for which the information owners have exercised a right to restrict access. For the purposes of this plan, restricted electronic data is further interpreted to include, but not be limited to, Social Security and numbers and other personal identifying information; confidential university business or personnel records; information about organizations, corporations or governmental units; or any information considered confidential by responsible university administrators.

The University's procedures for responding to *potential* data security incidents are spelled out in Purdue's IT Incident Response Policy at [http://www.purdue.edu/POLICIES/pages/information\\_technology/v\\_1\\_4.html](http://www.purdue.edu/POLICIES/pages/information_technology/v_1_4.html). After an electronic data security exposure has been *confirmed*, the following plan takes effect. The participants, critical timeline and prescribed actions follow:

### **Key participants in the response:**

- 1.) Core security team: VP for Information Technology and CIO, ITAP chief information security officer (CISO)
- 2.) Core communications team: ITAP media relations coordinator, Vice President for University Relations, University News Service.
- 3.) Area IT communicators team.
- 4.) Area administrators team: Dean, department head and general communication officers.
- 5.) Security Officers Group: Security administrators campuswide.

For names and contact information, please see: <http://news44.uns.purdue.edu/ITcontacts/>.

**Immediately after determining restricted data has been exposed (as indicated in the Purdue IT Incident Response Policy)**

Once the ITAP chief information security officer (CISO) determines information may have been compromised, this will constitute official notification. The officer then will immediately share the results of the investigation with the core communications team.

**Within 30 minutes of initial notification, based on a business day**

The ITAP media relations coordinator contacts the college's or area's IT and administrative teams to tell them of the findings and review notification procedures.

**Within one hour after initial notification, based on a business day**

The college or area's IT communications network representative, in consultation with the ITAP chief information security officer (CISO), drafts a short initial summary of exposure and sends to the core and area teams.

**Within two hours after initial notification**

Chief information security officer (CISO) notifies the university legal counsel and requests counsel to notify the Indiana Attorney General's Office or other government agencies of the compromise of restricted information if and as appropriate under applicable law.

The incident summary is shared with all teams described above plus the security officers group and other offices, as needed. These may include:

- The Office of Advancement if alumni are involved.
- The Registrar if student administrative or academic information is involved.
- The Purdue Health Insurance Portability and Accountability Act (HIPAA) officer at the Purdue Student Health Center if health information is involved.
- Financial Aid if related information is involved.
- The Office of the Dean of Students if students are involved as either potential victims or culprits.
- University Residences if a person living in university housing is involved.

*All information shared is to be treated as highly confidential.*

**Within 1 business day after initial notification**

The Office of the Vice President for University Relations, in consultation with legal counsel, decides what communications will be needed. This may include a letter to those affected, a news release, or a Web site.

**Within 2 business days after initial notification**

University legal counsel notifies Attorney General's Office if and as appropriate under applicable law.

The University News Service, which maintains the official templates for such communications, drafts the needed documents and sends drafts for review to the core teams, followed by area teams.

Area teams put together e-mail or postal mailing lists and prepare for distribution, which may involve Printing Services if numerous people are affected. Sources for mailing lists include:

- Purdue Human Resource Services.
- Office of Advancement.
- Registrar.

Area teams put together response plan to be submitted to VP for University Relations.

The plan should include:

- Designation of, and contact list for, staff to be involved in response.
- Phone numbers for those affected to call.  
(Contact ITAP Customer Service at 494-4000 for help setting up a toll free-line.)
- Written script, incorporating Web sites and FAQs for responding to phone calls.

#### **Within 2.5 business days after initial notification**

All teams send suggested changes to communication drafts to the News Service.

#### **Within 3 business days after initial notification**

News Service sends revised communication documents to team members.

Office of the VP for University Relations sends area teams any changes needed in response plan.

#### **Within 3 business days and 4 hours after initial notification**

All teams send any requested changes in communication documents and response plan back to core communications team.

The ITAP chief information security officer (CISO) has final authority over wording that pertains to the technical nature of the incident and its implications.

#### **Within 4 business days after initial notification**

News Service finalizes all communication documents and sends them to VP for University Relations for approval.

#### **Within 4.5 business days after initial notification**

Office of the VP for University Relations sends communication materials and response plan to university counsel for final review.

Area IT communicators team and chief area administrators budget clerical and professional time, including time from area head and that person's superior, to respond to phone calls. An "escalation" procedure is put in place for callers who want to talk to higher authorities so calls don't jump from clerical staff directly to the dean, vice president or president.

**Within 5 business days after initial notification**

Counsel sends VP for University Relations and University News Service needed changes.

University News Service passes needed changes in response plans to area teams and makes needed changes in all communications documents, forwarding the letter to area teams for processing.

**Within 5.5 to 10 business days after initial notification**

Area IT communications officer provide the script and plan to ITAP Customer Relations.

Area general communicators finalize letter, mail list and distribution method.

Once letters are ready to be mailed, area teams alert the News Service then launches Web page and issues the news release.

Letters sent.

Department staff informed and assignments made to respond to phone calls and readdress and resend returned mail.

**After notification**

Any inquiries from the news media should be referred to the News Service.

Area IT communicators team conducts post mortem with department staff to review processes and procedures. Team shares findings with IT Communications Network and News Service and files all pertinent information related to the incident for possible future action.

News Service in consultation with the core communications team will review notification plan's effectiveness, revise and redistribute as needed.

**60-90 days after notification or after two weeks without additional inquiries**

Area IT communicators team discontinues toll-free line and notifies News Service to deactivate Web site.