

Dealing with Data Exposures

1	Responsibilities.....	1
2	PIRN-Personal Information Requiring Notification.....	1
3	Data Exposure Remediation Procedure.....	2
4	Notification Examples.....	3
4.1	Example of PIRN data exposure through email.....	3
4.2	Example of stolen/lost laptop with PIRN.....	4
5	Data Stewards (5/10/2010).....	5

1 Responsibilities

Whenever Virginia Tech is notified of a (potential) data exposure, specific steps should take place to work with university officials to determine a course of action to ensure compliance with federal and state regulations. The department responsible for the exposure should inform their department head of the incident and work with the Office of Legal Counsel and the IT Security Office to determine appropriate action(s).

The department responsible for the exposure assumes primary responsibility for dealing with issues of the exposure according to the Virginia Tech procedure listed here. They should work with data stewards to verify the confidentiality of the data and take responsibility for developing a communications plan that includes any publicity, notification to individuals and others, and necessary remediation.

The group or department responsible for the data exposure is responsible for contacting individuals affected by the exposure and must consult with the IT Security Office and the Office of Legal Counsel to develop a communication plan.

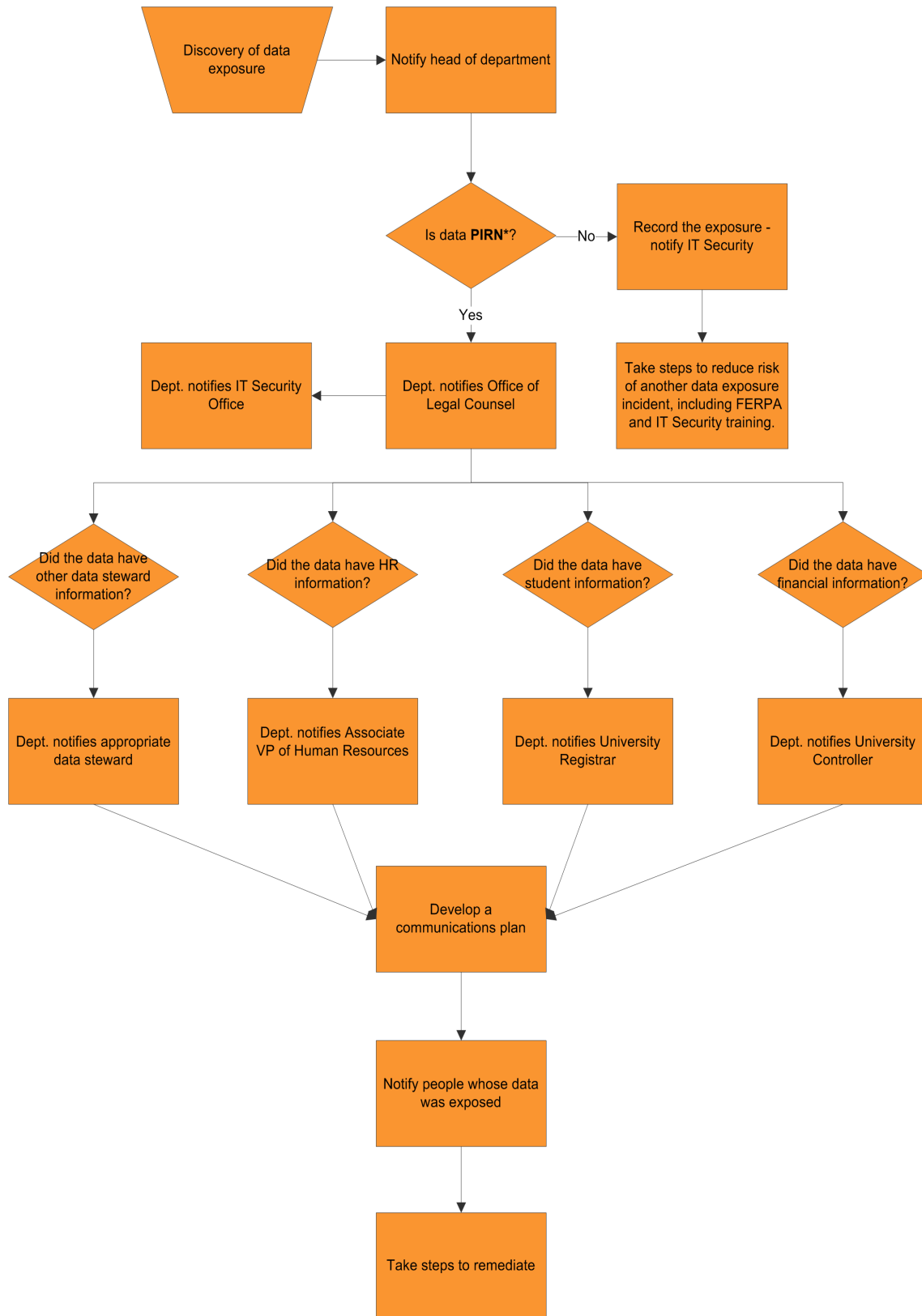
2 PIRN-Personal Information Requiring Notification

Personal information requiring notification (**PIRN**) includes sensitive information as covered by Virginia Tech's [Standard for Storing and Transmitting Personally Identifying Information](#):

- Social Security number
- Credit card number
- Debit card number
- Bank account number
- Driver's license number
- Passport number
- First name or first initial and last name with date of birth
- GPA or other information from a student's educational record

PIRN also includes elements of FERPA (Family and Educational and Privacy Act) and HIPAA (Health Portability Insurance and Accountability Act). Contact the IT Security Office or the Office of Legal Counsel for help determining if data qualifies as **PIRN**.

3 Data Exposure Remediation Procedure



4 Notification Examples

Examples of contact letters have been provided below to help guide the process of contacting those who have had their data exposed. The examples use a scenario of data exposures through email and a stolen laptop. The contact template could easily be changed to reflect a data exposure through a lost digital storage device. Contact the IT Security Office and Office of Legal Counsel to coordinate a communications plan.

4.1 Example of PIRN data exposure through email

<DATE>

<Addressee>

You are receiving this letter because on <date>, a handling error in our office resulted in a file containing some of your confidential data being sent to an incorrect e-mail address for which we cannot identify the owner.

The data file included the following information from your application to our program:

<List of data elements>

We have no evidence that an unauthorized individual has actually utilized any of this information, and notice was sent to the recipient's address advising that the file was sent in error and requesting that it be destroyed. We are bringing this incident to your attention, in accordance with Virginia law, so that you can be alert to signs of any possible misuse of your personal identity.

As the situation develops, we will send additional messages regarding any further information which we are able to discover. Please monitor your email in the coming days for messages from our office. We have also changed our handling procedures such that files containing confidential data are transferred through vehicles other than e-mail. If you have any questions, please contact our department at <department email>.

We apologize for this lapse and for any inconvenience it may cause.

Sincerely,

<Signature>

4.2 Example of stolen/lost laptop with PIRN

<Date>

Dear <student name>:

Virginia Tech recognizes the importance of safeguarding your personal information. To that end, we have implemented strict administrative, technical, and physical safeguards to protect that information. However, even the most rigorous safeguards cannot guarantee protection against criminal conduct. Virginia Tech officials have been notified of the theft of a laptop computer that contained a file that held some of your personal information. Specifically, the file contained <list of items> from several years ago.

Although we believe this theft was directed at the hardware, and not the contents, we wanted to act preemptively to notify you of this situation and inform you of the risk. We do not have evidence that anything has been done with the information, but we are bringing this incident to your attention so that you can be alert to signs of any possible misuse of your personal identity. We will continue to monitor the situation, and recommend you take precautionary steps to guard yourself against any potential identity theft.

[We have established a website at <(URL)> to provide you with information].**(Optional)** You may place a fraud alert with credit bureaus and/or periodically run a credit report to ensure accounts have not been activated without your knowledge. If you determine that an account has been fraudulently established using your identity, you should contact law enforcement and the financial agency with which the account was established. The following references provide additional information about identity theft:

- Federal Trade Commission website on identify theft (<http://www.consumer.gov/idtheft/>)
- Social Security Administration Fraud Line at 1-800-269-0271
- Major Credit Bureau Numbers
 - Equifax 1-800-525-6285
 - Experian 1-888-397-3742
 - Trans Union 1-800-680-7289

As an additional safeguard, you may choose to place a temporary “fraud alert” on your credit report. Fraud alerts can help prevent an identity thief from opening any accounts in your name. You are encouraged to contact the toll-free fraud number of one of the three main consumer reporting companies to place a fraud alert on your credit report. The toll-free number for one of the three, Equifax, is shown above. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report as well

Virginia Tech is committed to maintaining the privacy of present/past student information and takes many precautions for the security of personal information. Although social security numbers are no longer used for identification purposes in our automated systems, the files on the stolen laptop preceded the new identification policy and most records still contained the social security number. We sincerely regret any inconvenience this incident presents to you.

If you have any questions, please contact our department at <department email>.

Sincerely,
<Signature>

5 Data Stewards (5/10/2010)

Office or Area	Data Steward	E-Mail	Phone
Academic Advising	Kim Brown	ksbrown@vt.edu	231-8440
Accounts Receivable	James Elliot	elliojo@vt.edu	231-6277
Information Technology	Jeb Stewart	jeps@vt.edu	231-2134
Alumni	Tom Tillar	ttillar@vt.edu	231-6285
Athletics	Jim Weaver	weaverj@vt.edu	231-3977
Budget /Financial Planning	Tim Hodge	thodge@vt.edu	231-6419
Career Services	Donna Ratcliffe	cassell@vt.edu	231-8077
Communication Network Services	Judy Lilly	jlilly@vt.edu	231-8505
Controller's Office	Ken Miller	millerk@vt.edu	231-7448
Design /Construction	Jim McCoy	jmccoy@vt.edu	231-6449
Development	Rhonda Arsenault	arsenau@vt.edu	231-2833
Office of Diversity and Inclusion - Interim	Karen Sanders	kasande1@vt.edu	231-7500
Extension	Rick Rudd	rrudd@vt.edu	231-6836
Scholarship & Financial Aid	Barry Simmons	simmons@vt.edu	231-5179
Graduate School	Karen DePauw	kpdepauw@vt.edu	231-7581
Environmental Health & Safety	Zach Adams	adamsz@vt.edu	231-5985
Human Resources	Hal Irvin	hirvin@vt.edu	231-7784
Institutional Research	Kris Bush	khbush@vt.edu	231-1796
Investments & Debt Management	John Cusimano	cusi@vt.edu	231-7094
Real Estate Management	Elizabeth Reed	reede@vt.edu	231-8430
Parking Services	Steve Mouras	stmouras@vt.edu	231-0233
Physical Plant	Michael Coleman	colemanm@vt.edu	231-5530
Police	Wendell Flinchum	wendellf@vt.edu	231-6183
Provost Office	Ken Smith	kensmith@vt.edu	231-1807
Provost Office	Patricia Hyer	hyerp@vt.edu	231-2350

Office or Area	Data Steward	E-Mail	Phone
Purchasing	Tom Kaloupek	kals@vt.edu	231-6221
Records Management	Gerry Palmer	gepalmer@vt.edu	231-0226
Registrar	Wanda Dean	wdean@vt.edu	231-7951
Residential /Dining	Ed Spencer	espencer@vt.edu	231-8069
Risk Management	Fred Weaver	weaverf@vt.edu	231-7439
ROTC	Richard Roszak	roszakrs@vt.edu	231-9369
Schiffert Health Center	Kanitta Charoensiri	charkx@vt.edu	231-5313
Sponsored Programs	Linda Bucy	lbucy@vt.edu	231-5281
Student Affairs	Ed Spencer	espencer@vt.edu	231-6272
Undergraduate Admissions	Mildred Johnson	mildredj@vt.edu	231-6267
University Libraries	Eileen Hitchingham	hitch@vt.edu	231-5593
Veterinary Medicine	Michael Harness	harness@vt.edu	231-7177
Virginia Tech Services	Don Williams	dowilli3@vt.edu	231-5991