Copyright Ron Nichols & Kate Webster 2006. This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.
Properly Securing “Sensitive Information” Across The Campus

Copyright 2006 - University of Delaware
Information Technologies
User Services

Ron Nichols
Manager - Desktop Support

Kate Webster
Information Resource Consultant
The University of Delaware

Land Grant

Sea Grant

Space Grant

Urban Grant
The University of Delaware

16,000 undergraduates
7,300 students live in residence halls

99% own a computer
3,000 graduate students
Information Technologies

- Management Information Services
- University Media Services
- User Services
- Network & Systems Services
  - Includes Help Center
Properly Securing “Sensitive Information” Across The Campus

- PNPI -
Personal “Non-Public” Information
The Problem

- SSN used as student identifier
- Class Rosters
- Test scoring sheets
- Shadow systems
- Normal way to do business
Spring 2004

- Small IT Team Assigned (7 people)
- SSN & Credit Card Use
- Online Web Survey
Web Survey

Assess Use in Departments

Human Resources Liaisons
(185 People)

70% Responded
Secure Use of Personal Information at UD

For this section, please answer the nine questions about one practice in which your department or unit uses SSNs. These are questions about the specific practice: how, where, and how securely SSNs are stored; and whether or not there are appropriate or acceptable alternatives to SSNs for that particular practice.

After pressing the submit button, you will be able to describe another practice or to return another time to continue.

Your name: ____________________________

Department or unit: _______________________

HR liaison's name: _______________________

1) Describe one practice in which SSNs are used by your department or unit (payroll, attendance, grade recordkeeping, etc.).

________________________________________________________________________

2) How is the SSN information stored? (Mark all that apply.)

☐ Don't know
☐ In this particular case, SSNs are not stored in this department or unit.
☐ Paper record
☐ Word doc
☐ Excel spreadsheet
☐ Access database
Online Database

- Populated with data from survey
- Assigned callbacks - mostly done over the phone
- Follow-ups completed Spring 2005
- Stayed within the small team...
# Online Database

## SSN Information at UD

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Department</th>
<th>Assigned To</th>
<th>Issues</th>
<th>Key1</th>
<th>Key2</th>
<th>Key3</th>
<th>Key4</th>
<th>Key5</th>
<th>Key6</th>
<th>Key7</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>517</td>
<td>AG Departments</td>
<td>College of Agriculture and Natural Resources</td>
<td>Dyar, Gibson, Amsler</td>
<td>IT Comment</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
</tr>
<tr>
<td>545</td>
<td>Alba Bates</td>
<td>John Weinberg Center for Corporate Governance</td>
<td>Cindy/Ginny</td>
<td>IT Comment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
</tr>
<tr>
<td>352</td>
<td>Alison Brayfield</td>
<td>Museum Studies/Center for Material Culture Studies</td>
<td>John H and Kim</td>
<td>IT Comment</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
</tr>
<tr>
<td>371</td>
<td>Allan Fanjoy</td>
<td>Special Sessions</td>
<td>us-nichols</td>
<td>IT Comment</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pending IT System Conversion</td>
</tr>
<tr>
<td>372</td>
<td>Allan Fanjoy</td>
<td>Special Sessions</td>
<td>us-nichols</td>
<td>IT Comment</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pending IT System Conversion</td>
</tr>
<tr>
<td>373</td>
<td>Allan Fanjoy</td>
<td>Special Sessions</td>
<td>us-nichols</td>
<td>IT Comment</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pending IT System Conversion</td>
</tr>
</tbody>
</table>
Late Spring/Summer 2005

- Discovered a stolen computer contained 400 student SSNs
- House Bill 116 Pending
Mid-July Meeting w/VP

More Aggressive Effort!

Every Department on Campus Must Be Visited By IT Staff!

November 1, 2005 Compliance Date!
Top-Down Support

Memo went out from Executive Vice-President and Provost
Say What?

By When?
User Services Took Over Project

- Co-leaders
- Recruited User Services staff through managers
The Plan

- Team of 20 people!
- Weekly meetings
- IT Audit checklist was fine-tuned to get ready for interviews
- Mailing list created
The Plan

- Master list of departments
- Two staff members went to each visit
- Departments were assigned to staff (or volunteers)
Guidelines Were Created

Expanded to include all PNPI

FERPA
HIPPA
GLBA
There were existing policies

- Information Security
- Responsible Computing
- Records Retention
Communications
Federal laws and regulations govern the safeguarding of personal, non-public information (PNPI), such as Social Security Numbers (SSNs). The

- Family Educational Rights and Privacy Act (FERPA) [educational records],
- Gramm-Leach-Bliley Act (GLBA) [financial institution and customer data], and
- Health Insurance Portability and Accountability Act (HIPAA) [health information]

all require those who collect PNPI to follow strict guidelines. Protecting information is important because of identity theft.

At the University of Delaware, all departments must reduce their reliance on SSNs, using alternative forms of identifying students, clients, employees, and faculty whenever possible. Further, all University departments should follow good practices in safeguarding all personal non-public information (PNPI). Examples of PNPI include, but are not limited to:

- SSNs
- Credit card or bank account numbers
- Medical or educational records
- Other sensitive, confidential or protected data (e.g., grades used in context with personally identifiable information such as name, address, or other easily traceable identifiers).
LIFE Fest 2005 debuts at The Bob

It was standing room only, as staff, faculty and students joined about 1,700 freshmen to view the results of 100 collaborative projects at LIFE Fest 2005.

Read this story

NEWS

- UD among leaders in chemistry and chemical engineering
- Internet2 connects researchers around the world

NEED TO KNOW

- Winter box office hours set
- For the Record, Dec. 9, 2005
- Final exams are textbook buy-back time

WHAT'S HAPPENING

Special holiday public skating Dec. 23-Jan. 2

- Winter Session film series set
- Free midnight breakfasts during finals
- 'Curious George' on Mitchell Hall stage Feb. 18
PNPI Audit Process under way

12 p.m., July 22, 2005--In September 2004, UD’s office of Information Technologies launched a campaign to help campus departments protect sensitive personal nonpublic information (PNPI), such as Social Security and credit card numbers.

“We are helping departments develop more secure business processes and making sure each department understands that it is responsible for assuring compliance with the Family Educational Rights and Privacy Act (FERPA) and other laws that govern the use of PNPI,” Susan Foster, vice president for information technologies, said.

Information Technologies has released a new set of guidelines [www.udel.edu/ssn/guid.html] aimed at helping departments secure PNPI and make sure they are in compliance with the law.

The guidelines direct departments to ensure the privacy of PNPI by encrypting electronic transmissions, not storing PNPI locally and protecting PNPI when working from home or outside the University.

In addition, a team of Information Technologies staff members has begun visiting University offices to evaluate the processes for handling PNPI and to discuss measures that will help protect computer systems and sensitive information.
PNPI project prompts changes for faculty

3:45 p.m., Aug. 29, 2005--At the end of July, faculty received e-mail regarding the removal of Social Security Numbers (SSNs) from computerized test-scoring forms. Protecting the personal nonpublic information (PNPI) entrusted to faculty, goes far beyond test-scoring forms, however.

For years, SSNs have been used as identifiers at the University and elsewhere. "In today's world, with the threat of identity theft so prevalent, we are obligated to discontinue the use of SSNs wherever we can," Joseph DiMartile, assistant provost for student services and University registrar, said.

According to DiMartile, changes have been made to forms commonly used by faculty. Class rosters now list UDelNetIDs instead of SSNs. In addition, the following forms use a name "lookup" instead of the SSN to locate students:

- Supplemental Grade Roster Web Form;
- Incomplete Grade Extension Web Form;
- Incomplete Grade Explanation Web Form; and
- Change of Grade Web Form.

After Nov. 1, the Smith I/O Services (basement of Smith Hall in room 004) will no longer accept brown test-scoring response sheets with SSNs filled in. Instead, faculty can post or track grades by assigning students a random number known only to the instructor and the student. Students can use that number in the "Student ID Number" section of the test-scoring form. An alternative idea for a unique identifier is to have students enter their UDelNet ID in the "Last Name" space and the first 7 characters of their last name in the "First Name" space.

Kate Webster, information resource consultant, IT/User Services, points out that PNPI varies in degree of sensitivity.
Brochure Mailed to all Faculty/Staff

Protecting Personal Non-Public Information (PNPI)

UNIVERSITY DEPARTMENTS MUST ACT

• Any information that uniquely identifies a person and provides confidential information about that individual or that can be used to acquire such confidential information is considered Personal Non-Public Information (PNPI).
• State and Federal laws and regulations govern the safeguarding of PNPI.
• All University of Delaware departments must reduce their reliance on Social Security Numbers and use alternative forms of identification whenever possible.
• All University employees must follow good practices in safeguarding all PNPI.
• Each department must re-examine its use of PNPI, including its practices for retaining or storing this sensitive information.
• Annually, each department must review all processes that use or require access to PNPI.
• For more information, visit http://www.udel.edu/pnpi
Communications

- Seminars
- Presentations to departmental faculty/staff were offered
- E-mail notification
Office “Audit” Visits
Office “Audit” Visits

- Notes entered into database
- Unique needs discussed at weekly meetings
Results of Visits

- Technical staff assigned to help certain offices
- Some requests needed to go to central programming staff
Another Result...

Lots of Shredding!
Results of Visits

- Project leaders closely tracked status of visits
- Weekly report was created for VP
Simultaneously
Online Compliance Form

PNPI Management Compliance Report

Use this form to report your compliance with University policies, Delaware laws, and Federal laws (such as the Family Educational Rights and Privacy Act [FERPA]) that govern the security of Personal Non-Public Information (PNPI). For more information, visit UD's PNPI web site.

Every faculty and staff member must understand that each employee is responsible for securing any PNPI that he or she retains. Therefore, some department chairs or unit heads may ask individual faculty and staff to submit individual reports before the departmental report is submitted. If so directed, you can use this form to report your own compliance to your supervisor or department chair before he or she reports on behalf of your department to the appropriate administrative officer.

Symbol Key: * Required Information, ! Error

Submitter's name: Nichols Jr., Ronald R

I am answering on behalf of: *

Choose one

Department(s): *

E-mail of the person to whom you report: *

[lookup]
University of Delaware Policies and Procedures Manual

Section: Administrative  
Policy Number: 1-22  
Policy Name: Personal Non-Public Information (PNPI) Policy  
Date: October 6, 2005

I. PURPOSE

The purpose of the Personal Non-Public Information (PNPI) Policy is to expand on the Information Security Policy #1-15 to establish requirements for protecting personal, non-public information and notifying individuals whose personal, non-public information may have been disclosed by computer security breaches.
Software Tools

Contents

Introduction: University departments must act
Importance of protecting SSNs and other PNPI
Guidelines for protecting PNPI
Software Tools
For more information

Questions or comments

Copyright © 2005, University of Delaware

There are many different software tools that can help you safeguard PNPI stored on a computer. These tools are organized by the task that they help you perform.

How do I encrypt files that contain PNPI?
As a general rule, PNPI should not be stored on a "local" computer. However, in some circumstances (e.g., a faculty member who keeps grade records in Excel worksheets), it is necessary to do so. In those cases, you should follow the directions linked below to encrypt the files that contain PNPI.

- Encrypt Sensitive Data (link to directions for using the Windows and Macintosh operating systems' "native encryption")
- Encrypt Sensitive Data Using AxCrypt (link to directions for Windows users for using AxCrypt, free software that has additional features [e.g., sharing of encrypted files, easier encryption for Windows users whose computers are attached to a Windows domain, etc.])
Software Tools

- Encryption
- Search tools
- Electronic file shredding
- Complete hard drive wiping (e.g. surplus systems)
What Did We Learn?
Communication Isn’t Easy!

- Tough to get the message to everyone
- Consistency
- Faculty resist!
Timeline Was Aggressive

- As we met with offices we had no answers to certain questions
- Policy decisions were being fine-tuned during this time period
- Tools weren’t ready
Include Other IT Departments

- MIS & NSS to quickly answer questions and discuss issues and problems

- do-able or not?
Maintaining the Message

- Will be rolled into yearly records retention policies
- Will be mentioned at New Employee Orientations
Conclusion

- Project was a success
- Departments are responsible
- Not following up on non-compliance - we’re not the police
Questions?
Properly Securing “Sensitive Information” Across The Campus

Ron Nichols - nichols@udel.edu
Kate Webster - kate@udel.edu

URLs
http://www.udel.edu/UDaily (search for PNPI)
http://www.udel.edu/ssn

Copyright 2006 - University of Delaware