



Welcome to

**Protecting
Personally Identifiable
Information**

Training

Press here to continue

Instructions

Click on the control buttons along the bottom of each screen to navigate your way through this course. These buttons are defined as



Next screen



Previous screen

Each screen has a link that enables you to send comments about this training or e-mail your questions to an expert for answers.

This course takes about 20 minutes to complete (a little longer if you visit the web sites).



What is Personally Identifiable Information?

Personally Identifiable Information is defined as data that can be used to identify or contact a person uniquely and reliably, including but not limited to:

- Full Name
- Home Address
- Phone number
- Social Security Number
- Birth Date
- Medical Records
- Vehicle Registration and Driver's License Number
- Face, Fingerprints, or Handwriting



What is Personally Identifiable Information?

Personally Identifiable Information also consists of such information as:

- Name or address of a parent, family member or emergency contact
- List of personal characteristics
- Mother's maiden name
- Bank account information
- Credit card information
- Passport and visa information
- Citizenship
- Other information that would make the individual's identity easily traceable

Personal user preferences tracked by a Web site via a "Cookie" is also considered personally identifiable when linked to other Personally Identifiable Information provided by the user on line.



DOE Definition of Personally Identifiable Information:

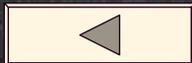
Public Personally Identifiable Information includes:

- First/last name, address, phone number, general education credentials

Protected Personally Identifiable Information includes:

- Social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records

Protected Personally Identifiable Information needs to be protected, Public Personally Identifiable Information also if co-mingled with Protected Personally Identifiable Information.



You Must Protect Sensitive Information

In addition to protecting Personally Identifiable Information, you are obligated to protect sensitive information including:

- Salary and Job Information



Protecting Personal Information

Any employee, guest or contractor who has access to records containing Personally Identifiable Information must successfully complete this course.

The purpose of this training is to inform you of the requirements and how to protect the personal information you handle in the day-to-day execution of your job.

Questions about identifying Personally Identifiable Information can be directed to Bonnie Miller at bmiller@bnl.gov, or Ext. 2875.

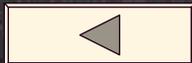
Questions regarding Cyber Security can be directed to cyberinfo@bnl.gov.



Objectives

After you complete this course, you will be able to:

1. Identify “Personally Identifiable Information.”
2. Protect Personally Identifiable Information in all forms (paper or electronic).
3. Recognize your responsibilities to protect such information.
4. Prevent the release of Personally Identifiable Information by instituting effective protections.
5. Make the proper checks before sharing Personally Identifiable Information with others.
6. Adhere to BNL regulations regarding the use of passwords on computer systems.



Your Role

Your role is to protect the sensitive and confidential personal information of employees, contractors and guests entrusted to you.

Employees with access to personal information, whether printed or electronic, are accountable for safeguarding this information from unauthorized access by practicing the safeguards covered in this training.



Why Protect Personal Information?

Various Federal regulations exist regarding a person's right to privacy, including but not limited to, the Privacy Act of 1974, the Financial Privacy Act of 1978, the Online Personal Privacy Act of 2002, and the May 22, 2006 memo from the Executive Office of the President emphasizing legal responsibilities to protect Personally Identifiable Information:

<http://www.whitehouse.gov/OMB/memoranda/fy2006/m-06-15.pdf>

It is for this reason that the Department of Energy (DOE) requires that all DOE contractor employees who handle Personally Identifiable Information complete training for the protection of personal information.



Accountability and Responsibility

Accountability for protecting personal information extends from the Laboratory Director to every employee and user.

The Personal Information Confidentiality Statement that appears on this web page:

<http://www.bnl.gov/HR/EERecords.asp>

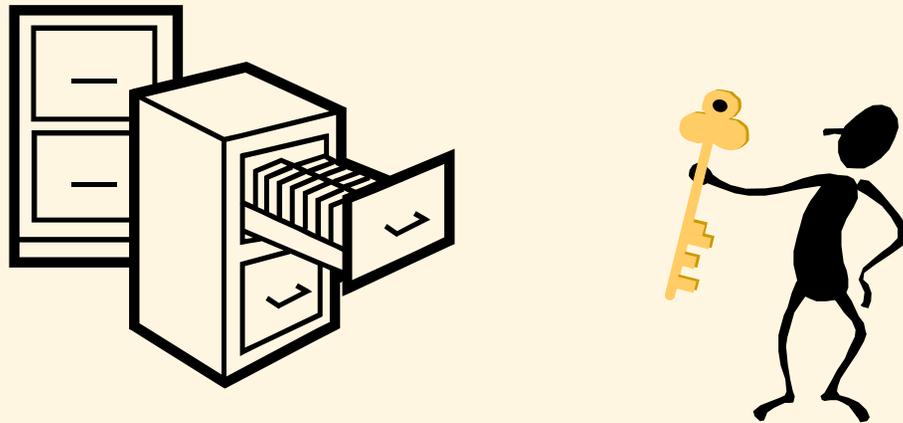
outlines the requirements for those who are entrusted with the personal information of employees and guests of BNL.

The following training material is based on these responsibilities.



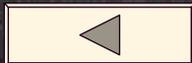
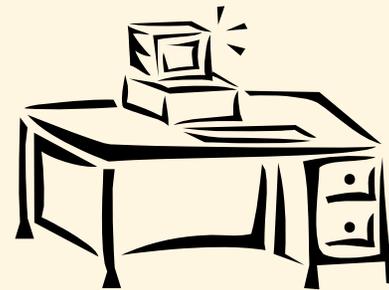
Keep Information Locked Up

Keep personal information in locked files, containers or areas.



Restrict Access

Restrict entry to areas
where personal information
is **not** locked.



Use a Screen Saver

Use password-protected screen savers to lock your computer when unattended.



It is required that you use a screen-saver password to lock your screen anytime your system is inactive for 15 minutes or more.



How to Use a Password-Protected Screen Saver

How to Lock Your Computer

In addition to the required logon password, you must use a screen-saver password to **lock your screen** when your system is unattended. This will prevent anyone from sitting at your computer and accessing your files, installing a keyboard sniffer, and decrease the risk of someone impersonating you (sending out e-mail under your name) and/or accessing systems you are connected to.

- You may immediately initiate the screen saver of a Windows computer by **holding down the Ctrl-Alt-Del keys all together, then releasing them and pressing the Enter key.**
- Unlock the computer by once again pressing Ctrl-Alt-Del and entering your password.

If you need instructions on how to set this up, call x5522, the ITD Help Desk.

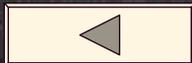


Screen Savers Don't Protect Against Hackers

Even with a screen-saver password, **your computer can be invaded by a hacker whenever it is connected to the network.**

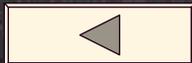
To reduce this risk, log off your computer if you are going to leave your computer system unattended for an extended period of time.

Also, ensure that your computer is fully patched and contains the latest version of Trend Micro antivirus software! Contact the ITD Help Desk at x5522 for help.



Don't Leave Personal Information Out and Unattended

Remove personal information from desks when it is not in use and lock it away.

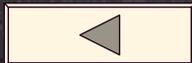


Don't Share Information

Before sharing personal information:

- Ensure that others are authorized to have access to that information
and
- Have a bona fide business related need-to-know

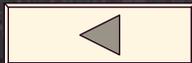
If there is any uncertainty about the request, call Employee and Guest Records at Ext. 2876.



Requirements for E-mailing Personally Identifiable Information

Whenever you e-mail Personally Identifiable Information, there are special precautions that must be used as there are many points at which an e-mail could be compromised.

- When sharing Personally Identifiable Information it must always be encrypted.
 - Software called “Entrust” may be used for encryption. Contact James Fung, Ext. 8403, to request this software.
 - Software that offers encryption:
 - Adobe Acrobat for PDF files <http://www.adobe.com/>
 - Microsoft Office encryption may be enabled (call the ITD Help Desk)
 - PGP <http://www.pgp.com/>
- Personally Identifiable Information should never be sent off-site.



Beware of E-mail Blunders!

Employees have the ability to access and transmit Personally Identifiable Information with a simple click of a button.

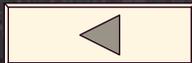
Minor e-mail mistakes can have major consequences.

- Misaddressing unencrypted e-mail containing Personally Identifiable Information will send critical data to a third party resulting in legal ramifications.
- Forwarding e-mail (or attachments) outside of BNL can be intercepted by malicious individuals resulting in **identity theft**.
- **Before clicking that button**, ensure the recipient is authorized to view the information.



Access Private Information Only for Job Need

Use private information only
for the reason access was provided.

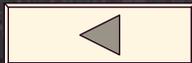


Follow Requirements for Passwords

Adhere to all Laboratory regulations covering the use of computer systems, particularly those covering password procedures.

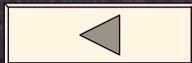
Follow Lab policies on creating secure passwords:

<http://www.bnl.gov/cybersecurity/passwords.asp>



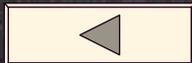
Discard Information Properly - Shred!

When discarding paper containing personal information,
it must be shredded.



Refer External Requests for Information!

Refer all outside requests for personal information
to
Employee and Guest Records
Ext. 2876.



Rules Apply for Laptop, Off-site and Home

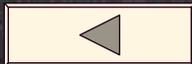
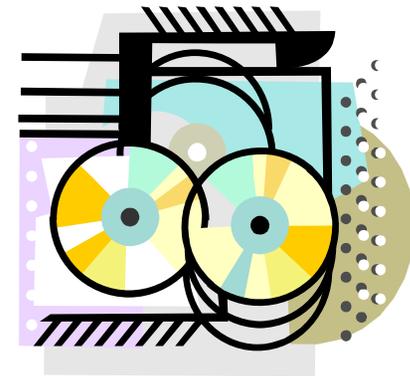
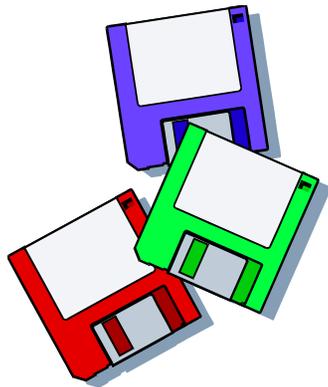
These responsibilities continue when working with Personally Identifiable Information from laptops and home computers.

- Laptops that store Personally Identifiable Information needs to be encrypted and approved every 90 days by DOE.
- When working off-site, you can only save Personally Identifiable Information to a secure BNL system.
 - Laptops with encryption
 - Your User folder on BNLNT1
 - Servers within your organization



Rules Apply For Other Mobile Media Use

Do not carry electronic media (floppy disks, CDs, DVDs, thumb drives) containing Personally Identifiable Information unless it is encrypted and approved every 90 days by DOE.



Notify Your Supervisor

Immediately notify your supervisor for potential loss of Personally Identifiable Information.



News Headlines

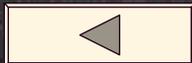
Recent news headlines revealed the loss of massive amounts of Personally Identifiable Information resulting from failure to protect this highly sensitive data:

- **VA Secretary Comes Under Fire At House And Senate Data Theft Hearings**
 - The hearings focused on the fallout of the May 3, 2006, data theft, after a VA analyst took his laptop home to do some after-hours work.
 - The data breach will cost taxpayers \$100 million to notify veterans that their information might be compromised and to offer credit protection services.
 - [Click Here](#) to read the entire article.



News Headlines

- Bank of America says Tapes with Customer Data Lost
 - CHARLOTTE, N.C. — Bank of America has lost computer data tapes containing personal information on 1.2 million federal employees, including some members of the U.S. Senate.
 - “Once again, consumers have been put at risk of identity theft because sensitive customer information held by a financial institution has been compromised,” Gail Hillebrand, senior attorney for Consumers Union, said in a prepared statement. “This is another reminder of how vulnerable consumers are to having their personal and financial information fall into the wrong hands.”
 - [Click Here](#) to read the entire article.



Protect Your Identity at Home too!

Do not reveal personal information about yourself or others to someone who calls and requests this information unless you are certain of that person's identity and that the request is legitimate. **NEVER** reveal your Social Security Number to anyone who calls you, at work or at home!

[Click Here](#) for Cyber Security Bulletin - How to Avoid Social Engineering and Phishing Attacks



Thank you for your Time and Attention.

Your Actions are Critical to Brookhaven's Ability to Protect our Personal and Private Information.

Your compliance, cooperation, common sense, and awareness helps to protect everyone.

Please don't hesitate to contact
Employee and Guest Records
Ext. 2876 with any questions.

