ESH223

CYBER SECURITY

EDUCATION AND AWARENESS

Welcome

Please Note: *Direct links to the resources referenced in this course are provided on the last page of this document.*

The cyber security program at Argonne National Laboratory promotes the safe use of information technology. Argonne plays a key role in America's continued leadership in computing sciences. However, the Laboratory must balance the expansion of computing technology with the need to protect its information infrastructure.

The threat to Argonne's cyber security is real. On an average day, the Laboratory defends against roughly 600,000 attempts to gain access to Laboratory systems. That's about 219 million attacks annually!

These attempts range from automated systems, such as SPAM and network probes, to more concise, targeted attacks against our employees. Unfortunately, even after all of our attempts to defend against these attacks, we still have roughly 10 successful attempts a year.

Because Argonne has distributed computing, cyber security must be a shared responsibility. Players include Laboratory management, the Cyber Security Program Office, various system administrators and the end users. This course was developed to help you meet your cyber security responsibilities.

Course Objectives

After you complete your annual cyber security refresher, you will be able to:

- Recognize your role in the cyber security program.
- Prevent computer misuse.
- Identify and prevent phishing and social engineering practices.
- Prevent computer theft.
- Recognize and report computer incidents.
- Identify the significance of backing up your data regularly.
- Recognize the importance of the Argonne National Laboratory Information Technology Access Agreement.

Passwords

Cyber security starts as soon as you log in to your computer. Two of the first key methods of keeping Argonne's computing and networking resources secure are selecting a secure password following DOE guidelines and changing your password at least once every six months.

At Argonne, passwords must:

- Consist of at least eight (8) non-blank characters
- Consist of a combination of:
    - Letters (upper and lowercase)

They must NOT:

- Include common words such as 'dog,' 'cat' or 'mom'
- Use numerals in the first or last position
- Be a simple pattern of letters or numbers such as xyz123

- Numbers
- At least one special character in first 7 positions (@#&*)!

NOTE: Percent sign (%) may prevent login to certain Argonne applications. In addition, some applications may not accept all special characters. Please refer to the particular application's password guidelines for details.

Locking your Workstation

Remember to lock your workstation! Argonne has configuration management to configure computers to automatically lock after 15 minutes of keyboard or mouse inactivity. In order to unlock your workstation, you must enter your password. If you leave your workstation for a short time (e.g. to pick up a printout or go to the restroom), you should manually lock the workstation.

How to Lock Your Computer
There are several ways to lock your computer, and the method you choose is a matter of personal preference. For detailed instructions on how to lock your workstation, contact the Argonne Service Desk (630-252-9999).

The Lab Monitoring and Warning Banner

The Laboratory provides access to state-of-the-art computing and network resources, including some resources generally unavailable to the public, industry, and academia.

The Laboratory expects end users to use these resources professionally, responsibly and in the best interests of the Laboratory. Argonne monitors usage of its computing and network systems to verify that this expectation is being met and that no abuse of the systems is taking place.

Each time you log in to a computer at Argonne, you should see a banner pop up to inform you about Argonne's monitoring practices. By clicking OK, you give your consent to the kind of monitoring described in the banner. If you do not see this warning banner when you log in, contact your Cyber Security Representative (CSPR). Link to the CSPRs are provided on the last page of this document.

Computer Misuse

Although personal use of Argonne computing resources is allowed, it is not to be abused. Argonne computer users must not engage in activities that are illegal, prohibited by laboratory policy or that are likely to incur incremental costs not related to Argonne's overall missions. Examples of prohibited activities include using Laboratory computers to:

- Access inappropriate Internet web sites such as sexually explicit or gambling sites.
- Receive, send, generate or store documents related to a personal business.
- Attack other sites.
- Participate in activities that are illegal or that otherwise may cause disrepute or legal liability for the Laboratory (see LMS-POL-51).
- Violate software license agreements.

This is not a comprehensive list. Engaging in any of these or similar prohibited activities can result in disciplinary action up to and including dismissal (see LMS-POL-44).

Controlled Unclassified Information (CUI)

Information or services that must be specially protected from alteration or disclosure is often known as Controlled Unclassified Information (CUI). CUI is comprised of the following information that you may be working with at the laboratory; this data may exist in paper OR electronic form:

- Financial risk
- Legal risk
- Privacy act
- Export Controlled Information (ECI)
- Official Use Only (OUO)
- Unclassified Controlled Nuclear Information (UCNI)
- Essential for day-to-day operation
- Collaborative Research and Development Agreements (CRADA)
- Personal Identifiable Information (PII)

These types of information require additional protection. Argonne CUI is not allowed to be stored on home computers. Contact your CSPR or your CASPIR Rep* and review LMS-POL-19, Protection of National Security and Other U.S. Interests and LMS-PROC-22, Protection of Controlled Unclassified Information, if your work involves critical/sensitive information.

* CASPIR - Critical and Sensitive Personal Information Reporting system.
CASPIR Reps are also known as Critical Program Information Coordinators.

Controlled Unclassified Information Handling

Desks: Do not leave paper documents or electronic media on your desktop. CUI should never be displayed or exposed to unauthorized persons. It might be appropriate to use locked filing cabinets to store some CUI. Please contact the Cyber Security Program Office (CSPO) for more information.

Computers: Laboratory computers store certain sensitive data. Only authorized employees may access sensitive data. CUI is not allowed to be stored on home computers under any circumstances.
Cloud storage of CUI should only be conducted on Argonne vetted and approved cloud storage locations like Box Plus. Please contact the Cyber Security Program Office for more information.

Filing Cabinets: To protect the information from alteration or disclosure, you may store certain Controlled Unclassified Information in LOCKED filing cabinets. Please contact the Cyber Security Program Office for more information.

Bulletin Boards: Controlled Unclassified Information should NEVER be displayed on bulletin boards or exposed in any other way to unauthorized persons.

Trash Cans or Recycling Bins: CUI should never be discarded in trash cans or recycling bins. Paper documents should be shredded and electronic media containing CUI should be rendered unusable when discarded.

Personally Identifiable Information (PII)

Argonne and its employees also have a duty to protect personally identifiable information (“PII”) from unauthorized use or disclosure. This duty extends both to your own PII as well as PII to which you may obtain access in the course of carrying out your job responsibilities. PII includes an individual’s first and last name combined with anyof the following:

- Social Security Number
- Passport Number
- Credit Card Number
- Clearance Levels
- Bank Numbers
- Biometrics
- Date of Birth
- Place of Birth
- Mother's Maiden Name
- Criminal Record
- Medical Records
- Financial Records
- Educational Transcripts

Caution: PII may be present within many types of records or items including passports, drivers' licenses, personnel files, job applications, school transcripts, etc.

The Laboratory is required to report any loss of PII to Congress within 45 minutes of the discovery of the loss. In addition, depending on the nature and extent of the unauthorized use or disclosure, Argonne may be under a legal duty to issue notifications to potentially affected individuals and mitigate such uses or disclosures, and could further be subject to severe penalties and damages for failing to do so.

Therefore, **if you have a reasonable belief that the unauthorized use or disclosure of PII has occurred, it is imperative that you notify your divisional CSPR immediately, and send an email to the OPSEC PII Task Force at pii@anl.gov.**

If in the course of carrying out your job responsibilities at Argonne you gain access to PII, you must comply with Argonne's policy for Safeguarding Protected Personally Identifiable Information and other applicable Argonne, DOE and legally imposed requirements.

The duties regarding the protection of PII include, without limitation, the following:

- Only access and disclose PII to the extent necessary to perform your official job responsibilities. Avoid unnecessary copying and transmission, even if the disclosure is the individual's own PII or it is made available to individuals with an authorized business need to access the information. For example, if a colleague needs to review a document that contains PII, but the PII is not relevant to the immediate business purpose, then redact the PII before transmission.

- If the PII is in tangible form (e.g., recorded on paper, a flash drive, etc.), store it in a secure locked container or area with access limited to authorized persons. Do not remove PII from Argonne's site, except to the extent required by law or necessary to carry out authorized Argonne-related job responsibilities.

- If the PII is in electronic form, ensure that it is only used, transmitted and stored on a system approved by Business and Information Services (BIS) that includes password protection, encryption, two-factor authentication, anti-virus and other data security features that comply with DOE, Argonne and other applicable legal standards. Do not store, use or transmit any PII in, to or through any Argonne, personal or third-party device or application, whether local, remote or online, that has not been specifically approved by BIS for those purposes. Do not store anyone else's PII on any personally owned devices or cloud or other services to which you personally subscribe. Do not store credit card or banking information on any Argonne systems.

- Timely notification of potentially affected persons and appropriate government authorities of the unauthorized use or disclosure of PII.

If you think you have PII stored on your computer or that you may possess it in paper form, you should ensure that it is appropriately secured on a system and in a manner specifically authorized by BIS, and you should contact your CSPR or CASPIR Rep. Your CSPR or CASPIR Rep will make a Critical Program Infrastructure entry.

Examples of PII include:

- Foreign national assignments
- Full school transcripts
- Conference credit card information
- Passport information for travelers

NOT PII:

- Pay Grades
- Badge Numbers
- Performance Appraisals

Argonne is not responsible for the protection of PII that is not Argonne specific, such as personal credit card or banking information. Employees are discouraged from storing this type of information on Laboratory computers.

The Laboratory has a CUI (Controller Unclassified Information) procedure, LMS-PROC-22, Protection of Controlled Unclassified Information, which you can reference for more information.

Privacy Act

What is the Privacy Act about?

- The Privacy Act of 1974 (5 U.S.C. 552a) establishes controls over what personal information is collected and maintained by the Executive Branch and how the information is used.
- The Privacy Act grants certain rights to an individual on whom records are maintained, and assigns responsibilities to an agency which maintains the information.
- All DOE employees and contractors are subject to the Privacy Act and must comply with its provisions.

What is the System of Records (SORs)?

Clause H.9 (Privacy Act Records) of the Prime Contract identifies the following SORs for which the Laboratory is responsible for ensuring compliance with the Privacy Act:

- Personnel Medical Records (except Contractor employees)
- Personnel Radiation Exposure Records
- Employee and Visitor Access Control Records
- Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites

What shall the employees do?

- Ensure that personal information contained in a System of Records, to which they have access to or are using to conduct official business, is protected to ensure security and confidentiality.
- Ensure that requests for information protected by the Privacy Act are in writing and signed.
- Not disclose personal information except as authorized.
- Report any unauthorized disclosures to your supervisor.

What shall the managers do?

- Ensure that all personnel who either have access to a System of Records or who develop/supervise procedures for handling records are aware of their responsibilities for protecting personal information.

What are the penalties for violating the Privacy Act?

- Both criminal and civil penalties are addressed in the Privacy Act for non-compliance.
- The penalty is a misdemeanor criminal charge, and a fine of up to $5,000 for each offense and/or administrative sanctions. Courts may also award civil penalties.

Information Protection

Most people recognize that their computers store sensitive information that is vital for their daily work and for the operation of the Laboratory. However, many computer users overlook the fact that sensitive data may be exposed as a result of discarding:

- Paper print outs
- Portable media devices such as floppy disks, CD-ROMs, and memory sticks
- Computers

These low-tech exposure risks can be eliminated by following simple strategies:

- Shred sensitive documents; do not simply place them in a recycling container.
- Erase electronic media before destroying it or submit it to BIS's electronic media destruction program. Please contact your CSPR or the Help Desk at 2-9999 - Option 2 for guidance.
- Deliver unneeded computers and hard disks to your CSPR for sanitization and disposal. Unneeded computers must be sanitized prior to disposal.

Information Protection and Cloud Services

Is it OK to use cloud services like Drop box, Gmail, Google Docs, Twitter, Facebook, OneDrive?
Currently, Box, a secure file storage system, is the only Argonne-approved cloud file storage solution.

What does this mean if you store or process Argonne data on non-Argonne owned or contracted services?
This means that you, the employee, are taking on the additional cyber risks which could lead you to be held personally responsible for loss, theft, unintended disclosure, E-Discovery, and data retention.
Never store or transmit PII or Controlled Unclassified Information (CUI), which may consist of data that is marked Official Use Only (OUO), using any information system, cloud or other service that has not been specifically approved by BIS for those purposes.

To read more about information sharing and the Box service, see the last page of this document for a link to the Box information page.

Bring Your Own Device (BYOD)

Although Argonne permits the appropriate use of personal devices to perform work, you must not store PII and you should avoid storing other sensitive data on your personal devices, personal email, or personal cloud or other personal network storage or services. In all cases, you should ensure that all information and data you create, use or access in relation to your job responsibilities at Argonne are stored on systems and services approved by BIS. In addition to creating further data privacy and security threats, the use of personal devices and services to store Argonne information or data may result in those personal devices and services becoming subject to legal discovery in the event of litigation involving Argonne.

This means that your personal devices or services may become subject to a litigation hold or subpoena that may require you to preserve all relevant information and to grant third parties access to your personal devices and services.

Therefore, a best practice is to ensure that all Argonne information and data that you use, create or transmit resides on Argonne approved and managed systems and services.

What are the rules for using my own device or email system at Argonne National Laboratory?

- Protect Lab sensitive data
  - i.e. PII needs to be encrypted at rest, in transit, and protected by 2-factor authentication if accessed remotely, and should never be saved on a personal device
- Protect access to your device by configuring a PIN/password and login timeout
- Immediately notify the CSPO if the device is lost, stolen or compromised to assess the impact of the data disclosure and determine and apply appropriate mitigations as determined by the lab
  - i.e. mitigations may include remote wipe, legal action, HR employee relations, law enforcement
- Remove all Argonne National Laboratory data before you dispose of your device, upon termination, or as requested by the laboratory to ensure compliance with Argonne, DOE, legal or regulatory requirements, policies and procedures.
- Your CSPR or the CSPO can help with understanding these requirements

Posting Information Online - Representing Argonne

In today's world, everyone is a potential web content provider. You don't have to be a web developer, but if you respond to a blog, for example, you are posting information on the web. Therefore, it is important to remember that all materials posted on publicly accessible web sites must:

- Enhance and protect Argonne and the Department of Energy's reputation
- Be in keeping with the publication desires of the work sponsor
- Be related to the Official Business of Argonne National Laboratory

Please Note: Scientific information must undergo a formal, documented review before posting. See Scitech 1 – 8 (available through the Document Center) and the Publication Approval Notification and Distribution Application (PANDA) website for more information.

Policies governing employee's public activity:

- LMS-POL-26, Employee Conflict of Interest
- LMS-POL-51, Employee Conduct

Protection of unclassified controlled information - resources:

- LMS-POL-19, Protection of National Security and Other U.S. Interests
- Classification Services

All links are available on the last page of this document.

Several types of information should not be posted on publicly accessible web sites:

- Classified, sensitive, Official Use Only (OUO), Unclassified Nuclear Information (UCNI), or export controlled materials
- Proprietary information related to intellectual property, potential patents, inventions, and trade secrets
- Personally identifiable information (PII)
- Personal information (such as home telephone numbers or addresses)
- Political endorsements
- Copyrighted materials
- Offensive materials

Social Engineering

Social Engineering (SE) is the practice of obtaining confidential information about a given individual and/or their company through the art of deception, and it usually leads to identity theft. SE risks are always present at home and at the Laboratory. Contact either your local CSPR or the CSPO when you

receive what you believe to be an SE attempt.
Be aware of suspicious requests in person, over the phone, or through e-mail for information such as:

- User names
- Passwords
- Organization charts
- Installation of software or security patches

Any media (CDs/DVDs, USB drives, memory cards) you receive that you did not specifically request should be treated with great care. Ignore e-mail hoaxes, and do not pass them on. Check with your CSPR if you think an e-mail is a hoax, or check a website such as **snopes.com**.

Phishing

E-mail is one of the most common platforms for Social Engineering attacks. Approximately 82% of all e-mail received at Argonne is tagged as spam. Most computer users know not to respond to spam e-mail, especially e-mails requesting personal information, since no legitimate organization is going to ask you for personal information via e-mail.

But did you know that just by clicking on a link or downloading and opening an attachment from an e-mail, malicious software can be downloaded and installed on your computer without your knowing it?

This is exactly what happens in phishing attacks. Phishing is an attempt to trick you into giving away personal information or installing malicious software by clicking on a link or opening an attachment in an e-mail. If this happens at the Laboratory, not only is your personal and professional data at risk for destruction or to be given away, but your computer can be used to infect the machines of your coworkers around the Laboratory.

Normally, the Laboratory firewall stops malicious links and attachments. But a new virus can slip through before the firewall can be updated, creating a window of vulnerability for the whole Laboratory. When this happens, links or attachments can also silently load onto your machine. Once installed, the malware is behind the firewall and can send your personal data out. And now, the malware can use your computer to infect other computers behind the firewall.

One common phishing method is to send you an e-mail that asks you to verify an account or to look into a problem with an account by clicking on a link. If you were to click on the link, you would be taken to a page that looks just like PayPal, for example, but isn't PayPal at all. If you typed your password in, you would be giving your info to the attacker. But worse than that, malware may be silently installed on your computer, putting personal and Laboratory data at risk.

Phishing scams come in all forms. In recent years, federal laboratories have come under increasingly sophisticated cyber security attacks. Many of these attacks come by e-mail, and the most effective appear to come from sources such as partner institutions, federal agencies or Laboratory management. In order to raise awareness of phishing attacks at the Laboratory, in 2006, the CSPO conducted a social engineering assessment approved by Laboratory management against a small number of Argonne employees.

The assessment worked like this: using a system operated and controlled by the CSPO, an e-mail was sent to 400 Argonne e-mail addresses. The e-mail included information about a recent Argonne Open House and a link that would supposedly take the user to pictures from the event.

========== From: Argonne Open House [mailto:openhouse@anl.gov]

Sent: Thursday, October 19, 2006 9:38 AM To: user Subject: Argonne Open House Pictures first name=, We hope that you enjoyed the ANL Open House. If you missed it, we took the time to take some pictures throughout the day. Click on the link below to browse the online picture gallery. Click Here -> Pointed to: http://www.fireintheh0le.org/.anl.gov/UI/login.php?id=83QU6EOc7k
==========

In order to simulate a real phishing attack, the CSPO carefully worked through the process, making every effort to ensure that only public information gathered off of the Argonne web was used in deriving the audience and the topic – information that any malicious user would have access to. The e-mail addresses were harvested from public-facing Argonne websites, and the Open House was chosen as a lure because the event had been covered in newspapers.

If the user clicked the link in the e-mail, he was directed to a website running on the CSPO web server that had the look and feel of the Argonne portal login and requested a username and password. If the user input his username and password, he was directed to a social engineering awareness page that discussed the specifics of this exercise and tips that can be used to aid in detection of real social engineering attempts. The CSPO did not collect any of the usernames or passwords that were supplied.
How many users were fooled?

The e-mail was sent at 9:38 AM. Within just 5 minutes, 23 users had clicked the link. Of those 23, 17 had entered their username and password. By 9:43, a user in BIO had reported the e-mail as suspicious. Had this been a real phishing attempt, the CSPO would have put in a block on that URL. By the time the CSPO estimates the blocks would have been put in, 40 users had entered their usernames and passwords. Within an hour of the e-mail being sent, 100 of the 400 people who had received the e-mail had clicked the link, and 75 had submitted their username and password. Had the e-mail gone unreported, and had the e-mail been a real attack, this could have cost Argonne hundreds of thousands of dollars in damages and lost productivity.

But how can you tell if a link is safe or not? The common defense against this kind of attack is to move your cursor over the link without clicking. Wait one or two seconds and what you'll see is a pop up window that will tell you exactly where that link will lead. If you look between the first two slashes following the http and the next slash, what you'll find is a code for the computer that the webpage is hosted on. In this example, we had an e-mail that seemed to come from PayPal. But you can see that this isn't the PayPal address at all; an e-mail that seems to come from PayPal, and a link that goes somewhere else. This is clearly a phishing attack. The best you can do is to delete the e-mail.

On most computers, only an administrator has the privileges to install software. Mac and UNIX systems typically have a separate login for installing software. But historically, Windows PC users have used a single login for both normal use and administrator tasks such as installing software. If you are using a PC and your user does not have administrator privileges, you are still vulnerable to loss of personal information, so you still need to be careful. But your computer is much less likely to be used as a platform to infect your coworkers' machines. The Laboratory has updated all PCs to separate user and administrator privileges.

Remote and Home Computing

Could your home computer be a back door? Absolutely!
Argonne incidents are often the result of infected home computers. Many employees use their home computers for work related to the Laboratory or to connect remotely to Argonne's systems using technology like VPN* (Virtual Private Network). You can use the strategies listed below to protect your home computer as well as Argonne's computing systems.

To protect the Laboratory while computing remotely:

- Install virus protection and spam filters.
- Maintain your home computer monthly. Visit the Cyber Security website to obtain a guideline for your home security (link is available on the last page of this document).
- Install a home firewall.
    - Antivirus software for personal use is available from your internet service provider for little to no cost.
    - A hardware firewall such as a Linksys router behind your cable modem or DSL service.

Implement home wireless networks with caution! Verify your home wireless access point is in a secure configuration. Malicious users exploit open wireless access points to give an extra layer of anonymity by making it look like their attack came from your home! Visit the Cyber Security website for more information.

Visit the Cyber Security web page to obtain a copy of the Cyber Security for Your Home Machine guide.
* Please note that a secure platform, Dash, is now available and it provides access to selected Argonne business applications without the need for VPN. To learn more, visit the link on the last page of this document.

Identifying and Reporting Potential Computer Incidents

You are Argonne's best mechanism for the identification and reporting of computer incidents. Although monitoring capabilities built into Argonne's computing architecture can identify system attacks, the most accurate monitoring capability is yours. The best way to detect intruders is to prepare beforehand.

Recognize abnormal behavior
First, you should be able to recognize what is normal behavior of your computing system. That way you will be able to identify any abnormal behavior. You will be aware of "strange and unexplained" things that might happen. These include:

- Unexpected disk accesses
- Unexpected new files
- Unexplained increased disk space usage
- Unexplained open applications
- Unexplained printouts
- Unexplained sluggishness on your system

These things might be the result of normal operation or they may signal an intruder. Intruders and intruder software can operate, if attempted by a skillful attacker, with little consumption of resources. Learn how your computer system generally reacts and identify abnormal behavior.

Incident Reporting

If you suspect an intrusion of your system has occurred:

- Don't panic.
- Contact your CSPR immediately. Every minute that passes provides more opportunity for the intruder to damage your computer, to use your computer to damage other computers, or allow time for others to find and exploit your vulnerability.
- Leave the computer ON.
- Do NOT modify any files.
- Do NOT close any applications.
- Start making notes of your discoveries and activities. Do not use a possibly compromised system to take notes or communicate about the suspected break in.
- Quarantine the system (leave it on with a sign on the monitor to warn against further use)

Reputable Sources
Only accept computer instructions from reputable sources like your system administrator or CSPR
Do not attempt to take care of the virus yourself. Far more damage to systems results from users trying to eradicate viruses and worms by themselves than from anything else.

Deterring Computer Theft

On average, 4 laptops are stolen from employees' hotel rooms and cars every year. Even here at Argonne, buildings with large common areas regularly experience the theft of components such as keyboards and mice.

For desktop computers:

- Use simple key locks with strong surface mount adapters to prevent equipment theft. Lock your office or lab when your computer is unattended for a significant amount of time.
- Turn on the computer software lock feature when you leave your computer for any reason.

For laptop computers:

- Notebook users must be particularly careful on travel. Airports and hotel lobbies are notorious venues for computer theft.
- Turn on Full Disk Encryption (FDE). This technology protects Argonne data if your device is lost or stolen. Contact your CSPR for assistance with FDE.
- Purchase Kensington or Kryptonite lock down cables. Do not save passwords that allow automatic login to systems/websites/intranet sites. This prevents unauthorized access to these areas in the event of computer theft.
- If you travel with your laptop in your car, store it in your trunk and not visible in the seat. Argonne employees' laptops have been stolen from their cars while parked in their driveway and hotel parking lots.
- When on travel for Laboratory business or pleasure, never let the laptop leave your sight including airport security checkpoints.

Data Restoration

Data loss can occur for multiple reasons, so a critical part of cyber security is the ability to restore a user's environment and data. Divisions have retention policies on how long backups are kept. Your environment and data should be part of a regular and reliable backup strategy that is to be used for disaster recovery only. Verify that backups are taking place and that your CSPR is aware of your computing environment and data needs. This may involve:

- A local backup of your computer.

- A general file system strategy for your organization.
- Storing your files in an approved cloud storage location like Box.com.

The backup strategy for your data must consider how quickly your environment must be restored and whether the data or system is sensitive or critical and so required to remain confidential or available.

Information Technology Access Agreement

This course covered several principles that govern the use of Argonne Information Technology (IT) assets.
The Argonne National Laboratory Information Technology Access Agreement (ANL-714) is a concise list of these principles and policies. By taking this course, you will be expected to comply with and abide by the conditions of the agreement as well as follow all policies set forth in the Cyber Security Program Plan (CSPP).

Please open and review both documents. Direct links are provided on the last page of this document.

Data Awareness Survey

*Please fill out the survey and fax it back to the **Argonne Cyber Security Office at (630) 252-9689**.*

Name: _____

Signature_____

Badge: _____ Division: _____ Date: _____

In your responsibilities at the Laboratory, do you work with the following types of sensitive data in electronic form?

- ☐ Personally Identifiable Information (PII)
- ☐ Export Controlled Information (ECI)
- ☐ CRADA/WFO
- ☐ Unclassified Controlled Nuclear Information (UCNI)

If you do work with the data types described above, please identify where the data is stored.

- ☐ Laboratory Desktop Computer System
- ☐ Laboratory Laptop Computer System
- ☐ Divisional File Share
- ☐ Laboratory Business Systems
- ☐ Removable Media
- ☐ Personally Owned Computer System
- ☐ Box (Cloud Storage System)

If you DO NOT work with any of the above, please check the following checkbox.

- ☐ I do not work with any of the above.

Helpful Links and Resources

- ANL-714 - Argonne National Laboratory Information Technology Access Agreement
  https://my.anl.gov/esb/view/STELLENT/ANL-714
- CSPP - Cyber Security Program Plan
  https://my.anl.gov/esb/view/STELLENT/567228
- Box Info Page
  https://my.anl.gov/app/box
- CASPIR Reps (Critical Program Information Coordinators)
  https://my.anl.gov/contact/isaac-critical-program-information-coordinators
- Classification Services
  https://my.anl.gov/sas/service/classification-services
- Cyber Security Program Office (CSPO) / Cyber Security Web Page
  https://my.anl.gov/bis/service/cybersecurity
- Cyber Security Representatives (CSPR)
  https://my.anl.gov/contact/r2a2-cyber-security-program-representatives
- Dash Web Page
  https://my.anl.gov/app/dash
- LMS-POL-19 - Protection of National Security and Other U.S. Interests
  https://my.anl.gov/esb/view/STELLENT/LMS-POL-19
- LMS-POL-26 - Employee Conflict of Interest
  https://my.anl.gov/esb/view/STELLENT/LMS-POL-26
- LMS-POL-44 - Limited Personal Use of Argonne Resources
  https://my.anl.gov/esb/view/STELLENT/LMS-POL-44
- LMS-POL-51 - Employee Conduct
  https://my.anl.gov/esb/view/STELLENT/LMS-POL-51
- LMS-PROC-22 - Protection of Controlled Unclassified Information
  https://my.anl.gov/esb/view/STELLENT/LMS-PROC-22
- Password Info
  https://servicenow.anl.gov/pr
- Publication Approval Notification and Distribution Application (PANDA)
  https://my.anl.gov/app/panda
- Scitech 1 – 8
  https://my.anl.gov/esb/view/STELLENT/SCITECH-1
- Snopes
  https://www.snopes.com/