

Instructions:

1. PRINT legibly, use BLACK INK --- stay inside the boxes
2. VERIFY Header information is complete and correct
3. Complete Badge No. field at bottom; Sign & Date

Index No. PX-3864-UNC
 Page No. 1 of 1
 Issue No. 020



Training Completion Report

(Ref. WI 02.03.02.03.03. WI 02.03.02.03.05, WI 02.03.02.03.06)

Employee Name _____

Badge No.

--	--	--	--

OR

LMS No.

--	--	--	--	--	--

Item Name

Computer Code of Conduct
Statement

Item No.

		7	5	.	3	1
--	--	---	---	---	---	---

Item Type

C	B
---	---

Item Revision Date

0	2	2	5	0	9
<small>M</small>	<small>M</small>	<small>D</small>	<small>D</small>	<small>Y</small>	<small>Y</small>

Test Version

1	2	0	1	1
---	---	---	---	---

Instructor Badge No.

--	--	--	--	--

Score

--	--

Complete

X	
<small>Y</small>	<small>N</small>

RIDS

B

Workflow Route No.

--	--	--	--	--	--

TSR-Related?

	X
<small>Y</small>	<small>N</small>

I am aware that use of Pantex computing resources is not a guaranteed right. By signing this document, I acknowledge and confirm that I will:

Use Pantex computer resources, including copiers, for official Department of Energy/National Nuclear Security Administration (DOE/NNSA) business only, unless the Information System Security Site Manager (ISSM) has given me written authorization to do otherwise, or the use is specifically approved in the Cyber Security Resource Manual, MNL-00070, or Cyber Security Work Instructions.

Use my access authorization appropriately, comply with individual responsibilities and operating rules listed in the security plan for a classified or unclassified system(s) or application(s) to which I have been given access.

Protect my password, never reveal it to anyone or write it down, and use only passwords that meet the guidelines in MNL-00070. I will change my password and contact the Cyber Hotline at ext. 7060 if I know or suspect it has been compromised (revealed).

Remain aware that my use of any Pantex computer resources is monitored and that there is no expectation of privacy of any information that I create, process, transmit or store, including email that I send or receive internally or via the Internet.

Understand that my account on any system can be suspended without notice if I do not log on for a period greater than 90 days, fail to keep mandatory cyber security training current, or fail to adhere to cyber security requirements.

Use only government-owned software and not introduce unauthorized or personal software, including screensavers, into the Pantex computing environment.

Not reconfigure or otherwise alter the Pantex standard image as installed on my system. Not use audio recording capabilities on any computing system.

Accept my responsibilities to protect classified and sensitive unclassified information (i.e. Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), Export Controlled Information (ECI), Privacy Act, Personally Identifiable Information (PII)) that I access or control, in accordance with DOE/NNSA requirements to protect information vital to the security of our nation, our work, and our personal identities.

Not electronically transmit information off Plant site unless it is protected as follows:

- Classified: **ENCRYPTED** via the SecureNet classified system.*
- UCNI: **ENCRYPTED** using the DAA-approved application.*
- OUO: **ENCRYPTED** using the DAA-approved application.*
- PII: **ENCRYPTED** using the DAA-approved application.*

*I will use only DAA-approved encryption tools when sending encrypted files.

Not knowingly introduce classified information to the unclassified network or other unclassified systems. Have a Derivative Classifier review all information with the potential to contain classified information, **prior to** processing the information on an unclassified computer (especially when combining two or more unclassified documents).

Contact the Pantex Classification Officer if I need to download or transfer unclassified information off a classified system.

Update the Pantex Property System (PPS) with all prospective security significant changes to the computer system assigned to me **before** making such changes.

Report cyber security issues or incidents, including viruses, to the Cyber Hotline at ext. 7060.

Virus scan all incoming removable media such as vendor software, before use on Pantex computer resources, and report to Cyber Help any problems or anomalies with my desktop virus protection software.

I acknowledge that failure to comply with any Cyber Security requirement will subject me to a Cyber Security incident and disciplinary action.

Badge No. (or LMS No.)

--	--	--	--	--	--

Employee Signature

Training Completion Date

<small>M</small>	<small>M</small>	<small>D</small>	<small>D</small>	<small>Y</small>	<small>Y</small>