U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Integrated Source Management Portfolio (ISMP) Security Awareness Training

ISMP Security Awareness Training

Introduction

Welcome to security awareness training for the Integrated Source Management Portfolio (ISMP). The information contained in this course is provided to inform ISMP Users of their responsibilities with regard to computer security while using ISMP.

This training is required by the Office of Management and Budget (OMB) under OMB Circular A-130 and the Nuclear Regulatory Commission (NRC) Office of Nuclear Material Safety and Safeguards (NMSS).

The course covers NRC policy on the authorized use of ISMP. The practices described in this course are designed to protect ISMP and ISMP information from unauthorized disclosure, alteration, or destruction.

You will be required to provide a digital acknowledgement of your understanding of the ISMP Rules of Behavior.

If you have any questions, please contact the **ISMP Helpdesk** at **1-877-671-6787**.

ISMP Security Awareness Training

Contents

- Attitudes & Fallacies
- IT Security Threats
- IT Security Measures
- Information Security
- System Use Message
- Rules of Behavior
- Best Practices

ISMP Security Awareness Training

Attitudes & Fallacies

Common Attitudes and Fallacies:

- The security or system staff take care of security.
- Nobody WANTS my authenticators (e.g., PIN, digital certificate, hard token).
- It is MY machine.
- Security is NOT my priority.

Attention: Security is everyone's responsibility!

ISMP Security Awareness Training

IT Security Threats

Two categories of IT security threats that ISMP Users should be aware of are:

- Illegal System Access
- Viruses and Malicious Software

Unauthorized users access the system by:

- Using an authorized user's login credentials
- Hacking into the system

Authorized users may also try to exceed their authorized level of access and hack into other's resources.

ISMP Security Awareness Training

IT Security Threats (cont.)

What is a computer virus?

- A virus is a program that copies itself to other programs or files.
- A virus is just one type of malicious software.

Other Types of Malicious Software

- Trojan – Disguised as a legitimate program, Trojans can create back doors to a system.
- Time Bomb – Code on a computer that triggers some damaging event at a particular time.
- Logic Bomb – Triggered by a particular event and behaves as a virus.

ISMP Security Awareness Training

IT Security Measures

ISMP Users must be aware of the following IT security measures that are implemented to protect ISMP from IT Security Threats:

- Strong authentication
- Cryptography
- ISMP User Responsibilities and Rules of Behavior

Types of Authenticators

- Digital Certificate: the digital equivalent of an ID card. Also called a digital ID, digital identity certificate, and public key certificate.
- Hard Token: a hardware security device that is used to authenticate a user (e.g., a smart card).
- One Time Password (OTP): a hardware security device providing Validated ID Protection used to authenticate a user (e.g., a security token).
- Personal Identification Number (PIN): a number used to confirm a user's identity when using a hard token.
- Password: a string of characters that is entered into a computer system to gain access to a resource.

ISMP Security Awareness Training

IT Security Measures (cont.)

Strong Authentication

Access to ISMP requires strong authentication using:

- NRC ICAM-issued digital certificates stored on NRC ICAM-issued hard tokens. (ICAM is identity, Credential and Access Management)
- Digital certificates and hard tokens are PIN-protected.
- One Time Password (OTP) and PIN.

Cryptography

Key Terms:

- Encryption is the process of encoding messages or information in such a way that only authorized parties can read it.
- Federal Information Processing Standard Publication 140-2 (FIPS 140-2) is a U.S. government computer security standard used to accredit cryptographic modules.
- An encrypted connection is established between the ISMP User and ISMP to protect ISMP data while it is transmitted over the internet.
- FIPS 140-2 compliant cryptography must be used. Additional details are provided in the Rules of Behavior.

ISMP Security Awareness Training

IT Security Measures (cont.)

ISMP User Responsibilities and Rules of Behavior

- To ensure the secure access and use of the system, ISMP Users are responsible for implementing security measures on their computer and local environment.
- The ISMP Rules of Behavior define these measures and responsibilities.

ISMP Security Awareness Training

Information Security

- ISMP information is categorized as Sensitive Unclassified Non-Safeguards Information (SUNSI).
- SUNSI must not be viewed or accessed inadvertently or willfully by a person who is not authorized access.

ISMP Security Awareness Training

System Use Notification Message

The ISMP System Use Notification Message is displayed to the user prior to each login attempt.

The message informs the user that by using the system, he/she agrees to the following:

- Consent to monitoring.
- No privacy expectations.
- Penalties for unauthorized access or misuse of system and system data.

ISMP Security Awareness Training

Rules of Behavior

The ISMP Rules of Behavior establish a set of rules that describe ISMP resident application user responsibilities and expected behavior with regard to information and system usage.

The ISMP Rules of Behavior cover the following:

- Applicability
- Consequence for Noncompliance
- General Protections
- NRC Identity, Credential, and Access Management (ICAM)
- Authenticators
- User Desktops and Laptops

ISMP Security Awareness Training

Best Practices

Authenticators

When selecting a PIN, users should avoid using the following:

- Your name, nickname, or initials
- Your user identification code or name (user ID)
- Special dates
- Your spouse or child's name
- Your telephone number, employee number, or social security number
- Anything that can be easily associated with you
- Consecutive or repeated numbers or letters (ABCDE, CCCCC, 123456, 88888)
- Dictionary words

Us3$tr0ngP@&SwOrd$!

ISMP Security Awareness Training

Best Practices

Authenticators (cont.)

- Sharing authenticators is prohibited.
- Never disclose or write down PINs.
- Remember to:
  - Protect yourself from misuse or abuse, protect your authenticators.
  - Report compromised authenticator incidents.

Others

- Cut and paste internet addresses from email messages into browsers instead of clicking links provided in the message.
- Do not download attachments, files, or programs from unknown sources.
- Never supply personal information to unknown addresses.
- Do not download shareware, freeware, or other programs.
- Contact the ISMP Helpdesk for suspected virus or malicious code incidents.

ISMP Security Awareness Training

CONGRATULATIONS

This completes ISMP Security Awareness Training.