WITS Prevention Data Stewardship

Thursday, November 30, 2023 | 9:00 am

I. Welcome and Overview

II. Data Security

III. SSRS Reports
   a. New Report: Number of Individual Participants – Education Strategy
   b. Questionnaire due by Friday, December 8th

IV. Questions and Answers

V. Reminders
   a. Community-based Strategies: One-Time vs Recurring
   b. WITS Crosswalk guidance document

VI. Quarterly Meetings, 9:00-11:00 am
   a. November 30, 2023
   b. February 29, 2024
   c. May 30, 2024
   d. August 29, 2024

VII. Closing

TIPS TO IMPROVE DATA SECURITY

November 30, 2023

Prepared for prevention data stewardship meeting

University of Hawaii Center on the Family

OVERVIEW

- Definition of data
- When and why data security matters
- Which information should be protected
- Actions steps with recommendations

Q1. WHAT ARE CONSIDERED DATA? (CHECK ALL THAT APPLY)

- A. A participant's name written on a sticky note at work
- B. Conversation about a participant's behavior
- C. Information entered or retrieved from WITS
- D. A group photo from a prevention program

DEFINITION OF DATA

- Any items of information in **electronic, paper or other format**.

WHEN AND WHY DATA SECURITY MATTER

- WHEN: Personally identifiable information (PII) is involved
- WHY: To be in compliance with federal, state, and local laws and policies. A data breach has great potential to harm individuals.
- Data protection is an organizational obligation; consequences can be severe if violated.

DATA SECURITY
(SOURCE: HTTPS://WWW.NCCOE.NIST.GOV/DATA-SECURITY)

- **Data Security:** “Process of maintaining the confidentiality, integrity, and availability of an organization’s data in a manner consistent with the organization’s risk [management] strategy. Before an incident happens, companies must have a security architecture and response plan in place”

Q2. WHICH INFORMATION SHOULD BE PROTECTED? (CHOOSE ALL THAT APPLY)

- A. DOB (MM/DD/YYYY)
- B. Student ID number
- C. First name initial and last name
- D. Handwriting
- E. Mother’s maiden name

WHAT IS PERSONALLY IDENTIFIABLE INFORMATION?
SOURCE: NIST HTTPS://CSRC.NIST.GOV/GLOSSARY/TERM/PII

- “Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.”
- “Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”

WHAT IS PII? (CONT.)
SOURCE: NIST HTTPS://CSRC.NIST.GOV/GLOSSARY/TERM/PII

- “Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.”

PII (PERSONALLY IDENTIFIABLE INFORMATION)

- Direct PII: Directly identifies an individual
  - e.g., name, address (both street and email), phone number,VIN, login credentials, IP (Internet Protocol) address, MAC (Media Access Control)
- Indirect PII & Identifiability: Identify specific individuals in conjunction with other data elements

Q3. CHOOSE BEHAVIORS THAT MAY POSE SECURITY RISKS

- A. Keep a flash drive that contains sensitive data in a desk drawer (people cannot see but can access)
- B. Temporarily keep confidential data on a personal laptop to work during PTO
- C. Share your login credentials with your colleague
- D. Use a free wifi connection in a hotel room to access the WITS during a business trip

ACTION STEP #1: ESTABLISH PHYSICAL SECURITY CONTROLS

- Recommendation #1: Storing devices in rooms requiring key access.
- Recommendation #2: Storing portable devices (e.g., flash drive) and hardcopies in a locked cabinet within a key-access room.

ACTION STEP #1: ESTABLISH PHYSICAL SECURITY CONTROLS (CONT.)

- Recommendation #3: Do not travel with data if possible

  If you must

  - Do not leave hardcopies or devices unattended
  - Do not make any unnecessary stops
  - Enable a remote wipe function if possible
  - Make sure BitLocker is on

ACTION STEP #1: ESTABLISH PHYSICAL SECURITY CONTROLS (CONT.)

- Recommendation #4: Visitation policies
- Recommendation #5: Use a privacy screen filter if necessary
- Recommendation #6: Do not print unless absolutely necessary
  - It is best not to print out any confidential information
  - If must, retrieve printed documents containing personal data immediately after they have been printed

ACTION STEP #1: ESTABLISH PHYSICAL SECURITY CONTROLS (CONT.)

- Recommendation #7: Use a shredder
  - Make sure to keep track of hard copies and completely destroy them as soon as you are done using it

ACTION STEP #2: ESTABLISH RULES ON DATA STORAGE

- Recommendation #1: The original confidential data will only be stored on the organization-owned encrypted device
  - e.g., BitLocker https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d

ACTION STEP #2: ESTABLISH RULES ON DATA STORAGE (CONT.)

- Recommendation #2: Confidential data should not be downloaded or stored on another device.
- Recommendation #3: Create a list of devices, i.e., the asset inventory.

Asset Type	Asset Nick Name	Make	Model	Serial/ Tag Number	Owner	Data
Workstation	AB's work desktop	Dell	XPS 1234	123ABC	Ash Brown User	
Laptop	TS's work laptop	Dell	XPS 17 5678	456DEF	Tom Smith User	
Flash Drive	Encrypted Green	Kingstone Encrypted	IronKey D500S	N/A	DOH	
Network Share Drive	Name of shared folder	Dropbox Enterprise	Shared Folder	N/A	DOH	

ACTION STEP #3: ESTABLISH RULES ON DATA ACCESS

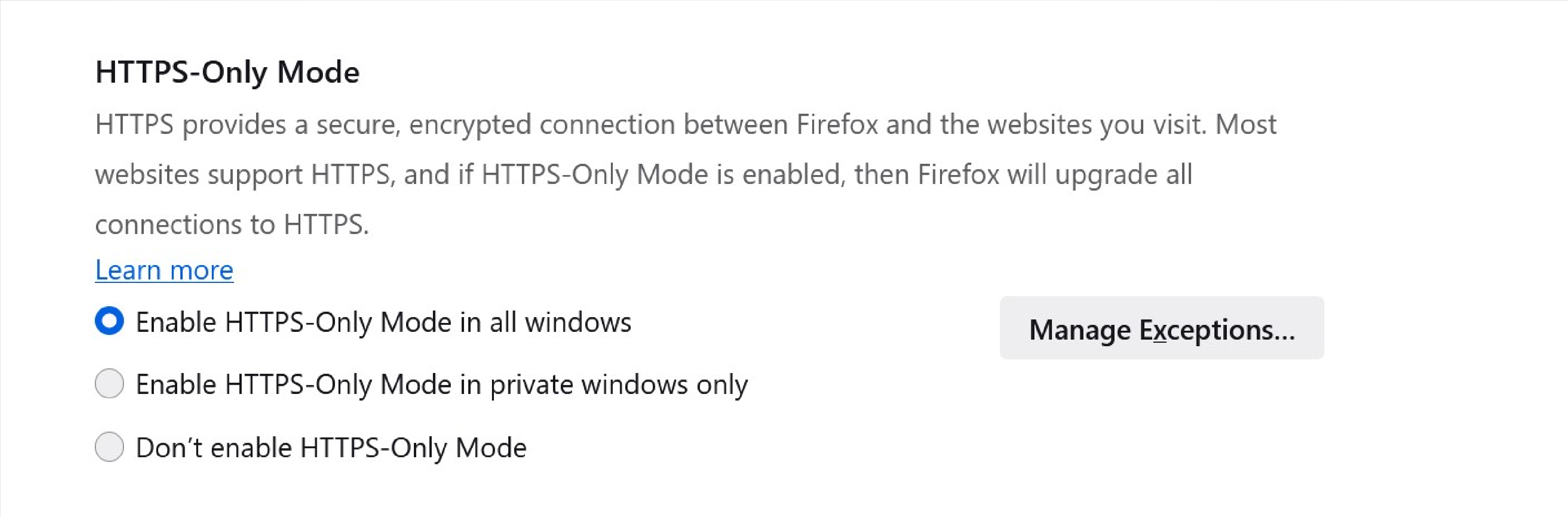
- Recommendation #1: Develop data access policy ("specify how access is managed and who may access information under what circumstances." by NIST https://csrc.nist.gov/glossary/term/access_control_policy)
- Recommendation #2: Follow the principle of least privilege
- Recommendation #3: Always complete data security training before access data

ACTION STEP #4: ESTABLISH DAILY PRACTICE POLICY

- Recommendation #1: ALWAYS install and timely update Antiviral Software
- Recommendation #2: ALWAYS update your operations systems and do not use any device that is no longer supported and at a security risk
- Recommendation #3: Use secure network connection only
    - Make sure the network connection is encrypted
    - Do not share your organization password with guests
    - NEVER use open access network when access data or update software

ACTION STEP #4: ESTABLISH DAILY PRACTICE POLICY (CONT.)

- Recommendation #4: Do not charge your device with public USB ports or public charging cables
- Recommendation #5: Do not access suspicious websites, even for work purposes
  - HTTP is not secure. Enable HTTPS-only mode if possible.



HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.

Learn more

● Enable HTTPS-Only Mode in all windows

○ Enable HTTPS-Only Mode in private windows only

○ Don’t enable HTTPS-Only Mode

ACTION STEP #4: ESTABLISH DAILY PRACTICE POLICY (CONT.)

- Recommendation #5: If anyone who handles PII data is allowed to telework, it is important for you to establish an appropriate telework security policy (e.g., use a VPN).
- Recommendation #6: Establish a login policy
  - Individual login credentials (do not share)
  - Automatic logout after inactivity

ACTION STEP #4: ESTABLISH DAILY PRACTICE POLICY (CONT.)

- Recommendation #6: Login policies (cont.)
  - Strong password requirements
    - Passwords must be 14-32 characters long;
    - Passwords contain one uppercase character, one lowercase character, one number, and one special character.
  - Do not use the same password you use elsewhere

Q4. WHICH BEHAVIORS MAY BE POTENTIALLY RISKY? (CHOOSE ALL THAT APPLY)

- A. Emailing a screenshot to the WITS Help Desk to seek assistance
- B. Providing participants' information via email to a colleague who works for the same organization
- C. Providing PII over the phone to a third party that is entitled to such information (e.g., WITS Help Desk)
- D. Sending PII via fax to a third party that is entitled to such information (e.g., WITS Help Desk)

REMINDER: END-USERS

- Recommendation #1: Email is not secure - Do not send sensitive PII via email without encryption
- Recommendation #2: If your device is shared, (1) sign out of the computer once your session is complete to prevent unauthorized access and (2) do not enable the auto login function (e.g., saved password)

REMINDER: END-USERS (CONT.)

- Recommendation #3: Do not post any work related information on social media (not even a group photo unless you have consents from participants)
- Recommendation #4: Do not use work devices for personal use

ACTION STEP #5: HIRING, TERMINATION, ROLE CHANGE

- Recommendation #1: Make sure a new employee gets necessary training before allowed to handle personal information
- Recommendation #2: Disable all relevant accounts on the last day of hire
- Recommendation #3: Always review the current access privilege when a role is changed

ACTION STEP #6: SECURITY INCIDENT AND REPORT

- Recommendation #1: Develop an incident response plan if your organization handles confidential data