`

National Assessment of Educational Progress

Web/Technology Development, Operations, and Maintenance (WTDOM)

Rules of Behavior for the NAEP System

1. INTRODUCTION

All users of the systems and applications belonging to the National Assessment of Educational Progress (NAEP) program at the National Center for Education Statistics (NCES), United States Department of Education, and hosted or maintained by the WTDOM contractor ("NAEP Sites") must acknowledge the following rules of behavior.

2. RULES

Use NAEP computing resources only for official Government business. These rules have been issued pursuant to Federal law and regulations.

1. Know the sensitivity of the information processed on NAEP computing resources (e.g., financial sensitive, Privacy Act sensitive).
2. Use NAEP software, hardware, and data only in compliance with licensing agreements and which has been authorized for use by NAEP.
3. Store no personally identifiable information or any sensitive information on the NAEP System unless authorized by NAEP.
4. Protect sensitive information, in storage, in transit, or in use, from access by, or disclosure to, unauthorized personnel.
5. Report immediately all security incidents and potential threats and vulnerabilities involving the NAEP System to security@naepims.org.
6. Create and use strong passwords and do not disclose your password to anyone. Users should lock their computers before leaving them unattended, and should arrange to have them lock automatically after a reasonable period of inactivity.
7. Report any compromise or suspected compromise of a NAEP System password to security@naepims.org.
8. Access only systems, networks, data, and software for which you have been authorized and have the appropriate clearance. When you no longer require access to one or more applications or to NAEP System, notify your IMS champion or, if you don't have one, contact security@naepims.org.
9. Ensure that system media and system output are marked according to their sensitivity and are properly controlled and stored.
10. Take necessary steps to avoid the introduction of malicious code into any computing resource.
11. Exercise due diligence to prevent physical damage to and theft of any NAEP computing resource.

3. SENSITIVITY OF INFORMATION

It is easy for computer system users to think that only classified or highly sensitive information requires protection from unauthorized disclosure. Furthermore, it is also quite easy for users to assume that

once data leaves the computer, (i.e. is printed or viewed on a computer screen); it somehow does not require the same protection level. However, according to guidance from the National Institute of Standards, all data, with the exception of the trivial, requires some level of protection.

The Federal Information Security Modernization Act (FISMA) of 2014 (P.L. 113-283) was enacted to create " a comprehensive framework for ensuring the effectiveness of information security controls over information resources" for federal unclassified computer systems. The Act also emphasizes that all federal information requires protection against unauthorized modification or destruction, as well as unauthorized disclosure.

The Computer Security Act of 1987 (P.L. 200-235), which FISMA supplements, provides a very broad definition of sensitive information:

“Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.”

Based on the above definition, it is not hard to see that NAEP data needs to be treated as sensitive information in accordance with the Computer Security Act and protected accordingly. In addition, some portions of NAEP data fall under the category of Privacy Act Data (protected under the Privacy Act) and financial information (protected under the Federal Manager’s Financial Integrity Act).

As a result of these requirements to protect all NAEP data (not just data stored on the Fulcrum NAEP computer systems), NAEP reports need to be treated as sensitive data and given appropriate protection. Examples of this protection include:

- Lock up reports and computer media containing sensitive data when you leave your work area;
- Clear reports off your desk or lock your office door while you are away from your desk or at the end of the day;
- Ensure that reports or your computer screen are not visible to others/visitors when viewing/entering sensitive information (like your passwords);
- Store reports/data in binders or folders so that others do not easily see them;
- Discard sensitive information in such a way that unauthorized individuals cannot recover the data (Printed reports should be finely shredded, while data on magnetic media should be overwritten or shredded);
- Lock your workstation when away and utilize the a password protected screen saver feature;
- Do not leave sensitive documents stranded or orphaned at the printer or fax machine. If you are printing a sensitive document or receiving a fax, remember to check the printer or fax machine often.

- Label sensitive data and reports appropriately to ensure that they are handled properly. For example: computer media should be labeled “For Official NAEP Use Only.”