

Approved: 11-23-99

Expires: 7-1-00

**SUBJECT: PASSWORD GENERATION, PROTECTION, AND USE**

---

1. **OBJECTIVE.** To establish minimum requirements for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified Department of Energy (DOE) information systems.
2. **CANCELLATION.** DOE M 471.2-2, Chapter VI, Paragraphs 4j(2), and 4j(6); also Chapter VII, Paragraph 12a(2)(a). All remaining provisions of DOE M 471.2-2 remain in effect.
3. **APPLICABILITY.**
  - a. This Notice applies to all DOE elements requiring access to classified and unclassified DOE information systems.
  - b. The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements to be applied to DOE contractor and sub-contractor organizations requiring access to classified and unclassified DOE information systems.
4. **REQUIREMENTS.**
  - a. All classified and unclassified DOE multi-user information systems, desktops, and laptops—excluding Personal Digital Assistants (e.g., “Palm Pilots”) and those information systems intended to provide unrestricted public access (e.g., public web servers)—must have and use a password mechanism that authenticates the identity of each person accessing the DOE information system. DOE organizations operating classified information systems shall continue to use automatic password generation software as required by DOE M 471.2-2, Chapter VI, Paragraph 4j(3).
  - b. DOE site managers and Lead Program Secretarial Officers (LPSOs) must designate an individual for each DOE organization who is responsible for the implementation of this policy.
  - c. Each DOE organization must develop, implement, and document in its computer security program plan (CSPP) a password policy commensurate with the level of

---

**DISTRIBUTION:**  
All Departmental Elements

**INITIATED BY:**  
Office of Security  
and Emergency Operations

security required for the organization's environment and specific needs. DOE organizations must address the guidance provided in DOE G 205.3-1 and issue clear instructions to their users regarding password standards. Deviations from DOE G 205.3-1 must be documented in an organization's CSPP.

- d. All DOE organizations are required to have a plan to eliminate the use of clear text reusable passwords, and they must include this plan, with schedule and milestones, in their respective CSPPs.
6. CONTACT. Questions concerning this Notice should be addressed to the Office of the Chief Information Officer, at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:



DAVID M. KLAUS  
DIRECTOR OF MANAGEMENT  
AND ADMINISTRATION

**CONTRACTOR REQUIREMENTS DOCUMENT**  
**DOE N 205.3, PASSWORD GENERATION, PROTECTION, AND USE**

The contractor is required to ensure that the following actions and directions are implemented and complied with to the extent technically feasible.

1. Each Department of Energy (DOE) contractor must ensure that all classified and unclassified DOE multi-user information systems, desktops, and laptops under its purview—excluding Personal Digital Assistants (e.g., “Palm Pilots”) and those information systems intended to provide unrestricted public access (e.g., public web servers)—have and use a password mechanism that authenticates the identity of each person accessing the DOE information system.
2. Each DOE contractor operating classified information systems shall continue to use automatic password generation software as required by DOE M 471.2-2, Chapter VI, Paragraph 4j(3).
3. Each DOE contractor must designate an individual to be responsible for implementation of this policy.
4. Each DOE contractor must develop, implement, and document in its computer security program plan (CSPP) a password policy commensurate with the level of security required for the organization’s environment and specific needs. DOE contractors must follow the guidance provided in DOE G 205.3-1, PASSWORD GUIDE, and issue clear instructions to their users regarding password standards. Deviations from DOE G 205.3-1 must be documented in an organization’s CSPP.
5. Each DOE contractor is required to have a plan to eliminate the use of clear-text reusable passwords, and they must include this plan with schedule and milestones in their respective CSPPs.

## DEFINITIONS

**Multi-user System.** A system that under normal operations has more than one user accessing it simultaneously. Systems accessed by more than one user sequentially (i.e., by one user at a time) without undergoing the necessary procedure to remove residual data between users; are also considered multi-user systems.

**Reusable Password.** A data item associated with a user ID that remains constant and is used for multiple access requests over some explicit time interval.

**Special Character.** Any non-alphanumeric character.