JUL 1 2 2018

Approved for Release
Kevin E. Mahoney
Director for Human Resources Management and
Chief Human Capital Officer

7-12-18
Date

**DEPARTMENT OF COMMERCE**
**OFFICE OF HUMAN RESOURCES MANAGEMENT**

**HUMAN RESOURCES (HR) BULLETIN #225, FY18**

**SUBJECT:** Procedures, Roles, and Responsibilities on Providing Access to Historical webTA Data via ArchiveTime

**EFFECTIVE DATE:** Upon release of this HR Bulletin

**SUPERSEDES:** None

**EXPIRATION DATE:** Effective until superseded or revoked

**PURPOSE:** This bulletin provides guidance on the procedures, roles, and responsibilities for those responsible for providing access to the ArchiveTime system.

**BACKGROUND:** The ArchiveTime system stores historical webTA data. It has some of the same roles for users as does webTA, the web-based time and attendance system of the Department of Commerce (Department). Each Servicing Human Resources Office (SHRO) is responsible for determining how ArchiveTime is accessed by HR employees. Once determined, it is the responsibility of the SHRO to grant access to ArchiveTime as appropriate, including adding new employees to the ArchiveTime application to allow them to adequately view time and attendance data. To accomplish this, each SHRO must assign at least one primary and one secondary ArchiveTime user to serve as the SHRO ArchiveTime Security Officers. The designated personnel will have administrative access to ArchiveTime and be responsible for providing access to the ArchiveTime system.

**PROCEDURES:** It is the responsibility of the SHROs to:

- Assign at least one primary and one secondary ArchiveTime Security Officer from the SHRO to ensure that security functions can continue if the primary ArchiveTime Security Officer is unavailable.

- Inform the Department's ArchiveTime Security Program Manager (via the NAccess@doc.gov mailbox) of any changes in personnel assigned to be ArchiveTime Security Officers. Notification must be provided within 5 business days of the change. The Department's ArchiveTime Security Program Manager will keep a list of all active ArchiveTime Security Officers.

ArchiveTime Security Officers are required to:

- Keep a record of the HR employees they provided system access to. Information to be recorded include: name, user ID, date access was granted, and the level of access. This record must be made available to the Office of Human Resources Management, auditors, and other authorized persons upon request.

  Note: Currently, ArchiveTime does not have access reporting in the system, thereby making this requirement a necessity. If/when an access report-generating capability has been added to ArchiveTime, this requirement will be re-examined, as authorized personnel will be able to obtain this information from ArchiveTime directly.

- Conduct internal review audits of all ArchiveTime accesses currently in effect (the re-certification process), semiannually, at the end of Q1 and Q3, to ensure that the level and scope of access is still valid and required, and to resolve issues found in the audit.

- Provide security awareness information to all employees who receive ArchiveTime user accounts, including supplying and receiving signatures on a Rules of Behavior form, which includes informing employees that they must keep their user accounts safe and not divulge their passwords.

- Ensure that procedures are in place to immediately remove ArchiveTime access for users who have separated or transferred out of the security officers' area of responsibility; ensure that removal of access has been confirmed and recorded, and that documentation has been retained.

- Adhere to security rules prohibiting users from making security-access changes to one's own user account.

- Provide access only for authorized functions assigned to you and your bureau/operating unit.

- Ensure procedures are in place that allow for password resets and unlocking of accounts for users upon request.

**ACCOUNTABILITY:**

- SHROs are required to provide validation that they have performed the required internal review audits (the re-certification process) by sending an e-mail to the NAccess@doc.gov mailbox. The validation must consist of a narrative explaining the results, which includes at a minimum:
  - Who performed the audits;
  - When they were performed;
  - What was audited: that is, a complete list of all supervisors, timekeepers, and administrators who were checked; and the bureau(s)/Personnel Office Indicator(s) that were checked; and
  - What issues were resolved.

- The validation and results narrative must be completed by the 15th calendar day after the end of the quarter (i.e., January 15 for Q1, and July 15 for Q3) or the next business day if the 15th falls on a non-business day. Send it to the NAccess@doc.gov mailbox.

- The Department's ArchiveTime Security Program Manager will review the validation submissions to ensure that all procedural requirements have been satisfied, and to look for systemic issues that need to be addressed either Department-wide or within an SHRO.

**REFERENCES:** Not applicable

**OFFICE OF POLICY AND PROGRAMS:** Valerie Smith, Director, vsmith@doc.gov, (202) 482-0272

**PROGRAM MANAGER CONTACT INFORMATION:** James Hoebel, JHoebel@doc.gov, (202) 482-6372