ITA Publication No.: CIO 19-G-SEC-003	Effective Date: 5/XX/2019
Revision Date: N/A	

ACCOUNT ACCESS GUIDANCE

1. PURPOSE

To provide International Trade Administration (ITA) Account Access guidance.

2. BACKGROUND

Title I of the Federal Electronic Communications Privacy Act of 1986 (18 United States Code (USC) Sections 2510, 2701, and 3121) states that any workplace correspondence[1] on a government[2] device is the property of the employer. At ITA, any government-furnished equipment supplied to an employee is the property of ITA and shall be used for authorized purposes or according to guidance in the limited personal use policy. Accessing an employees' account may be needed to secure evidence in the case of a lawsuit or the government may want to monitor the e-mails of an employee suspected of sending proprietary or inappropriate information[3] to outside agencies. The Account Access Policy protects ITA from legal liability, reputation damage, and potential security breaches and can be used as a mechanism for ensuring that the workplace is free of harassment. This guidance provides the instances that warrants accessing an employees' account and the steps for obtaining authorization.

3. SCOPE AND APPLICABILITY

This guidance applies to all employees of ITA including contractors.

4. GUIDANCE

ITA has the right to monitor the employees' use of their accounts and must ensure that all personnel who use these accounts are aware of this fact. Upon logging on to any ITA computer system, all employees are informed that usage may be monitored, recorded, read,

[1] "Correspondence" refers to any written form of communication (paper or electronic media) including letters, notes, memoranda, and e-mail.

[2] "Government" in this document refers to any information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

[3] "Information" is a communication or representation of knowledge such as facts, data or opinions, including, but not limited to, numerical, graphic or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, magnetic tape, etc.

Figure 1 – Department of Commerce International Trade Administration Login Banner

copied, and disclosed by and/or to authorized personnel for official purposes, including criminal investigations (Figure 1) and that there is no expectation of privacy[4]. Access or use of the ITA computer system by any person, whether authorized or not, constitutes consent to these items.

There is a myriad of specific instances for Directors, Supervisors, System Administrators, and/or individuals acting on their behalf to access the accounts of ITA employees. These occurrences are, but not limited to, a criminal investigation, an unexpected passing of the employee, and/or the need by an authorized individual to access time-sensitive material on the employees account.

- **EXAMPLES OF INSTANCES REQUIRING ACCESS TO EMPLOYEE ACCOUNTS (NOT ALL-INCLUSIVE):**

  A. Criminal Investigation: The actions of Federal employees might result in a reprimand or firing. Allegations of misconduct for federal employees can involve both internal civil or administrative investigations along with criminal proceedings. While criminal investigations related to federal employee misconduct may begin at the same time as an internal administrative investigation, they must be handled like any other criminal investigation. Once ITA is notified that an employee is under any investigation, the appropriate adjudicating authority may compel access to all government accounts used by the individual suspected of the offense.

  B. Passing of an Employee: If a current or former ITA employee has passed, ITA can access all accounts used for official business-related purposes.

  C. Time-Sensitive Requirement: If a superior has requested a deliverable that is needed immediately from an employee who is incapacitated and cannot immediately access their ITA account, a Superior may require access their account to retrieve this specific item. Superiors are defined as Political Appointees, Senior Executive Services Members, and other Key Staff.

[4] "Privacy" is the right of an individual to have the information about him/her adequately protected to avoid the potential for substantial harm, embarrassment, inconvenience or unfairness.

D. FOIA Request: Under the FOIA, agencies must disclose any information that is requested except to the extent that such records[5] (or portions of them) are protectable from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions.

All ITA Employees have acknowledged this document based on their consent to monitoring on the start-up page and the annually signed accepted Rules of Behavior memorandum.

Additionally, the Federal Records Act (Code of Federal Regulations (CFR) 36 and 44 USC), generally requires agencies to keep and organize electronic messages relevant to agency[6] business as official agency documents, subject to disclosure under the Freedom of Information Act (FOIA) and for other purposes. All ITA staff, including key staff, must adhere to all applicable records management policies, including those defined by their Business Unit (BU), the ITA, and the National Archives and Records Administration.

5. RELATED DOCUMENTS

A. TSI IT Information Management Policy
B. IT Security Policy
C. ITA Rules of Behavior for Network Access

6. WAIVERS

There are no waivers from this guidance. There may be waivers or exemptions for certain specifications in the procedures and standards.

7. ADDITIONAL INFORMATION

For further information about this document, please contact the Policy and Strategic Planning Directorate at ITA.

8. AUTHORITY

A. Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35)
B. Information Technology Management Reform Act of 1996 (absorbed under Clinger-Cohen Act of 1996) (40 U.S.C. § 1401)
C. E-Government Act of 2002 (P.L. 107-347, 44 U.S.C. Chapter 36)
D. Records Management by Federal Agencies (44 U.S.C. Chapter 31)

[5] "Records" means all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law.

[6] "Agency" information for this guidance is defined as information that is gathered or created and maintained by ITA or data collected from other sources for which ITA accepts a stewardship role.

E. National Archives and Records Administration Code of Federal Regulations, 36 CFR Subchapter B, Records Management
F. Section 508 of the Rehabilitation Act (29 U.S.C. § 794(d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998

9. MATERIAL SUPERSEDED

N/A

APPROVED BY:

Joe Ramsey
Chief Information Security Officer
Technology, Services and Innovation
International Trade Administration