The Commonwealth of Massachusetts
Executive Office of Technology Services and Security
One Ashburton Place, 8th Floor
Boston, Massachusetts 02108

MAURA T. HEALEY
Governor

KIMBERLEY DRISCOLL
Lieutenant Governor

JASON SNYDER
Secretary/ CIO

MEMORANDUM

To: All Executive Branch Designated Security Officers (DSOs) and IT Liaisons (ITLs)

From: Executive Office of Technology Services and Security

CC: All Executive Branch CISOs and General Counsel

Date: August 29, 2023

Subject: Exception Requests for International Access

Purpose

This Executive Office of Technology Services and Security (EOTSS) Policy establishes standards and guidelines for Executive Branch employees and staff on the use of Commonwealth Issued Devices, (laptops, cell phones, tablets, etc.), and employee access to Commonwealth databases and information systems, including Microsoft Office 365, while travelling outside of the United States, (collectively, International Access).

Mobile devices are issued to employees to facilitate staff communication and remote work on behalf of the Commonwealth. EOTSS Asset Management Standard IS.004 6.7.10 specifically requires that Commonwealth-owned or managed devices do not leave the United States. These devices have access to Commonwealth databases and information systems that contain sensitive data. The use of these devices exposes the Commonwealth to multiple risks, including theft, loss, confiscation, and potential security breach, when connected to unknown and/or unsecure networks, when employees take these devices while travelling internationally.

Policy

Accordingly, in view of the potential cyber security risks associated with the use of Commonwealth Issued Devices, and employee access to Commonwealth databases and information systems, while travelling outside of the United States, exception requests from the requirements of Standard IS.004 6.7.10 will be approved in situations in which the employee

demonstrates an operational need, that is supported by a mission-critical business justification from the employee's manager to the DSO/ ITL, (as determined by the agency), and is approved by both the secretariat Chief Information Security Officer (CISO), or his or her designee, and the secretariat General Counsel (GC), or his or her designee.

All requests for users travelling to a country that is "deny-listed" by the Commonwealth Chief Information Security Office (CISO), will be reviewed by the EOTSS CISO, or his or her designee for approval or denial.

Such written agency/secretariat approval should only be granted in appropriate cases in which the agency DSO/ITL, CISO and General Counsel have all determined the following:

- The duties and functions performed by the requesting employee are of high criticality to the continued business and operational functioning of both the agency and the Commonwealth.
- The agency does not have any other employee, or combination of employees capable of temporarily performing these duties and functions.
- The risks of temporarily suspending the duties and functions performed by the requesting employee are greater than the cyber security risks posed by permitting the employee to remove his/her/their mobile device(s) from the United States; and
- Permitting the employee to access Commonwealth databases and information systems while travelling outside the United States is in the best interests of the Commonwealth to grant this exception.

Procedure

To request an exception request, the agency DSO/ITL must do the following:

1. All exception requests must be submitted through ServiceNow using the approved form. Request submitted through email, or other means are not acceptable and will not be approved.
2. The DSO/ITL must request and submit a complete exception no later than fourteen (14) calendar days before the user's departure from the United States.
3. The exception request must include all required information. Incomplete applications will not be processed.
4. The exception request must include a written detailed business justification from the employee's manager.
5. The requesting employee must be up to date/completed their most recent cyber security training.
6. Requesting employee and/or DSO/ITL must certify they have reviewed applicable policies and standards.

7. The exception request must specifically state that it is approved by both the agency/secretariat CISO, and the agency/secretariat General Counsel (GC), or their designee(s).
8. The DSO/ITL must complete and sign the certification.

Post Approval Procedures

When an exception is granted, EOTSS strongly recommends that all Executive Branch Agencies do the following before any Commonwealth Issued Devices are removed from the United States:

1. Agencies should ensure that the employee's devices do not have any sensitive data stored on the hard drive or internal memory.
2. Agencies should ensure that all devices are updated with the most recent operating systems and security patches.
3. All Commonwealth issued and/or managed devices should have Bitlocker and Intune installed to allow for remote wiping of the device.
4. All system permissions and database access authorizations should be reduced to the lowest level possible to permit the employee to work while travelling internationally.
5. Multi-Factor Authentication is required to obtain access to Commonwealth databases and information systems.
6. Users should not use COMA devices and/or programs to download or otherwise access applications, websites, programs, or information from foreign states identified by federal authorities to pose higher information security risks to United States citizens and/or government data.
7. Users will immediately contact their direct supervisor, IT Department, and EOTSS in the event of theft, loss, confiscation, or compromise of a COMA device.
8. DSOs/ITLs will track employee exception requests and ensure any approved use/access begins and terminates automatically on the international travel dates submitted by the employee with their initial request. Extensions of time will require a supplemental exception request.

Compliance

Compliance with this policy is mandatory for the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of employment and/or assignment with the Commonwealth.

Questions regarding this policy should be directed to ERM@mass.gov.