Maryland Judicial Branch
Electronic Resource Protocols for International Travel

(a) Purpose and Scope

(1) Purpose. To support the continuous operations of the Maryland Judiciary, an employee or covered individual must follow the protocols set forth herein prior to, during, and after international travel if they need to access Judiciary electronic resources and/or travel with their Judiciary Electronic Device.

The approval by the Administrative Head and JIS does not guarantee that a Judiciary Electronic Device complies with or does not otherwise violate any restriction on the import and use of any encryption tools, software, or hardware imposed under foreign law. Refer to the U.S. Department of State's International Travel guidance for the most current information about the travel destination.

(2) Scope.

(A) This protocol applies to:

(i) all persons employed by a court, unit, or judicial entity organized within the Judicial Branch who are issued a Judiciary Electronic Device

(I) including regular, temporary, and contractual employees;

(II) regardless of the source of the employee's compensation (*e.g.*, county, state, federal, grant).

(b) Definitions

(1) Administrative Head:

(A) For the Supreme Court of Maryland, the Clerk of the Court for all employees under the Clerk's supervision and the Chief Justice for all other employees of that Court;

(B) For the Appellate Court of Maryland, the Clerk of the Court for all employees under the Clerk's supervision and the Chief Judge for all other employees of that Court;

(C) For the circuit courts, the Clerk of the Court for all employees under the Clerk's supervision, and the County Administrative Judge for all employees under their supervision;

(D) For the District Court, the Chief Judge of the District Court, the Chief Clerk, the Administrative Clerk, or Administrative Commissioner for all employees under their supervision;

(E) For the Administrative Office of the Courts (AOC), the State Court Administrator;

(F) For units organized within the Judicial Branch, the head of the unit where the employee works; and,

(G) Any person who, by express written designation, serves as the authorized designee of an administrative head.

(2) Covered Individual – Any person issued a Judiciary Electronic Device by the Administrative Office of the Courts or the District Court who is not defined as an employee.

(3) Employee – Any person employed by the Maryland Judiciary and paid through the Central Payroll Bureau of the Comptroller, or employed by a unit, including justices, judges, magistrates, Clerks of Court, and elected officials**.**

(4) Judiciary Electronic Device – Any laptop, tablet, iPad, smart phone, or external hard drive (but not including a USB thumb drive) owned by the Maryland Judiciary and issued to an employee or covered individual.

(5) Judiciary Electronic Resources – VDI Horizon Client, ShareFile, Self Service Password Reset, Office365, Outlook Web Access and Connect.

(6) JIS – The Judicial Information Systems Division of the Administrative Office of the Courts.

(7) Judicial Entity – The Supreme Court of Maryland; the Appellate Court of Maryland; a circuit court or any department therein; the District Court or any department therein; the Administrative Office of the Courts or any department therein; a unit of the Judiciary.

(8) Judiciary Human Resources Division (JHRD) – The division within the AOC that is responsible for, but not limited to, the following functions for State employees in the Maryland Judiciary: human resources policy development, administration, and interpretation; talent acquisition; employment and orientation services; employee benefits; position classification and salary administration; employer-employee relations; and judicial services and information privacy.

(9) Unit – The Attorney Grievance Commission, the Client Protection Fund, the State Board of Law Examiners, the Thurgood Marshall State Law Library, the Commission on Judicial Disabilities, and the Supreme Court of Maryland Standing Committee on Rules of Practice and Procedure.

(c) International Travel without a Judiciary Electronic Device and accessing Judiciary Electronic Resources

(1) Prior to travel

(A) If an employee or covered individual plans to access Judiciary electronic resources, an email must be sent 10 days in advance to the JIS Security Operations Center: jissoc@mdcourts.gov with travel plans to include prospective travel destinations and dates at each location.

(B) The email should include a list of Judiciary Electronic Resources as defined in section (b)(5).

(d) Request and Approval to Travel with Judiciary Electronic Device

(1) An employee or covered individual planning to travel internationally with a Judiciary Electronic Device shall send a written request to the Administrative Head for approval.

(A) The request shall include the name of the individual, a description of the Judiciary Electronic Device for which approval is sought, prospective travel destinations, dates at each location, and a statement of reasons why it is necessary to travel internationally with the Judiciary Electronic Device.

(B) If the request is approved by the Administrative Head, the Administrative Head shall, at least ten (10) business days prior to the first date of international travel, send the request to JIS for approval by opening a ServiceNow ticket.

(C) An employee or covered individual may take their Judiciary Electronic Device when traveling internationally only if approved by both the Administrative Head and JIS.

(2) An Administrative Head planning to travel internationally with a Judiciary Electronic Device shall send the request to JIS for approval by opening a ServiceNow ticket.

(A) The request shall include the name of the Administrative Head, a description of the Judiciary Electronic Device for which approval is sought, prospective travel destinations, and dates at each location.

(B) An Administrative Head may take their Judiciary Electronic Device when traveling internationally only if approved by JIS.

(3) A justice or judge planning to travel internationally with a Judiciary Electronic Device shall send the request to JIS for approval by opening a ServiceNow ticket.

(A) The request shall include the name of the justice or judge, a description of the Judiciary Electronic Device for which approval is sought, prospective travel destinations, and dates at each location.

(B) A justice or judge may take their Judiciary Electronic Device when traveling internationally only if approved by JIS.

(e) Approved Travel with Judiciary Electronic Device

(1) Prior to Travel

(A) An employee or covered individual must connect their Judiciary Electronic Device to the Judiciary network to ensure that it has the most recent operating system, software updates, and the ability to log into the network.

(B) An employee or covered individual shall ensure that no confidential or sensitive files are stored directly on the hard drive of their Judiciary Electronic Device.

(C) An employee or covered individual is advised that some countries have restrictions on the import and use of encryption tools, certain software, or certain hardware and do not allow such products to be imported or used within their borders without a license, or in some cases, at all.

(i) The employee or covered individual – not the Maryland Judiciary – shall have sole responsibility for ensuring that their Judiciary Electronic Device complies with or does not otherwise violate any restrictions on the import and use of any encryption tools, software, or hardware imposed under foreign law.

(D) The employee or covered individual is strongly advised to refer to the U.S. Department of State's International Travel guidance for the most current information about the travel destination.

(E) If the employee or covered individual has an iPhone issued by the District Court, they shall contact the telecom coordinator in Engineering and Central Services if international calling or texting needs to be added to their iPhone.

(F) The employee or covered individual is strongly advised to make a separate, written record of the following email addresses: MissingDevices@mdcourts.gov which should be used to report a Judiciary Electronic Device that is taken, lost, or stolen and jissoc@mdcourts.gov which should be used to report a Judiciary Electronic Device that is compromised.

(2) During Travel

(A) The employee or covered individual shall maintain awareness of their Judiciary Electronic Device when going through airport or building access X-ray machines and other physical security examination equipment.

(B) The employees or covered individual shall ensure the physical safety of their Judiciary Electronic Device and never leave it unsecured (i.e. attending a conference).

(C) An employee or covered individual who is required to surrender their Judiciary Electronic Device for inspection to a government official, such as at customs or a border crossing, shall not disclose any passwords used for encryption or access control, unless otherwise required to do so by the government official.

(D) Employees and covered individuals shall not connect to open Wi-Fi networks that are not password protected by a trusted source. It is preferred that employees and covered individuals use the hotspot on their mobile phone or mobile hotspot device to connect to the Internet.

(I) If Wi-Fi networks at hotels (regardless of size or country of ownership), restaurants, airports, or networks of other commercial institutions must be used, avoid maintaining a connection for extended periods of time.

(II) Terminate the Wi-Fi connection or turn off the Judiciary Electronic Device when not in use.

(III) Never save the Wi-Fi source as a trusted connection.

(IV) Never automatically connect to a Wi-Fi source.

(V) Avoid using a Wi-Fi source in areas of unknown security.

(VI) Use of password-protected Wi-Fi is required.

(E) The employees or covered individual shall turn off wireless communications on their Judiciary Electronic Device (e.g., Bluetooth, Wi-Fi) when not in use.

(F) Judiciary Electronic Devices should be turned off when not in use.

(I) When the Judiciary Electronic Device is turned on, the lock screen should be utilized.

(G) The employee or covered individual shall not download or install any freeware or other software on their Judiciary Electronic Device unless permitted by JIS.

(H) If an employee or covered individual suspects that their Judiciary Electronic Device is compromised, they shall immediately notify the JIS Security Operations Center at jissoc@mdcourts.gov.

(I) If an employee or covered individual suspects that their Judiciary Electronic Device was inspected by a foreign government or agent thereof, they shall immediately notify JIS.

(J) If a Judiciary Electronic Device is suspected of being compromised, JIS may disconnect it from the network without notice.

(3) After Travel

(A) Upon return from international travel, employees and covered individuals shall connect their Judiciary Electronic Device to the Judiciary network.

(f) Lost or Stolen Judiciary Electronic Device

(1) If the Judiciary Electronic Device is lost or stolen, the employee or covered individual shall immediately report to: MissingDevices@mdcourts.gov**,** notify their supervisor and follow established procedures.

(2) For procedures governing lost or stolen Judiciary Electronic Devices administered by District Court, the employee or covered individual shall refer to the Warehouse Inventory Manual available on CourtNet, and notify the Director and Deputy Director of Engineering of Engineering and Central Services.

(3) For procedures governing lost or stolen Judiciary Electronic Devices administered by Administrative Office of the Courts refer to AOC Fixed Asset Inventory Control Manual section (D)(5), available in the Judiciary Employee Handbook**.**

(g) Compliance

Judiciary Electronic Devices that are discovered to be located outside the United States without prior authorization shall be subject to quarantine. A quarantined Judiciary Electronic Device shall not be able to connect to the Internet.

(h) Exceptions

The Chief Justice of the Supreme Court, the State Court Administrator, or the Chief Judge of the District Court, in consultation with JIS, may make exceptions or waive any of the protocols set forth herein.

(i) Interpretive Authority: Judicial Information Systems is responsible for the interpretation of this protocol.

(j) Not a Contract

This protocol does not constitute or create an express or implied contract. It is not intended to, and does not, create contractual obligations with respect to any matter it covers.