106-SOUTH JERSEY TRANSPORTATION AUTHORITY
Policies and Procedures

106 – Policy on Sensitive Information
Revised February 10, 2026

At times electronic communications may include Sensitive Information. All employees who receive, generate, store, handle, and/or transmit Authority Sensitive Information in hard copy or electronically are to adhere to this policy to protect and safeguard Authority Sensitive Information.

Authority Sensitive Information is defined as any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of Authority programs or the privacy to which individuals are entitled under applicable law. This includes sensitive personally identifiable information, which is information that if lost, compromised, or disclosed without authorization, could result in substantial harm to an individual. Such information includes, but is not limited to, social security numbers, financial account numbers, biometric data, etc. Information that is publicly available is not sensitive personally identifiable information for the purposes of this policy.

Guidelines:

1. Development and Storage:

    a. Hard copy documents containing Authority Sensitive Information should be secured in a locked office, filing cabinet or desk.

    b. Documents containing Authority Sensitive Information should be marked “Confidential”.

    c. Files containing Authority Sensitive Information should not be shared with anyone who is not authorized to access this information and access should be limited only to those who have a legitimate business reason to the information.

    d. When Authority Sensitive Information is stored, it should be protected by using file privileges or available user authentication. This includes storage of Authority Sensitive Information on laptops, PC’s, and mobile devices.

e. Authority Sensitive Information should not be stored on unencrypted USBs, drives, CDs, or DVDs.

f. Passwords, PINs, secrets, and any authentication information must never be written down on sticky notes and placed under keyboards or on monitors.

g. When traveling or working remotely in a home office, Authority Sensitive Information must never be visible by parties without the authorization or the need-to-know. This includes Authority Sensitive Information on hard copy documents and monitors or screens.

h. Whiteboards, glass walls, and other display surfaces containing Authority Sensitive Information must be erased when no longer being viewed or worked on.

i. Screens on laptops, tablets, and mobile phones must be locked when stepping away from and not in use.

j. Staff are prohibited from picking up and using USB and removable storage drives where the source of the device is in question.

k. If using USB or removable storage drives, the devices must never be left in the open when not in use and kept with other important personal belongings.

2. Transmission:

a. The transmission of Authority Sensitive Information via electronic communication must be transmitted using Microsoft Outlook encryption tools.

b. If transmission is via Fax, the sender should ensure the individual receiving the fax is available to receive and must confirm receipt of the faxed document.

c. If transmittal is via mail, a form of certified mail or mail service such as UPS or FedEx should be used to ensure delivery to the recipient.

d. When faxing Authority Sensitive Information, a cover page should be used on the transmission.

3. Disposal:

    a. Written notes, hardcopy/printout, and faxes should be shredded when no longer needed.

    b. The retention period of documents containing Authority Sensitive Information should be determined according to SJTA's and State Records Retention Schedules. Documents should be protected as directed in this policy until the retention period has ended and can be destroyed properly.

    c. Discarded computer equipment (including printer/fax machines) must be decommissioned and the hard drive destroyed by the Information Technology Department.

    d. Any computer equipment being sold or transferred to other organizations must be properly sanitized (securely cleared of all information) by the Information Technology Department.

    e. Authority issued devices and equipment that are lost or stolen must be reported to the IT Department immediately. If an employee suspects a device has been stolen, he or she must contact local law enforcement and complete a police report.

4. Access:

    a. Employee access to Authority systems, programs or files containing Authority Sensitive Information must be approved by a Department Director.

    b. If an employee obtains access to Authority Sensitive Information that is outside the employee's job role and could be indicative of an overexposure of information, the employee must contact the IT Department immediately.