SOUTH JERSEY TRANSPORTATION AUTHORITY
Policies and Procedures
Revised effective February 10, 2026

103-Policy on Electronic Communications

E-mail, messaging platforms, voice mail, document storage, and access to the internet are made available to staff members of the Authority for the purpose of conducting work-related business. Employees provided with these resources are expected to use them professionally in a responsible and productive manner. Employees, contractors, and consultants must acknowledge that all electronically created digital artifacts will remain the property of the Authority. Against this background, the following guidelines have been established to assist employees in the use of Authority provided resources.

I. E-mail and Voice Mail

a) The content of e-mail, messaging, voice mail, files, and documents may not contain anything that would reasonably be considered offensive or disruptive to any staff member. Offensive content includes, but is not limited to: sexually explicit material; racial slurs; threatening language; descriptions and images of violence; and comments that would offend someone on the basis of age, sex (including pregnancy), race, color, sexual orientation, gender identity or expression, religious or political beliefs, familial status, marital or civil union status, national origin, nationality, ancestry, and disability.

b) The Authority reserves the right to access and monitor messages, documents, and communications on its systems as deemed necessary and appropriate. Messages and communications are not private. All communications including text, images, and video may be subject to disclosure to law enforcement or other third parties without the prior consent of the sender and the receiver. The confidentiality of any message, document and communication should not be assumed. Even when such is deleted or erased, it is still possible to retrieve.

c) Notwithstanding the Authority's right to retrieve and read any electronic voice, e-mail or message, all communications must be treated as confidential by other staff and accessed only by the intended recipient. Employees are not authorized to retrieve messages intended for other parties except when granted electronic proxy rights.

d) The Authority reserves and will exercise the right to access, review and audit email, voice mail, electronic communications and internet browsing at

any time, with or without notice, and that such access may occur during or after working hours.

e) Audits of email, voice, and electronic record or communications must be conducted by the IT Department. Such audits are only possible with the written request of at least two Authority Directors.

f) Email and user files will be purged periodically. All official correspondence and documents must be stored in designated departmental folders for proper archiving and resiliency. Department folders are viewable by all members of that department.

II. Internet Access

a) Access to the internet is provided to staff based on need. Employees, contractors and consultants who require internet access to certain sites, such as social media, must provide justification and obtain approval from the Director overseeing their department.

b) The Authority utilizes security technologies that provide protection from unauthorized access. These services categorize and block access to websites considered unsafe, unacceptable, or distracting. The IT Department manages such security technologies and periodic reports may be produced and used for monitoring. These reports can provide considerable details including but not limited to identifying users who attempt to visit blocked sites and listing visitors to unblocked sites.

c) Employees granted access to the internet represent the Authority and must conduct themselves in a manner consistent with the Authority's values. Employees are responsible for using the internet in an effective, ethical, and lawful manner. Internet access on Authority owned and supported systems must not be used for personal gain or advancement of individual views. Use of the internet must not be disruptive to the workplace or interfere with productivity.

d) Each employee, contractor and consultant is responsible for the content of text, video, audio, voice and images stored and sent from their designated laptops, computers and devices provided by the Authority. Fraudulent, threatening, harassing, or obscene messages are prohibited. No messages should be transmitted under an assumed name. Users must not attempt to obscure the origin of any message, voice mail, or communication. Information submitted to the internet should not violate or infringe upon the rights of others.

e) Information shall not be released via the Authority intranet and internet without Director level approval. Exceptions to this include information

released in an official capacity and when prior approval is obtained from the appropriate owner of the information.

f) The Authority will cooperate with proper requests made under the "Freedom of Information Act" and the "New Jersey Open Public Records Act." All such requests must be approved by the Executive Director or his designee after consultation with General Counsel.

g) For further information, you may refer to the Freedom of Information Act, (5 U.S.C 552) and/or The Open Public Records Act, (N.J.S.A 47:1A-1 et seq.)

h) To prevent computer malware from being transmitted, the unauthorized downloading of software is prohibited. All software downloads must be done through the IT Department.

III. Sensitive Information

At times electronic communications may include Sensitive Information. The guidelines for transmitting and receiving such information are set forth in Policy No. 106 – Policy on Sensitive Information.

IV. Responsibilities

This policy applies to all users of Authority computer systems, including employees, contractors, and consultants, as well as anyone with access to Authority information. Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination. If necessary, the Authority will advise appropriate legal officials of any illegal violations.

For all union employees, all disciplinary action shall be in accordance with the Collective Bargaining Agreement.