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

208 Onboarding, Separation, & Transfer Security Policy

This policy outlines the mandatory requirements for onboarding new employees and contractors ("new hires"), as well as for processing staff separations and transfers within SJTA. Its goal is to ensure the secure and efficient modification of digital identities and access based on the principles of "least privilege" and "needs-to-know."

I. Onboarding

A. Training & Policy Acknowledgement

New hires must complete the following within a reasonable amount of time after employment or a contract begins:

1. New Hire Security Training: This demonstrates basic techniques for identifying indicators of compromise. Additional training will show users how to correctly report suspicious activity to the IT Department (IT).

2. Electronic Communications Policy: New hires must read and sign the Employee Electronic Communications Policy. The Human Resources (HR) department must confirm and store receipt of the signed document.

3. The Hiring Manager must complete the ***New Hire Equipment Form*** provided by the IT Department and ensure IT has a copy.

4. Where necessary, hiring managers will provide role-based training on the responsibilities necessary for successful job functioning.

B. Background Checks

1. Pursuant to the official document ***201 Policy on Hiring***, all offers of employment are conditioned upon applicants successfully passing the following: criminal background checks; medical / physical examinations; drug screenings; employment verification;

and depending on the position specific driver's license information may be required.

2. Logical access to SJTA systems and physical access to SJTA buildings and property will not be granted to any new hire without explicit approval from HR.

C. Access Provisioning Based on "least privilege" and "needs-to-know":

1. When background checks and drug screenings have been successfully completed, a member of HR will notify the Hiring Manager that a full offer of employment has be extended to the candidate.

2. IT will create identities and access for the new hire based on the ***New Hire Equipment Form***.

II. Separation

A. During the separation process, the Hiring Manager must complete the ***Transfer / Termination Checklist*** located on the ***Employee Portal***, ensuring that all property of the Authority is securely returned by the departing employee or contractor.

B. When employee or staff separation is known by HR, a member of HR shall notify IT of this change within one business day.

C. Employees, contractors, and consultants must have all logical access, including access to the Authority's directory services, disabled by close of business (COB) of the staff member's last day.

1. It is HR's responsibility to disable the separating staff member's access within the Authority's payroll system.

2. In instances where employees and contractors are terminated or suspended, access must be disabled immediately. HR must notify IT immediately of a staff member's termination or suspension.

3. Upon approval from 2 directors or higher, the IT Department can grant access to the departing staff member's email, files, and folders for continuation of business purposes. If / when this occurs the access shall not exceed sixty days.

4. Employees, contractors, and consultants must have physical security badges disabled by COB on their last day.

a) In instances where employees and contractors are terminated or suspended, the physical security badge must be electronically disabled immediately.

D. Working with the Hiring Manager, IT will use the ***New Hire Equipment Form*** to determine equipment that has not been returned by the former employee.

E. The IT Department reserves the right to remotely "wipe" or make unusable any device or electronic equipment owned by the Authority and not returned.

F. For employees separating with knowledge of building alarm codes, IT must contact the Maintenance Department to have the code(s) disabled.

G. HR is responsible for contacting IT to report employees under suspension and entering temporary leave. The access of these employees will be determined by relevant laws, Authority policies, and the principles of least privilege and needs-to-know.

III. Transfers and Promotions

A. The HR Department must notify the IT Department immediately of employees being transferred to another position or being promoted.

B. The employee's new supervisor must complete the ***Transfer / Termination Checklist*** located on the Employee Portal and email to IT.

C. The IT Department will either create new access or modify existing based on staff's needs-to-know and the requirements in this document.

1. The employee's former access will remain in place for up to 30 days upon request.

D. If an additional background check is required, the new or modified access may be revoked depending on the outcome.