Network Security Standards

Authentication
- API requests must use authentication.
- Passwords must not be stored in plain text. This applies to user and API credentials.
- Passwords must be stored using a cryptographic hash.
- Passwords must be stored with a hashing function that incorporates a salt.
- If asymmetric encryption is used for authentication it must use an industry-standard Public Key Cryptography (PKI) algorithm.
- Any private keys for PKI must be secured.
- All authentication that uses username and password credentials and is accessible from the Internet must use multi-factor authentication.

Encryption
- All sensitive information must be encrypted in transit. Sensitive information includes authentication traffic, credentials, personally-identifiable user information, and vehicle information.
- Encryption must be done using an industry-standard protocol such as TLS or IPsec.
- All web (HTTP) traffic must be encrypted and use TLS.
- TLS in use must be TLS 1.2.
- A VPN may be used (IPsec or OpenVPN) to secure traffic that is not encrypted by the application.

Security Testing
- The application must pass cybersecurity testing using SEPTA’s contracted cybersecurity vendor.
- Any issues identified during the testing must be addressed before the app is put into production.

Network segmentation
- Where possible, traffic should be segmented so that only those devices and users that need to communicate with a given system are able to access that system.
- SEPTA maintains a centralized firewall with Intrusion Prevention (IPS) and Intrusion Detection (IDS) capabilities. This firewall is used to segment all network traffic on SEPTA’s network.
- All protocols should use their standard TCP and UDP ports.
Third-party libraries

- Any third-party libraries used by the app must be approved by SEPTA.
- The vendor must supply SEPTA with a list of third-party libraries used by the app and their versions for approval.