AUTHANTICATION FLOW

Creating an Account on the Client
→ Request Minimum Password Length 8
Upper Case, Lower Case, Digits, Special Characters

→ Don't allow password hints

→ Avoid Security Questions

Login
→ Don't let the user know the password was incorrect when he is logging in, instead mention that the combination of the password and username is incorrect

Use HTTPS Protocol

Credential Storage
→ Password Storage, use Aragon 2 for Hash the password and save it.
The `salt` should be a random string stored alongside your password.
The `secret` should be a random key only usable at hashing time.

Password Reset
→ Predicatable Tokens - Tokend based on current time are a good example
→ Storage - Generate a long token and Hash it as a Password
→ Expiring your Token
→ Ask for the Email address where to send the Reset Token as Second Data Verification

API Credentials Tokens
→ **Over HTTPS**

Rate Limiting Account Locking
→ Run an Reverse Proxy like NGINX and allow Rate Limiting to request.
At least, use a Rate Limiting middleware for Express