Cyber Security Assessment and Tasks

Features

- Account Onboarding: The application includes an in-app onboarding form that must properly capture demographics prior to full account access.
- Data Sharing: The app contains a child sharing feature that operates between multiple parent accounts.
- Admin Authentication: Two-factor authentication (2FA) will be added to the admin portal login to ensure that access to sensitive administrative controls is strictly protected. Upgrading to Firebase Authentication with Identity Platform allows the use of SMS or Time-based One-Time Passwords (TOTP) as a second factor.
- Domain Security: We need to secure an HTTPS certificate for our recent domain name. By demonstrating control over the domain to a Certificate Authority, we can provision a TLS certificate to ensure all web traffic remains securely encrypted.
- User Account Role: We are currently storing roles as a key in our document-based database. Ideally we migrate this to token based authentication at some point in the life cycle of this app.

Final Cyber Security Assessment

- We are prioritizing the resolution of security issues as recommended by our cyber team.
- During our reviews, we found outdated npm packages within the Firebase functions.
- We also identified new vulnerabilities with Firebase that involved Gemini API security.
- To resolve this specific Firebase vulnerability, the Gemini API just needs to be disabled.
- Gemini API Key Vulnerability Details:
    - Truffle Security discovered nearly 3,000 publicly exposed Google API keys that can now authenticate to Gemini, allowing malicious actors to exhaust quotas, generate massive bills, and scrape private cached data.
- Axios NPM Supply Chain Attack:
    - On March 31, 2026, the highly popular axios npm package was compromised when a lead maintainer's account was hijacked.
    - The attackers published malicious versions (1.14.1 and 0.30.4) containing a phantom dependency called plain-crypto-js.

    - This dependency acted as an obfuscated dropper that silently deployed a cross-platform Remote Access Trojan (RAT) across Windows, macOS, and Linux systems upon installation.

Periodic Cyber Security Checklist

- API Key Auditing: Verify that no unrestricted or public-facing API keys have unintended access to the Generative Language API, and ensure all keys are explicitly scoped strictly to their required services.
- Dependency Management & Version Pinning: Routinely check for and update outdated npm packages found within Firebase functions. Explicitly pin critical dependencies to known safe versions (e.g., reverting to axios@1.14.0 or axios@0.30.3) to mitigate sudden supply chain compromises.
- API Configuration: Verify that unnecessary services are turned off to avoid new vulnerabilities with Firebase. Ensure specifically that the Gemini API remains disabled.
- Access Gate Verification: Periodically test the password gate to ensure restricted areas remain securely locked and disable the account if too many login attempts occur.
- Cyber Team Audits: Continue to review and fix any emerging security issues as recommended by the cyber team.
- Domain & Certificate Renewal: Monitor the expiration date of the domain's HTTPS certificate and verify that automatic renewals (such as those configured via ACME clients) execute successfully prior to expiration.
- Admin Access Review: Periodically audit admin portal accounts to ensure that two-factor authentication remains actively enforced for all privileged users.