FOR FRONTEND TEAM (Website Design Team)

□ 1. HTTPS everywhere:
□ All resources load via HTTPS
□ No "mixed content" warnings

□ 2. External resources secure:
□ List ALL external scripts/fonts/images
□ Use Subresource Integrity (SRI) for external scripts
□ Example: <script src="..." integrity="sha256-...">

□ 3. Form security:
□ Client-side validation (but don't rely on it!)
□ Display clear error messages
□ No sensitive data in URL parameters

□ 4. Data handling:
□ NO sensitive data in localStorage
□ Clear forms after submission
□ Auto-logout after inactivity (if login implemented)

□ 5. Error handling:
□ User-friendly error messages
□ No technical details shown to users
□ Log errors securely

□ 6. Cross-Origin settings:
□ List domains needed for CORS
□ Test with cybersecurity's CORS settings

User Interface Security Checklist:

- □ 1. Privacy notices:
- □ Clear "how we use your data" notice
- □ Simple language (not legal jargon)
- □ Prominent placement

- □ 2. Data minimization:
- □ Only ask for necessary information
- □ Mark optional fields clearly
- □ Explain why each piece of data is needed

- □ 3. Secure design:
- □ Forms clear and easy to understand
- □ Confirmations for important actions
- □ Loading states show progress