FOR BACKEND TEAM (Sarah's Team)

- [ ] 1. ALL API endpoints use HTTPS (no HTTP)
- [ ] 2. Input validation on EVERY endpoint:
- [ ] Business type: only ['butchery', 'grocery', 'supermarket']
- [ ] City: max 100 characters, no special symbols
- [ ] Monthly spend: number between 0-1,000,000
- [ ] Equipment: valid list format

- [ ] 3. Add cybersecurity's security middleware:
- [ ] Rate limiting middleware added
- [ ] Input validation middleware added
- [ ] Security headers middleware added
- [ ] Logging middleware added

- [ ] 4. Error messages NEVER show technical details:
  ✅ Good: "Internal server error"
  ❌ Bad: "SQL error: SELECT * FROM users WHERE id='123' OR '1'='1'"

- [ ] 5. Database connections use SSL:
- [ ] Connection string includes: ?ssl=true&sslmode=require
- [ ] Test connection works with SSL

- [ ] 6. Sensitive data marked for encryption:
- [ ] Monthly spend field
- [ ] Business name (if collected)
- [ ] Any financial data

- [ ] 7. Implement cybersecurity's safe query functions:
- [ ] Use prisma.$queryRaw with parameters
- [ ] NEVER concatenate strings in SQL

- [ ] [ ] 8. Health check endpoint includes security status:
- [ ] [ ] Returns: {"ssl": true, "rate_limiting": "enabled"}

PDF Report Security Checklist:

- [ ] 1. Reports have watermark:
- [ ] Shows report ID
- [ ] Shows generation timestamp
- [ ] Light gray, not obvious

- [ ] 2. Secure file permissions:
- [ ] Reports folder: 750 permissions
- [ ] Report files: 644 permissions

- [ ] 3. Automatic cleanup:
- [ ] Delete reports older than 24 hours
- [ ] Test cleanup works

- [ ] 4. Download security:
- [ ] Rate limit: max 10 downloads/hour per IP
- [ ] Validate report ID before serving