Security & Data Handling Compliance

1. Authentication and Access Controls

1.1 User Authentication Requirements

Requirement	Status	Implementation
Email verification	■ Required	Send verification link on signup
Phone verification	■ Required	SMS/OTP verification
Strong password policy	■ Required	Min 8 chars, mixed case, numbers
MFA support	■ Recommended	TOTP or SMS-based
Session management	■ Required	Secure token handling

Password Requirements (if password-based login)

- ■ Minimum 8 characters
- ■ At least one uppercase letter
- ■ At least one lowercase letter
- ■ At least one number
- ■ At least one special character (recommended)
- ■ Password strength indicator
- ■ Breached password check (recommended)

Session Security

- ■ Secure, HTTP-only cookies
- ■ Session timeout (30 days mobile, 24 hours web)
- ■ Force logout on password change
- ■ Device management (view/revoke sessions)

1.2 Admin/Internal Access Controls

Role	Access Level	Approval Required
Developer	Code repositories, staging	Team lead
Admin	Production read access	Both founders
Super Admin	Full production access	Both founders

Role-Based Access Control (RBAC) Requirements:
- ■ Principle of least privilege enforced
- ■ Access reviews quarterly
- ■ Access immediately revoked on departure
- ■ Audit log of all admin actions

---

2. Encryption Standards

2.1 Data in Transit

Requirement	Standard	Status
HTTPS everywhere	TLS 1.2+ minimum	■ Required
Certificate management	Auto-renewal (Let's Encrypt/AWS ACM)	■ Required
HSTS enabled	max-age=31536000	■ Required
Certificate pinning (mobile)	Optional but recommended	■ Recommended

Implementation Checklist:
- ■ TLS 1.2 or higher enforced
- ■ TLS 1.0/1.1 disabled
- ■ Strong cipher suites only
- ■ HSTS header configured
- ■ SSL Labs grade A or higher

2.2 Data at Rest

Data Type	Encryption Method	Key Management
Photos	AES-256	AWS KMS / Cloud KMS
PII (email, phone, name)	AES-256	AWS KMS / Cloud KMS
Location data	AES-256	AWS KMS / Cloud KMS
Messages	AES-256	AWS KMS / Cloud KMS
Database	Encrypted volumes	Cloud provider managed

Implementation Checklist:
- ■ Database encryption enabled (RDS/Cloud SQL)
- ■ S3/Cloud Storage encryption enabled
- ■ Encryption keys managed via KMS
- ■ Key rotation policy (annual)
- ■ Backup encryption enabled

2.3 Token Security

- ■ Session tokens use cryptographically secure random generation
- ■ Tokens stored securely (Keychain/Keystore on mobile)
- ■ Token expiration enforced
- ■ Refresh token rotation implemented

3. User Content Safety Controls

3.1 Photo Moderation Pipeline

```
■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■ ■ User Upload ■■■■■■
Content Scanner ■■■■■■ Review Queue ■ ■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■
■■■■■■■■■■■■■■■■ ■ ■ ▼ ▼ ■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■ ■ Auto-Approve
■ ■ Manual Review■ ■ (Safe Content)■ ■ (Flagged) ■ ■■■■■■■■■■■■■■■■■
■■■■■■■■■■■■■■■
```

3.2 Content Categories to Detect

Category	Action	Tool/API

Nudity/Explicit	Block + warn	Google Vision / Hive
Violence	Block + warn	Google Vision / Hive
Hate symbols	Block + warn	Hive / ActiveFence
Minors	Block + escalate	Google Vision / Hive
Spam/Fake profiles	Flag for review	Custom ML + Sift

3.3 Recommended Moderation Services

Service	Capability	Pricing Model
Google Cloud Vision	Image labeling, SafeSearch	Per image
Hive Moderation	Comprehensive content moderation	Per image/text
ActiveFence	Trust & safety platform	Enterprise
Sift	Fraud + content moderation	Per event
AWS Rekognition	Content moderation	Per image

3.4 Text/Message Moderation

- ■ Profanity filter
- ■ Spam detection
- ■ External link detection
- ■ Phone/email sharing detection
- ■ Harassment pattern detection

4. Incident Response Plan

4.1 Incident Classification

Severity	Description	Response Time	Escalation
Critical	Data breach, system compromise	Immediate	Both founders
High	Service outage, security vulnerability	1 hour	Tech lead
Medium	Partial outage, suspected attempt	4 hours	On-call
Low	Minor issue, no user impact	24 hours	Normal ticket

4.2 Security Breach Response Procedure

Phase 1: Detection & Containment (0-4 hours)

1. ■ Identify breach scope
2. ■ Isolate affected systems
3. ■ Preserve evidence (logs, snapshots)
4. ■ Activate incident response team

Phase 2: Assessment (4-24 hours)

1. ■ Determine data affected
2. ■ Identify attack vector
3. ■ Assess user impact
4. ■ Document timeline

Phase 3: Notification (24-72 hours)

1. ■ Legal counsel consultation
2. ■ Regulatory notification (if required)
   - GDPR: 72 hours to supervisory authority
   - CCPA: "Without unreasonable delay"
3. ■ User notification (if required)
4. ■ Public communication (if needed)

Phase 4: Recovery & Prevention

1. ■ Remediate vulnerability
2. ■ Restore services
3. ■ Post-incident review
4. ■ Update security measures
5. ■ Document lessons learned

4.3 Notification Templates

User Notification Template:

```
Subject: Important Security Notice from [App Name] Dear [User], We are writing to inform
you of a security incident that may have affected your account. [Description of incident]
What happened: [Brief description] What data was affected: [Specific data types] What
we're doing: [Remediation steps] What you can do: [User actions recommended] Contact us:
security@[company].com
```

4.4 Logging & Monitoring Requirements

Log Type	Retention	Storage	Alerting
Authentication logs	1 year	CloudWatch/Stackdriver	Failed attempts
API access logs	90 days	CloudWatch/Stackdriver	Anomalies
Admin action logs	2 years	Immutable storage	All actions
Error logs	30 days	CloudWatch/Stackdriver	Critical errors
Security events	2 years	SIEM	All events

5. Security Implementation Checklist

Immediate Priorities

- ■ Enable HTTPS/TLS 1.2+ on all endpoints
- ■ Enable database encryption
- ■ Implement email/phone verification
- ■ Set up basic logging

Short-term (30 days)

- ■ Integrate content moderation API
- ■ Implement RBAC for admin panel
- ■ Set up security monitoring alerts
- ■ Document incident response procedures

Medium-term (90 days)

- ■ Penetration testing
- ■ Security awareness training
- ■ Implement MFA for users (optional)
- ■ Set up SIEM solution

Ongoing

- ■ Quarterly security reviews
- ■ Annual penetration testing
- ■ Regular dependency updates
- ■ Security patch monitoring

Last Updated: December 2024
Review Due: March 2025