Business Continuity & Operations

Incident Response, HR & Operational Procedures

1. Security Incident Handling

1.1 Incident Response Team

Role	Primary	Backup	Contact
Incident Commander	[Founder 1]	[Founder 2]	[Phone/Email]
Technical Lead	[Founder 2]	[Founder 1]	[Phone/Email]
Communications	[Founder 1]	[Founder 2]	[Phone/Email]
Legal/Compliance	External Counsel	-	[Contact]

1.2 Incident Classification

Severity	Description	Response Time	Examples
P1 - Critical	Service down, data breach	Immediate (< 15 min)	Full outage, confirmed breach
P2 - High	Significant degradation	< 1 hour	Partial outage, security vuln
P3 - Medium	Minor impact	< 4 hours	Feature broken, perf issue
P4 - Low	No user impact	< 24 hours	Internal issue, minor bug

1.3 Incident Response Procedure

Phase 1: Detection (0-15 minutes)

1. ■ Incident reported/detected
2. ■ Initial assessment of severity
3. ■ Notify incident commander
4. ■ Start incident log

Phase 2: Containment (15-60 minutes)

1. ■ Isolate affected systems
2. ■ Preserve evidence (logs, snapshots)
3. ■ Implement temporary fixes
4. ■ Assess scope of impact

Phase 3: Investigation (1-24 hours)

1. ■ Root cause analysis
2. ■ Impact assessment
3. ■ Determine user/data affected
4. ■ Document timeline

Phase 4: Resolution (varies)

1. ■ Implement permanent fix
2. ■ Verify resolution
3. ■ Restore normal operations
4. ■ Monitor for recurrence

Phase 5: Post-Incident (within 48 hours)

1. ■ Conduct post-mortem
2. ■ Document lessons learned
3. ■ Implement preventive measures
4. ■ Update procedures as needed
5. ■ Notify affected parties (if required)

1.4 Incident Communication Templates

Internal Alert:

```
INCIDENT ALERT - [SEVERITY] Time: [Timestamp] Issue: [Brief description] Impact:
[User/system impact] Status: [Investigating/Mitigating/Resolved] Lead: [Name] Next
update: [Time]
```

User Communication (if needed):

```
Subject: Service Update from [App Name] We're currently experiencing [brief issue
description]. Our team is working to resolve this. Impact: [What users might experience]
Status: [Current status] Expected resolution: [If known] We apologize for any
inconvenience. Updates will be posted at [status page URL].
```

2. Production System Access

2.1 Access Control Matrix

Person	Role	Production DB	Production Servers	Admin Panel	AWS Console
[Founder 1]	Co-founder	✓ Full	✓ Full	✓ Full	✓ Full
[Founder 2]	Co-founder	✓ Full	✓ Full	✓ Full	✓ Full
[Future Dev]	Developer	■ None	■ Read-only	■ Limited	■ Limited
[Future Support]	Support	■ None	■ None	■ User lookup	■ None

2.2 Access Provisioning Process

Granting Access:
1. Business justification documented
2. Approval from both founders
3. Minimum necessary permissions assigned
4. Access logged in access register
5. Training completed (if needed)

Revoking Access:
1. Immediate revocation on departure
2. All credentials rotated
3. Session tokens invalidated
4. Access removal logged
5. Verification of removal

2.3 Access Review Schedule

Review Type	Frequency	Reviewer
Active access audit	Monthly	Both founders
Permissions appropriateness	Quarterly	Both founders
Third-party access	Quarterly	Both founders

Service account review	Semi-annually	Technical lead

3. User Support Handling

3.1 Support Channels

Channel	Response SLA	Priority
In-app support	24 hours	Standard
Email (support@)	24 hours	Standard
Safety reports	4 hours	High
Legal requests	24 hours	High

3.2 Support Ticket Categories

Category	Handling	Escalation Path
Account issues	Support team	Technical lead
Billing/Payment	Support team	Finance
Safety/Abuse	Priority queue	Founders
Technical bugs	Log + prioritize	Technical lead
Feature requests	Log + review	Product
Legal/Privacy	Immediate escalation	Founders + Legal

3.3 Support Escalation Matrix

Issue Type	Level 1	Level 2	Level 3
General inquiry	Support	-	-

Technical issue	Support	Tech lead	Founders
Safety concern	Support	Founders	Legal
Legal request	Founders	Legal counsel	-
Security issue	Tech lead	Founders	External security

3.4 Support Response Templates

Account Issue:

```
Hi [Name], Thank you for contacting [App Name] support. [Response to their specific
issue] If you have any other questions, please don't hesitate to reach out. Best,
[Support Name] [App Name] Support Team
```

Safety Report Acknowledgment:

```
Hi [Name], Thank you for reporting this concern to us. We take safety seriously and will
review this report promptly. For your safety: - You can block this user immediately - We
recommend not sharing personal information - If you feel unsafe, please contact local
authorities We'll take appropriate action based on our review. [App Name] Safety Team
```

---

4. Outage Procedures

4.1 Outage Response

Immediate Actions (0-15 minutes):

1. ■ Confirm outage scope
2. ■ Check infrastructure status (AWS/GCP)
3. ■ Check recent deployments
4. ■ Activate incident response
5. ■ Post to status page

Investigation (15-60 minutes):

1. ■ Review error logs
2. ■ Check monitoring dashboards
3. ■ Identify root cause
4. ■ Implement fix or rollback

Communication:

1. ■ Update status page every 30 minutes

2. ■ Prepare user communication (if extended)
3. ■ Document for post-mortem

4.2 Rollback Procedure

Application Rollback:

1. Identify last known good version
2. Deploy previous version
3. Verify functionality
4. Monitor for issues
5. Investigate failed deployment

Database Rollback:

1. Stop application writes
2. Identify restoration point
3. Restore from snapshot/backup
4. Verify data integrity
5. Resume operations
6. Document data loss (if any)

4.3 Status Page Requirements

Information to Display:

- Current system status
- Incident history (90 days)
- Scheduled maintenance
- Subscribe to updates option

Status Categories:

- ■ Operational
- ■ Degraded Performance
- ■ Partial Outage
- ■ Major Outage

5. Escalation Contacts

5.1 Internal Escalation

Situation	Primary Contact	Backup Contact
Production issues	[Founder 2 - Tech]	[Founder 1]

Security incidents	[Founder 2 - Tech]	[Founder 1]
User safety	[Founder 1]	[Founder 2]
Legal matters	[Founder 1]	External counsel
Financial issues	[Founder 1]	[Founder 2]
PR/Communications	[Founder 1]	[Founder 2]

5.2 External Escalation

Vendor/Service	Support Contact	Account Manager
AWS	AWS Support	[If applicable]
Stripe/Payments	[Support link]	-
SendGrid/Email	[Support link]	-
Twilio/SMS	[Support link]	-
Apple (App Store)	App Store Connect	-
Google (Play Store)	Play Console	-

5.3 Emergency Contacts

Type	Contact	When to Use
Legal counsel	[Law firm]	Legal emergencies
Security consultant	[If applicable]	Security incidents
PR firm	[If applicable]	Crisis communications

6. Business Continuity Plan

6.1 Critical Business Functions

Function	RPO	RTO	Recovery Priority
User authentication	5 min	1 hour	Critical
Matching/discovery	1 hour	4 hours	High
Messaging	5 min	2 hours	High
Payments	1 hour	4 hours	High
User support	24 hours	24 hours	Medium

6.2 Disaster Scenarios

Scenario	Probability	Impact	Mitigation
Region outage	Low	Critical	Multi-region DR
Data breach	Medium	Critical	Incident response plan
Key person unavailable	Medium	High	Cross-training, documentation
Vendor failure	Low	Medium	Alternative vendors identified
DDoS attack	Medium	Medium	CDN, WAF protection

6.3 Recovery Procedures

Region Failover:
1. Detect region failure
2. Activate DR region
3. Update DNS/routing
4. Verify services operational
5. Communicate status
6. Plan return to primary

Key Person Unavailable:
1. Activate backup contact
2. Access shared credentials (if needed)
3. Review documentation

4. Consult external resources if needed
5. Document actions taken

7. Documentation & Training

7.1 Required Documentation

Document	Owner	Review Frequency
System runbooks	Technical lead	Quarterly
Incident response plan	Both founders	Semi-annually
Access control procedures	Both founders	Annually
Vendor contacts	Operations	Quarterly
Recovery procedures	Technical lead	Semi-annually

7.2 Training Requirements

Topic	Audience	Frequency
Incident response	All team	Annually
Security awareness	All team	Annually
On-call procedures	Technical team	As needed
Customer support	Support team	Onboarding + updates

7.3 Drill Schedule

Drill Type	Frequency	Last Conducted	Next Due
Tabletop incident exercise	Semi-annually	-	-
Failover test	Annually	-	-

Backup restoration	Quarterly	-	-
Security drill	Annually	-	-

8. Operational Checklist

Daily Operations

- ■ Monitor system health dashboards
- ■ Review error logs
- ■ Check support queue
- ■ Review safety reports

Weekly Operations

- ■ Review security alerts
- ■ Check backup status
- ■ Review metrics/KPIs
- ■ Team sync on issues

Monthly Operations

- ■ Access review
- ■ Vendor invoice review
- ■ Performance review
- ■ Update documentation

Quarterly Operations

- ■ Full access audit
- ■ Backup restoration test
- ■ Procedure review
- ■ Security update review

Last Updated: December 2024
Review Due: June 2025