# ATC Crisis Management System – Change Control Expectations

## Purpose

This document defines **expectations, guardrails, and responsibilities** for making changes to the ATC Crisis Management System. It exists to protect system reliability, security, and trust—especially during emergencies.

This document applies to: - Application code changes - Power Automate flow changes - Security and identity configuration changes

---

## 1. Guiding Principle

This system is **mission-critical**.

Changes must prioritize: - Stability over speed - Predictability over optimization - Operational safety over convenience

If a change introduces uncertainty during an emergency, it is not acceptable.

---

## 2. Approved Change Categories

### Low-Risk Changes (Generally Safe)

- Text updates (labels, copy, descriptions)
- Non-functional UI adjustments
- Adding new checklist items *without* logic changes
- Updating documentation

### Medium-Risk Changes (Require Testing)

- Checklist logic changes
- Leadership alert trigger conditions
- Form field additions or validation changes
- SharePoint list schema updates

### High-Risk Changes (Restricted)

- Authentication or token handling
- Power Automate trigger logic

- Microsoft Graph permissions
- Custom connector changes
- Authorization conditions

High-risk changes must be reviewed and tested deliberately.

---

## 3. Versioning Discipline (Application)

### Required Practice

- **Every deployment must increment the application version**
- Version changes are not optional

### Why This Matters

- The PWA enforces version consistency
- Users may be offline for extended periods
- Failure to bump versions causes:
- Cache conflicts
- Unexpected reload behavior

### Expectation

- Version bump occurs *before* deployment
- No exceptions

---

## 4. Power Automate Change Rules

### Flow Modifications

- Never edit production flows directly during business hours
- Changes should be made during low-impact windows

### Required After Any Flow Change

- Test with a known, controlled input
- Confirm:
- SharePoint write success
- Teams notification delivery
- Leadership alert behavior

### Rollback Awareness

- Understand how to revert to the previous flow version
- Never deploy without a rollback path

---

## 5. Security Configuration Changes

### Includes

- App registration secrets
- Graph permissions
- Custom connector credentials

### Rules

- Changes must be documented
- Secrets must be rotated deliberately
- Expiration dates must be tracked

Failure in this area impacts **all notifications**.

---

## 6. Testing Boundaries

### Production Testing Rules

- Never test leadership alerts in production
- Never test during live incidents
- Use test modes and test recipients

### Assumption

Every test message may be seen by a real person if misconfigured.

---

## 7. Deployment Timing Expectations

Avoid deploying: - During known severe weather events - During business-critical hours - When on-call coverage is unavailable

Deployments should assume: - Immediate rollback may be required

---

## 8. Ownership and Accountability

Anyone making changes: - Owns the outcome - Owns the rollback - Owns the communication if something breaks

This system supports real people during real emergencies.

---

## Final Expectation

If you are unsure whether a change is safe: - Do not deploy it

Stability and trust outweigh feature velocity.