

# MFA Readiness Checklist

MFA becomes required for ServTraq and CALIHEAPApply in January. Use this page to get your agency ready ahead of time, not on deadline day.



## WAYS TO DO THE SECOND STEP, STRONGEST FIRST

### Security key or passkey

A small USB or tap key, or a passkey on your phone. Strongest, and built to resist phishing.

### App with number match

The sign in screen shows a number. Type it into your authenticator app to approve.

### App code

A 6 digit code in your authenticator app that changes every 30 seconds.

### Text or call code

A code sent by text or phone call. Better than nothing, best as a backup.

## 1 Know your accounts

- ☐ List every staff member who logs in to ServTraq or CALIHEAPApply.
- ☐ Disable accounts for anyone who has left.
- ☐ Replace shared logins so every person has their own account.
- ☐ Know who the administrator is for each system.

## 3 Turn on MFA everywhere you can

- ☐ **Email:** Microsoft 365 or Google Workspace, for every user.
- ☐ **Money:** bank, payroll and payment portals.
- ☐ **Admin accounts:** the keys to everything else.
- ☐ **Remote access:** VPN and remote desktop tools.

## 2 Get every person ready

- ☐ Confirm each person has a phone or device for the second step.
- ☐ Plan for staff without a smartphone, such as a security key or a call code. Ask ServTraq which methods it supports.
- ☐ Have each person complete a test login before January.
- ☐ Tell staff who to call if they get locked out.

## 4 Make verification normal

- ☐ New bank details or a payment request? Call a number you already have, not the one in the email.
- ☐ Never read out, forward or type in a code or number for someone else, even if they say they are IT.
- ☐ Make it safe for staff to stop, verify and report.

**The one rule:** if you get a prompt, a code or a number request when you are not signing in, someone else has your password. **Deny** it, never share or type the code, change your password and tell IT right away.

## 5 Plan for a bad day

- ☐ Know who gets called if an account is compromised.
- ☐ Know how to disable an account and reset its password and MFA quickly.
- ☐ Keep backups of critical data, and test a restore.
- ☐ Store MFA recovery codes somewhere safe, not in email.

### Want a second pair of eyes? Ask for a free first look.

One conversation and a straight answer about where your agency stands. No cost, no commitment, no pitch.

**akrom@zakhidov.ai**  
zakhidov.ai