

AGENCY SECURITY QUICK REFERENCE

Do's and Don'ts for security etiquette, password safety, MFA, email security, and protecting client data.

Protect Your Passwords

- ✓ Use a unique password or passphrase for every business account
- ✓ Use an approved password manager
- ✓ Use encrypted email if a password must ever be shared
- ✗ Store passwords in spreadsheets, sticky notes, or browsers on shared PCs
- ✗ Reuse your agency password on personal sites

Multi-Factor Authentication (MFA)

- ✓ Approve MFA prompts only when you started the sign-in
- ✓ Use Microsoft Authenticator or another agency-approved app
- ✓ Keep your phone and recovery methods up to date
- ✗ Approve a prompt just to make repeated requests stop
- ✗ Share MFA codes with anyone, including "IT support" callers

Email Security

- ✓ Hover over links before clicking and check the real address
- ✓ Call back on a known number to verify ACH, wire, or premium payment changes
- ✓ Watch for look-alike domains (e.g., rn instead of m)
- ✓ Report phishing using your agency's reporting process
- ✗ Open unexpected attachments, even from "carriers" or clients
- ✗ Reply to the email to verify a request; use a known contact instead

Client Information Security

- ✓ Access only the client data you need for your work
- ✓ Verify caller identity before discussing policies, claims, or billing
- ✓ Save documents only in approved agency systems
- ✓ Use encrypted email when sending applications, loss runs, or IDs
- ✗ Email SSNs, driver's license numbers, or bank details unencrypted
- ✗ Save client files to personal email, USB drives, or home PCs

AI and Data Privacy

- ✓ Use only AI tools approved by the agency
- ✓ Ask first when unsure whether data can be uploaded
- ✗ Enter SSNs, DOBs, driver's license numbers, or claims details into public AI tools

Working Remotely

- ✓ Use the agency VPN or secure connection when required
- ✓ Keep laptops and phones locked and physically secure
- ✓ Use a strong password and WPA2/WPA3 encryption on home Wi-Fi
- ✗ Do sensitive work on public or hotel Wi-Fi
- ✗ Leave client information visible in public places or on screen

Physical & Desk Security

- ✓ Lock your screen every time you step away: Windows + L
- ✓ Shred printed applications and documents with client data
- ✗ Let unknown visitors or "vendors" in without checking

SECURITY GOLDEN RULES

- Lock your screen: Windows + L
- Verify before you trust
- When unsure, ask IT
- Protect client information like it's your own
- Report suspicious activity immediately
- Money changes always get a phone call