Onboarding Password Policy Checklist

STACK CYBERSECURITY

Password Creation

- [ ] My password is at least 8 character long
- [ ] I used a passphrase or a mix of letters, numbers, and symbols
- [ ] My password is not a common or easily guessed word (e.g., “123456”, “password”)
- [ ] I did not reuse a password from another account
- [ ] I verified my password is not listed in known breach databases

Password Storage and Transmission

- [ ] I do not store passwords in plain text or unsecured files
- [ ] I use a password manager to store and manage my credentials
- [ ] I understand that passwords are encrypted during transmission

Password Changes

- [ ] I will change my password only if it is suspected to be compromised
- [ ] I understand that regular forced changes are not required unless mandated by policy

Failed Login Attempts

- [ ] I know that multiple failed login attempts may trigger a temporary lockout
- [ ] I will contact IT if I am locked out or suspect unauthorized access

Multifactor Authentication (MFA)

- [ ] I have enabled MFA for all sensitive systems
- [ ] I use a secure second factor (e.g., app, token, biometric)

Password Manager Use

- [ ] I use an approved password manager to generate and store passwords
- [ ] I understand how to securely share credentials when necessary
- [ ] I know how to monitor for breaches using the password manager’s tools

Reporting and Response

- [ ] I will report any suspected password compromise immediately
- [ ] I understand that IT wil handle resets and access audits
- [ ] I will follow the organization’s incident response procedures