COMPYL

CONTINUOUS COMPLIANCE

# Fundamentals Information Security Checklist

85% of this list can be implemented in ***under 10 days with Compyl***

## Business Continuity Plan Essentials

- □ Emergency contact information of key personnel documented.
- □ Contact information for key service providers & vendors documented
- □ Stand operating procedures documented
- □ Core business operations listed by criticality (i.e. restored first)

## Financial Security Essentials

- □ Set up alerts for bank accounts, payment services, credit services
- □ Enforce "Separation of duties"
- □ Limit amount of money different employees can approve
- □ Cybersecurity insurance purchased
- □ Employee background checks performed

## Security Incident Response Essentials

- □ Security incident response plan created
- □ Board, legal counsel, executive staff, and customer notification processes created.
- □ Security logs securely stored & indexed.

## Customer Essentials

- □ Privacy Policy & Terms of Use created
- □ Security mailbox create; contact information published on main site
- □ For B2B: Security "Sales Kit" created

## Compliance Essentials

- □ Understand industry compliance, breach notification, and cybersecurity requirements

## Security Awareness Training Essentials

- □ Security is understood as everyone's responsibility
- □ Employees trained annually on business procedures & business continuity plan
- □ Employees trained during onboarding (and annually thereafter) on phishing, social engineering, Business Email Compromise, & fraud
- □ Acceptable Use Policy created & signed
- □ Social Media Policy created & signed

## IT Security Essentials

- □ Default system credentials are changed
- □ SPF, DMARC, DKIM DNS records created
- □ Spam filtering enabled
- □ Passwords are never reused or shared
- □ 2fa enabled for email and Identity Provider
- □ Laptop operating systems are updated monthly, at most
- □ Antivirus on laptops enabled, auto-updates
- □ Disk encryption on laptops enabled
- □ Access revoked for outgoing employees
- □ Access to data & systems limited to only those needed to perform job duties

## Product Security Essentials

- □ Data backups created && securely stored
- □ Application security scans performed
- □ Third-party penetration tests performed
- □ Set password policy for users
- □ Application logs securely stored
- □ For B2Bs: Minimal Viable Secure Product guidelines followed (mcps.dev/)

## Cloud Security Essentials

- □ Network flow logs enabled & securely stored
- □ 2fa is enabled on the root account
- □ Access keys deleted for root account
- □ Full and accurate asset inventory created & kept up-to-date
- □ Native cloud security controls are implemented
- □ Networks are monitored for security events

## Security Architecture Essentials

- □ Public-facing systems do not contain critical data
- □ Unused ports & protocols disabled
- □ Access to production data severely limited
- □ Databases are encrypted; keys are stored separately
- □ Networks are segmented
- □ Firewalls implemented & packet filtering enabled
- □ Servers are patched regularly

High Performer FALL 2022

Easiest To Use FALL 2022

Easiest To Do Business With FALL 2022

Best Support FALL 2022

hello@compyl.com