# Family Cyber Safety Framework (FCSF) V1.0

## Introduction

The Family Cyber Safety Framework (FCSF) is an original, easy-to-follow framework designed specifically for households and families. It adapts proven principles from NIST, CSF, ISO/IEC 27001, and the CIS Critical Security Controls to help non-technical parents and guardians protect their homes, children, and personal data.

## Goals of the Framework

- Provide a structured yet simple approach to home cybersecurity.
- Use plain language instead of technical jargon.
- Align with leading global standards while being feasible for everyday parents.
- Promote a security culture for all family members, including children.

## The Framework

The FCSF is built of three easy to remember **Steps** and 16 practical **Activities:**

1. **Prepare -** set the house rules and who does what, list the people, devices, and accounts to protect.
2. **Protect -** put the everyday protection in place, notice when something's wrong.
3. **Respond -** follow a short plan when trouble happens, restore your stuff and improve for next time.



www.aidit.co.il | roman.vaintraub@aidit.co.il | +972 54 2482454

| Step | Activity | Description | Review Frequency |
|---|---|---|---|
| **Prepare** | (1) Family Cyber Rules | One page of house rules: time online for children, what's private, define Roles and Permissions, who uses admin and who uses standard accounts. | Yearly |
| | (2) Devices and Accounts list | The list includes Devices that need protection (phones, tablets, PCs, smart TV, router, cameras, game consoles), Account Inventory (emails, banking, socials, gaming, school portals) classified according to their criticality and who uses what (parents, kids, grandparents, visitors). | Yearly or when a change happens |
| **Protect** | (3) Strong Sign-in | Password manager, unique passphrases, 2-step login on critical accounts (email/bank/social). | Every six months or when new account is added |
| | (4) Safe Devices | Antivirus on Computers, App hardening and permissions review on Smartphones, SW based Firewall. | Every six months or when new Device is added |
| | (5) Safe Browsing | DNS family filter. | Every six months or when new device is added |
| | (6) Update Everything | Auto-updates on OS, apps, router/IoT firmware. | Every six months or when new device is added |
| | (7) Safe Network | WPA2/3, new router admin password, router auto-updates or scheduled firmware checks, guest/IoT network separation from home NW. | Every six months or when new device is added |

| | | | |
|---|---|---|---|
| | (8) Parental Control | Age filters, app store approval, screen-time limits. | Every six months or when new device is added |
| | (9) Privacy by Default | Private profiles, location sharing off by default, minimal data in forms. | Every six months |
| | (10) Backups | 3 copies, 2 types of media, 1 on cloud. | Every six months |
| | (11) Security Alerts | Email/login alerts on major accounts; bank/SMS alerts for transactions. | Every six months |
| | (12) Home Check-ups | Monthly 10-minute review: new devices? updates failed? odd emails? | Monthly |
| **Respond** | (13) "What If" plan | Create a list of "what If" scenarios, simple list that will be used as incident response plan (e.g., disconnect Wi-Fi, change password, call bank/school). The What If plan helps us to adopt the "stop-think-act" approach. | Yearly |
| | (14) Lost Device Playbook | What actions to take if a device is lost (locate/lock/wipe with Find My/Android Device Manager, change major passwords).<br>Review Frequency: Yearly | Yearly |
| | (15) Restore & reset | How to clean reinstall if malware suspected, restore from backup, re-enable 2-step login. | Yearly + Yearly Drill |
| | (16) Learn & improve | Write 2 lines: what happened, what to change (e.g., add 2FA for X, move camera to guest Wi-Fi). | When incident happens |

The Family Cyber Safety Framework is a fresh, practical approach for households. By following its Steps families can dramatically reduce risk, protect personal data, and teach children digital life skills.


www.aidit.co.il | roman.vaintraub@aidit.co.il | +972 54 2482454