Root Kilt Security
Personal Cybersecurity Framework (PCF)

This framework is designed to help individuals take a structured, prioritized approach to personal cybersecurity. By applying weighted controls across key areas—Identify, Protect, Detect, Respond, and Recover (Derived adaptation from NIST SP 800-53 & ISO 27001)—it provides high-level actionable guidance to safeguard devices, accounts, cryptocurrency, and sensitive data.

Root Kilt Security's PCF empowers users to proactively reduce risks, respond effectively to incidents, and maintain resilience in today's evolving threat landscape. However no framework or technical control can provide a 100% secure guarantee.

Index

1. Purpose

This framework provides individuals with a practical, actionable cybersecurity structure to protect social media accounts, mobile devices, cryptocurrency assets, and personal devices. Each control is assigned a weighting to indicate its relative importance, and includes recommended actions for implementation.

2. Scoring and Weighting System

Weight	Description
5	Critical – Must be implemented immediately, prevents high-impact incidents.
4	High – Strongly recommended, significantly improves security.
3	Medium – Provides value but less urgent.
2	Low – Some benefit, less impact.
1	Minimal – Low value, mostly optional.

3. Framework Structure & Controls

Identify

Control	Weight	Objective	Recommended Actions
Asset Inventory	Weight 5	Record all personal devices, accounts, and wallets.	Maintain an up-to-date list of all devices/accounts; include serial numbers; review every 6 months.
Data Classification	Weight 4	Identify sensitive personal data and where it is stored. This can be: Personal documents, family photos, Home Videos etc.	Label or understand the location of important files; store in encrypted folders understand access and limit access. Including cloud services such as iCloud.
Account Mapping	Weight 5	Maintain recovery details for all accounts.	Document recovery email/phone; test recovery regularly. Know which recovery processes are linked to which devices, accounts (email) and mobile numbers.

Protect

Control	Weight	Objective	Recommended Actions
MFA/2FA Enforcement	Weight 5	Enable MFA on all critical accounts.	Use app-based MFA or hardware tokens; avoid SMS-based & Knowledge-based MFA
Password Management	Weight 5	Use unique, strong passwords.	Install a password manager; generate random passwords for each account. Backup your password manager file in an encrypted format.
Patch Management	Weight 4	Apply OS and app updates promptly.	Enable automatic updates; check manually monthly.
Crypto Cold Storage	Weight 5	Store cryptocurrency offline securely.	Use hardware wallets; store seed phrases offline in a fireproof safe.
Social Media Privacy	Weight 4	Limit exposure of personal data online.	Review privacy settings at least quarterly; remove unnecessary personal info

			from public view.

Device Hardening	Weight 4	Secure personal devices.	Enable full-disk encryption;
			Disable unused services;
			install antivirus/firewall.

Detect

Control	Weight	Objective	Recommended Actions
Account Monitoring	Weight 4	Receive alerts for unusual activity.	Enable login alerts; check account activity logs monthly.
Breach Monitoring	Weight 4	Detect breaches quickly.	Subscribe to breach notification services; act immediately on alerts.
Crypto Alerts	Weight 5	Monitor wallet transactions in real-time	Set up alerts; Confirm every transaction personally. Review outgoing transactions at start or end of month.

Respond

Control	Weight	Objective	Recommended Actions
Incident Response Plan	Weight 4	Have a documented or practised incident response process. (What to do if/when you misplace a device, or have a burglary for example)	Write down steps for account/device compromise; keep printed copy safe if possible or have at least key contact numbers and information (IMEI) and customer numbers stored safe.
Access Revocation	Weight 5	Immediately revoke compromised credentials.	Maintain quick links to security settings; practice revoking access.
Crypto Asset Migration	Weight 5	Transfer crypto securely after a compromise.	Pre-configure backup wallets; test migration with small transactions.

Recover

Control	Weight	Objective	Recommended Actions
Encrypted Backups	Weight 5	Maintain secure, offline backups.	Use encrypted external drives/cloud storage; backup monthly.
Backup Restoration Testing	Weight 4	Ensure backups work.	Test restoring files quarterly.
Post-Incident Review	Weight 4	Learn from incidents.	Document cause, impact, and prevention steps.

4. Appendix – Weightings Table

Weight	Description
5	Critical – Must be implemented immediately, prevents high-impact incidents.
4	High – Strongly recommended, significantly improves security.
3	Medium – Provides value but less urgent.
2	Low – Some benefit, less impact.
1	Minimal – Low value, mostly optional.

5. Disclaimer & Contact Information

This document is provided as a guideline only and does not guarantee complete immunity from cyber threats. Cybersecurity is a continuous process requiring monitoring, updates, and expert consultation.

Root Kilt Security recommends seeking professional advice (From people like us!) for tailored protection.

Contact Root Kilt Security:

■ Web: www.rootkiltsecurity.com
■ Phone: +44 7902500190