Choosing the right hardware

- [ ] System supports SecureBoot (*ESSENTIAL*)
- [ ] System has no firewire, thunderbolt or ExpressCard ports (*NICE*)
- [ ] System has a TPM chip (*NICE*)

Pre-boot environment

- [ ] UEFI boot mode is used (not legacy BIOS) (*ESSENTIAL*)
- [ ] Password is required to enter UEFI configuration (*ESSENTIAL*)
- [ ] SecureBoot is enabled (*ESSENTIAL*)
- [ ] UEFI-level password is required to boot the system (*NICE*)

Distro choice considerations

- [ ] Has a robust MAC/RBAC implementation (SELinux/AppArmor/GrSecurity) (*ESSENTIAL*)
- [ ] Publishes security bulletins (*ESSENTIAL*)
- [ ] Provides timely security patches (*ESSENTIAL*)
- [ ] Provides cryptographic verification of packages (*ESSENTIAL*)
- [ ] Fully supports UEFI and SecureBoot (*ESSENTIAL*)
- [ ] Has robust native full disk encryption support (*ESSENTIAL*)

Distro installation guidelines

- [ ] Use full disk encryption (LUKS) with a robust passphrase (*ESSENTIAL*)
- [ ] Make sure swap is also encrypted (*ESSENTIAL*)
- [ ] Require a password to edit bootloader (can be same as LUKS) (*ESSENTIAL*)
- [ ] Set up a robust root password (can be same as LUKS) (*ESSENTIAL*)
- [ ] Use an unprivileged account, part of administrators group (*ESSENTIAL*)
- [ ] Set up a robust user-account password, different from root (*ESSENTIAL*)

Password managers

- [ ] Use a password manager (*ESSENTIAL*)
- [ ] Use unique passwords on unrelated sites (*ESSENTIAL*)
- [ ] Use a password manager that supports team sharing (*NICE*)
- [ ] Use a separate password manager for non-website accounts (*NICE*)

Post-installation hardening

- [ ] Globally disable firewire and thunderbolt modules (*ESSENTIAL*)
- [ ] Check your firewalls to ensure all incoming ports are filtered (*ESSENTIAL*)
- [ ] Make sure root mail is forwarded to an account you check (*ESSENTIAL*)
- [ ] Set up an automatic OS update schedule, or update reminders (*ESSENTIAL*)
- [ ] Check to ensure sshd service is disabled by default (*NICE*)
- [ ] Configure the screensaver to auto-lock after a period of inactivity (*NICE*)
- [ ] Set up logwatch (*NICE*)
- [ ] Install and use rkhunter (*NICE*)
- [ ] Install an Intrusion Detection System (*NICE*)

Browsing

- [ ] Use two different browsers (*ESSENTIAL*)
- [ ] Use Firefox for work and high security sites. Install the following Firefox add-ons:
  - [ ] NoScript (*ESSENTIAL*)
  - [ ] Privacy Badger (*ESSENTIAL*)
  - [ ] HTTPS Everywhere (*ESSENTIAL*)
  - [ ] Certificate Patrol (*NICE*)
- [ ] Use Chrome/Chromium for everything else
- [ ] Use two different browsers, one inside a dedicated VM (*NICE*)
- [ ] Fully separate your work and play environments via virtualization (*PARANOID*)

Securing SSH and PGP private keys

- [ ] Strong passphrases are used to protect private keys (*ESSENTIAL*)
- [ ] PGP Master key is stored on removable storage (*NICE*)
- [ ] Auth, Sign and Encrypt Subkeys are stored on a smartcard device (*NICE*)
- [ ] SSH is configured to use PGP Auth key as ssh private key (*NICE*)

SELinux on the workstation

- [ ] Make sure SELinux is enforcing on your workstation (*ESSENTIAL*)

Personal workstation backups

- [ ] Set up encrypted workstation backups to external storage (*ESSENTIAL*)
- [ ] Use zero-knowledge backup tools for off-site/cloud backups (*NICE*)

Checklist priority levels

The items in each checklist include the priority level, which we hope will help guide your decision.

(**ESSENTIAL**) items should definitely be high on the consideration list. If not implemented, they will introduce high risks to your workstation security.

(**NICE**) to have items will improve the overall security, but will affect how you interact with your work environment, and probably require learning new habits or unlearning old ones.

(**PARANOID**) is reserved for items we feel will significantly improve your workstation security, but will require a lot of adjustment to the way you interact with your operating system.