Cette procédure s'appuie sur les recommandations officielles de l'ANSSI et le cadre réglementaire français, notamment la loi AGEC et le Référentiel Général de Sécurité (RGS).

Elle vise à garantir la sécurité, la conformité et la traçabilité lors du reconditionnement de postes de travail (PC portables ou fixes).

---

1. Analyse préalable et organisation

- Réaliser une **analyse de risques** spécifique à l'intégration de matériels reconditionnés dans le système d'information, en identifiant les usages, les risques résiduels et les mesures d'atténuation.
- Limiter la diversité des modèles pour faciliter la gestion de la sécurité et la maintenance.
- Définir les cas d'usage adaptés (éviter les postes critiques comme l'administration système ou financière).

---

2. Audit et préparation du matériel

- **Contrôler l'intégrité physique** de chaque appareil : vérifier l'absence de composants ajoutés (microphones, caméras, modules suspects), de modifications matérielles ou de traces de compromission.
- S'assurer que le matériel dispose d'une **garantie minimale d'1 an** et de la possibilité de recevoir des mises à jour de firmware pendant au moins 2 ans.
- Vérifier la présence de **fonctionnalités de sécurité matérielle** : puce TPM 2.0, Secure Boot UEFI, possibilité de modifier les clés UEFI Secure Boot.

---

3. Effacement sécurisé des données

- **Effacer de façon sécurisée** tous les supports de stockage (SSD, HDD, eMMC), en privilégiant :
  - L'effacement cryptographique par perte de clé si le disque était chiffré à l'origine (avec TPM, carte à puce ou token).
  - Sinon, utiliser des outils certifiés (CSPN) ou reconnus (ex : Blancco Drive Eraser, hdparm, outils du fabricant)
- Adapter la méthode d'effacement à la sensibilité des données traitées et tenir compte des secteurs défectueux non effaçables.
- **Retirer tous les supports amovibles** (cartes SD, SIM, etc.) et effacer les composants mémoires annexes.

---

4. Réinstallation et sécurisation logicielle

- Installer soi-même un système d'exploitation propre, à partir d'une image maîtrisée et à jour, plutôt que d'utiliser un OS préinstallé par un tiers.
- Appliquer toutes les mises à jour de sécurité du système et des firmwares (BIOS, UEFI, etc.).
- **Activer le chiffrement du disque** dès l'installation du système d'exploitation.

- Configurer les paramètres de sécurité du firmware (désactiver les ports inutiles, activer le Secure Boot, etc.).

---

5. Contrôles, documentation et traçabilité

- Effectuer un contrôle post-reconditionnement pour s'assurer de la conformité des opérations et de l'absence de comportements suspects ou de compromission.
- Documenter toutes les étapes du reconditionnement, y compris les outils utilisés, les numéros de série, les dates et les personnes responsables.
- Révoquer les droits, identifiants ou accès associés à l'ancien usage du matériel et anonymiser l'appareil (suppression d'autocollants, QR codes, etc.).

---

6. Déploiement et suivi

- Affecter les matériels reconditionnés à des usages non critiques ou à des périmètres bien identifiés pour limiter l'exposition aux risques.
- Assurer un suivi des mises à jour logicielles et matérielles pendant toute la durée de vie du matériel.

Résumé des points clés à respecter

Étape	Action essentielle
Analyse de risques	Intégrer le reconditionné dans l'analyse de risques SI
Audit matériel	Vérification physique, garantie, sécurité matérielle
Effacement sécurisé	Effacement cryptographique ou logiciel certifié, retrait des supports amovibles
Réinstallation OS	Installation d'un OS propre, mises à jour, chiffrement disque
Contrôles & documentation	Vérification finale, traçabilité, anonymisation
Déploiement & suivi	Affectation adaptée, gestion des mises à jour

---

Cette procédure doit être adaptée en fonction de la sensibilité des données, des contraintes techniques et du contexte d'usage. Les recommandations de l'ANSSI doivent être appliquées strictement pour garantir la sécurité et la conformité réglementaire.

Sources et liens

- https://cyber.gouv.fr/publications/recommandations-pour-le-reconditionnement-des-ordinateurs-de-bureau-ou-portables
- https://cyber.gouv.fr/sites/default/files/document/anssi-guide-reconditionnement_ordinateurs_bureau_portables_v1-0.pdf

- https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs
- https://www.it-connect.fr/les-bonnes-pratiques-de-lanssi-pour-les-ordinateurs-reconditionnes-achat-cession/
- https://www.silicon.fr/Thematique/workspace-1376/Breves/PC-reconditionnes-les-recommandations-de-l-AnSSI-387123.htm
- https://www.lemondeinformatique.fr/actualites/lire-pc-reconditionnes-ou-cedes-l-anssi-donne-ses-conseils-de-securite-91760.html