# Arrêté du ….

Portant instruction pour les contrôles annuels de maintenance préventive des systèmes d’information

La ministre de la transition écologique et de la cohésion des territoires et la ministre de la transition énergétique,

Vu la loi du 21 juin 2004 pour la confiance dans l'économie numérique,

Vu l’arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité,

Vu la loi du 20 juin 2018 relative à la protection des données personnelles,

Arrêtent

# Article 1

Le maintien en condition opérationnelle et de sécurité des systèmes d’information prévu dans le règlement général de sécurité ainsi que la politique de sécurité des systèmes d’information de l’Etat implique une maintenance préventive qui se matérialise par des contrôles au minimum annuels.

Ces points de contrôles incluent les mesures définies en annexe.

# Article 2

Sont visés par cette instruction tous les systèmes d’information qui totalisent 500 h d’utilisation par mois (l’usage est estimé par multiplication du nombre usuel d’utilisateurs et leur durée habituelle d’usage mensuel).

# Article 3

Les maîtres d’ouvrage et donneurs d’ordre sont responsables du bilan annuel de maintenance.
Ils peuvent déléguer la maintenance préventive et la réalisation des points de contrôle à la maîtrise d’œuvre de leur choix.

# Article 4

Les systèmes d’information qui n’avait pas de politique de maintenance préventive préexistante disposent d’un délai supplémentaire jusqu’au 31 décembre 2024 pour réaliser le premier bilan annuel.

# Article 5

Le présent arrêté sera publié au Journal officiel de la République française.

# Annexe

Points de contrôle de la maintenance d’un système d’information

## Article 1 – Traçabilité

Les contrôles ne sont pas nécessairement réalisés le même jour, mais ils sont synthétisés dans une fiche datée par rubrique qui reprend les articles de cette annexe dans l’ordre.

## Article 2 - Sauvegardes et capacité de redémarrage

Des données de sauvegardes, locales et distantes, sont restaurées. En particulier, il est contrôlé l’âge des dernières sauvegardes exploitables, après déchiffrement éventuel pour les sauvegardes distantes. Tout âge de dernière sauvegarde supérieur à une semaine est justifié.

Une relance machine vérifie les capacités de redémarrage sans assistance manuelle, et évalue la durée d’un tél redémarrage. Tout temps de service machine continu « uptime » supérieur à un an est justifié.

## Article 3 - Contrôle des composants par rapport à des failles connues et au support

Les versions des composants sont comparées aux bases d’inventaires des failles connues.

La filière Sécurité des Systèmes d’Information est chargée de tenir à jour la panoplie d’outils permettant l’automatisation de ces contrôles. Exemple à date des outils recommandés pour les piles technologiques les plus courantes du ministère, des couches les plus basses au plus hautes.

* Linux : audit Lynis
* Conteneur : scan docker ou trivy
* Java : rapport dependency-check
* PHP : rapport symfony security-checker ou repman security scanner
* Node.js : rapport npm audit

Ce contrôle s’assure aussi du support de l’éditeur ou d’une communauté active, par exemple via le référentiel <https://endoflife.date>

Toute utilisation d’un composant présentant une faille avec un score CVSS supérieur ou égal à 7 ou sans support depuis 6 mois est justifié.

## Article 4 - Mises à jour des enregistrements

La maîtrise d’ouvrage actualise les inventaires suivants :

* cartographie des acteurs sur le portail Support Produits et Services (SPS) ;
* couverture des tests de supervision réalisés par le pôle de supervision informatique national (PSIN) ;
* abonnements aux fils d'alerte de sécurité des composants ;
* échéances d'homologation SSI, déclaration CNIL.

## Article 5 - Revue des incidents

La maîtrise d’œuvre synthétise les événements d’exploitation notables de la période extraits de :

* historique des indisponibilités non programmées,
* tickets d’incidents et problèmes récurrents.