Voici un **plan d'action détaillé** pour l'homologation sécurité de votre application, un **site Web grand public** au sein du ministère de l'Écologie, basé sur les référentiels généraux et les dispositions particulières du ministère. Ce plan suit les étapes clés définies par l'ANSSI et les documents ministériels.

---

1. Préparation et Cadrage

1.1. Identifier l'autorité d'homologation (AH)

- **Responsable** : MOA (Maîtrise d'Ouvrage) et RSSI (Responsable Sécurité des Systèmes d'Information).
- **Action** :
  - Identifier l'**Autorité d'Homologation (AH)** désignée par le ministère de l'Écologie.
  - Vérifier que l'AH est enregistrée auprès du **FSSI** (Fonctionnaire de Sécurité des Systèmes d'Information).
  - **Référence** : Politique ministérielle de sécurité numérique, §4.1.1.5.

1.2. Évaluer les enjeux du site Web

- **Responsable** : MOA et RSSI.
- **Action** :
  - Classer le site Web comme un **SI à enjeux faibles** (grand public, peu de données sensibles).
  - **Référence** : Fiche méthode homologation, §3.2.

---

2. Réalisation des Études et Documents Obligatoires

2.1. Évaluation des besoins de sécurité numérique

- **Responsable** : MOA et RSSI.
- **Action** :
  - Rédiger un **document d'évaluation des besoins de sécurité** en identifiant :
    - Les données traitées (ex : données personnelles, informations publiques).
    - Les services proposés (ex : consultation, téléchargement de documents).
    - Les risques potentiels (ex : cyberattaques, fuites de données).
  - **Référence** : Guide ANSSI - Homologation en 9 étapes, Étape 1.

2.2. Mise en conformité avec le socle de sécurité numérique

- **Responsable** : RSSI et équipe technique.
- **Action** :
  - Appliquer le **socle de sécurité minimal** pour les SI à enjeux faibles :
    - **Mesures techniques** :
      - Chiffrement des échanges (HTTPS).
      - Mises à jour régulières des logiciels et dépendances.
      - Protection contre les attaques courantes (DDoS, injections SQL, XSS).
    - **Mesures organisationnelles** :
      - Sensibilisation des équipes à la cybersécurité.
      - Gestion des accès (habilitation, authentification forte si nécessaire).
  - **Référence** : RGS v2.0, §2.4 et Politique d'homologation, §3.2.

2.3. Rédaction du dossier de sécurité numérique

- **Responsable** : MOA et RSSI.
- **Action** :
  - Constituer un **dossier de sécurité numérique** incluant :
    - L'évaluation des besoins de sécurité.
    - La description des mesures de sécurité mises en place.
    - Les preuves de conformité (ex : rapports de scans de vulnérabilités, certificats SSL).
  - **Référence** : Politique d'homologation, §3.2.

---

3. Soumission et Décision d'Homologation

3.1. Soumission du dossier à l'AH

- **Responsable** : MOA.
- **Action** :
  - Transmettre le dossier complet à l'**Autorité d'Homologation (AH)**.
  - Préparer une présentation pour la **commission d'homologation** incluant :
    - Le périmètre du site Web.
    - Les référentiels appliqués (RGS, RGAA, etc.).
    - Les plans d'action pour les éventuelles non-conformités.
  - **Référence** : Politique d'homologation, §3.2.

3.2. Décision d'homologation

- **Responsable** : AH.
- **Action** :
  - L'AH prononce une **décision d'homologation** :
    - **Homologation ferme** (valable 3 ans maximum).
    - **Homologation provisoire** (6 mois à 1 an avec plan d'action).
    - **Homologation ajournée** (si des mesures critiques manquent).
  - **Référence** : Politique d'homologation, §5.2.

---

4. Suivi Post-Homologation

4.1. Maintien en condition de sécurité (MCS)

- **Responsable** : Équipe technique et RSSI.
- **Action** :
  - Mettre en place un **suivi opérationnel** :
    - Surveillance des journaux d'événements.
    - Mises à jour correctives et correctifs de sécurité.
    - Veille sur les menaces (ex : abonnement aux alertes du CERT-FR).
  - **Référence** : RGS v2.0, §2.5.

4.2. Révisions périodiques

- **Responsable** : MOA et AH.
- **Action** :
  - Prévoir une **révision de l'homologation** tous les 3 ans ou en cas de :
    - Changement majeur du site (nouvelle fonctionnalité, refonte).
    - Évolution des menaces ou des réglementations.
  - **Référence** : Guide ANSSI - Homologation en 9 étapes, Étape 9.

---

5. Documents et Ressources Clés

- **Référentiels généraux** :
  - Référentiel Général de Sécurité (RGS).
  - Guide ANSSI - Homologation en 9 étapes.
- **Dispositions ministérielles** :

- Politique ministérielle de sécurité numérique.
- Politique d'homologation du ministère.

---

6. Calendrier Prévisionnel

Étape	Responsable	Durée estimée	Livrable
1. Préparation et cadrage	MOA, RSSI	2 semaines	Identification AH, évaluation enjeux
2. Études et conformité	RSSI, Équipe technique	4 semaines	Dossier de sécurité, preuves de conformité
3. Soumission et décision	MOA, AH	2 semaines	Décision d'homologation
4. Suivi post-homologation	Équipe technique, RSSI	Continu	Rapports de surveillance, mises à jour

---

7. Points de Vigilance

- **Accessibilité** : Vérifier la conformité au **RGAA** (Référentiel Général d'Accessibilité pour les Administrations).
- **Protection des données** : Si le site traite des données personnelles, réaliser une **AIPD** (Analyse d'Impact relative à la Protection des Données) en collaboration avec le DPO (Délégué à la Protection des Données).
- **Interopérabilité** : Respecter le **Référentiel Général d'Interopérabilité (RGI)**.

Ce plan est adapté pour un **site Web grand public** avec des enjeux faibles. Si des éléments spécifiques (ex : traitement de données sensibles) sont identifiés, des étapes supplémentaires (audits, tests d'intrusion) pourront être ajoutées.