



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Objectifs et règles de sécurité numérique du ministère de l'Intérieur

PGSN – A10

Sécurité du développement des systèmes

Version 1.0

NON PROTEGE

Préambule

Le présent document est une composante à part entière de la politique générale de sécurité numérique du ministère de l'Intérieur (PGSN-MI).

Les principes stratégiques de la PGSN-MI et les dispositions générales de l'instruction sont traduits au sein du présent document en objectifs à atteindre, reprenant la structure de la politique de sécurité des systèmes d'information de l'Etat (PSSI-E).

Des règles techniques ou non techniques permettant de contribuer à la réalisation de chaque objectif sont énoncées au sein du présent document :

- Les mesures préfixées par « PSSI- », suivies de la nomenclature seule, sont des règles inchangées de la PSSI-E de 2014. Des modifications peuvent néanmoins y être effectuées sur l'appellation de certaines fonctions propres au ministère.
- Les mesures préfixées « MI- » sont des mesures venant préciser la règle originale ou définir des règles propres au ministère de l'Intérieur, formulées par le SHFD.

Toute dérogation à un objectif ou une règle du présent document, doit se faire en conformité avec la règle *MI-ORG-PGSN-DEROG* du document [PGSN-A01] du corpus de la sécurité numérique.

Sécurité des développements

1. Développement des systèmes

Objectif A10-1 : prise en compte de la sécurité dans le développement des SI. Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.

PSSIE-DEV-INTEGR-SECLOC : intégrer la sécurité dans les développements locaux. Toute initiative locale de développement informatique doit respecter les exigences nationales en matière de SSI, concernant la prise en compte de la sécurité dans les projets et les développements informatiques. Le service à l'origine du projet se porte garant de l'application du référentiel général de sécurité, et de l'application d'une démarche d'homologation du système.

MI-DEV-SOUS-TRAIT : intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique. Lors de l'écriture d'un contrat de sous-traitance de développement, plusieurs clauses relatives à la SSI doivent être intégrées :

- Formation obligatoire des développeurs sur le développement sécurisé et sur les vulnérabilités classiques, en s'appuyant sur des bases reconnues comme celles fournies par l'OWASP ou le système CVE ;
- Utilisation obligatoire d'outils permettant de minimiser les erreurs introduites durant le développement (outils gratuits d'analyse statique de code, utilisation de bibliothèques réputées pour leur sécurité, ...) ;
- Production de documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement, ...) ;
- Respect des lois, règlements et décrets devant être pris en compte le développement du SI ;
- Respect des normes de développement sécurisé, qu'elles soient propres au développeur, publiques ou propres au commanditaire ;
- Obligation pour le prestataire de corriger, dans un temps raisonnable et pour un prix défini, les vulnérabilités introduites durant le développement et qui lui sont remontées, en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation.

La manière dont le sous-traitant répond à ces exigences doit être formalisée dans un plan d'assurance sécurité (PAS) conformément au document [PGSN-B02] du corpus de la sécurité numérique.

MI-DEV-INTEGR-SECEXT : intégrer la SSI dans les développements externalisés. Tout développement informatique externalisé doit respecter les exigences nationales en matière de SSI telles que décrites dans le cadre de cohérence technique (CCT) ministériel, partie développement. Il appartient à la maîtrise d'ouvrage du projet d'initier et de piloter la démarche d'homologation du système.

MI-DEV-INTERNE-FORM : formation des développeurs internes. Tout agent destiné à assurer des développements logiciels doit avoir été formé au langage utilisé et notamment au principe de développement sécurisé.

MI-DEV-SPEC-LOG : Développement spécifique sur des progiciels. Les modifications spécifiques sur des progiciels ne doivent pas être encouragées et être limitées aux changements strictement nécessaires. Tout changement doit être strictement contrôlé et validé par les équipes métiers.

2. Développement logiciels et sécurité

Objectif A10-2 : prise en compte de la sécurité dans le développement des logiciels. Mener les développements logiciels selon une méthodologie de sécurisation du code produit.

PSSIE-DEV-FUITES : limiter les fuites d'information. Les fuites d'informations techniques sur les logiciels utilisés permettent aux attaquants de déceler plus facilement d'éventuelles vulnérabilités. Il est impératif de limiter fortement la diffusion d'informations au sujet des produits utilisés, même si cette précaution ne constitue pas une protection en tant que telle.

PSSIE-DEV-LOG-ADHER : réduire l'adhérence des applications à des produits ou technologies spécifiques. Le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. En phases de conception et de spécification technique, il est nécessaire de s'assurer que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent (Par exemple : Navigateurs Web déployés sur les postes de travail). En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent. En plus du maintien en condition de sécurité propre à l'application, il est donc nécessaire de pouvoir faire évoluer son environnement pour garantir sa sécurité dans la durée.

PSSIE-DEV-LOG-CRIT : instaurer des critères de développement sécurisé. Une fois passées les phases de définition des besoins et de conception de l'architecture applicative, le niveau de sécurité d'une application dépend fortement des modalités pratiques suivies lors de sa phase de développement.

PSSIE-DEV-LOG-CYCLE : intégrer la sécurité dans le cycle de vie logiciel. La sécurité doit être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

PSSIE-DEV-LOG-WEB : améliorer la prise en compte de la sécurité dans les développements Web. Les développements Web (et les développements en PHP en particulier) font l'objet de problèmes de sécurité récurrents qui ont conduit à la constitution de référentiels de sécurité¹. Ces référentiels ont pour objectif de fixer des règles de bonnes pratiques à l'usage des développeurs. Ce sont des règles d'ordre générique ou pouvant être spécifiques à un langage (PHP, ASP, NET, etc.).

PSSIE-DEV-LOG-PASS : calculer les empreintes de mots de passe de manière sécurisée. Lorsqu'une application doit stocker les mots de passe de ses utilisateurs, il est important de mettre en œuvre des mesures permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute, etc.

¹ A titre d'exemple, il est possible de s'appuyer sur les guides et outils de l'Open Web Application Security Project (OWASP).

MI-DEV-LOG-CLOIS : cloisonnement des traitements sensibles. Lors du développement d'applications métier intégrant des traitements accessibles au citoyen (ou à des tiers) et strictement interne aux services du ministère, il est obligatoire de concevoir l'application de sorte que ces fonctions puissent être déployées sur des serveurs physiquement dédiés. Les bases de données sensibles devront être également installées sur des serveurs accessibles uniquement depuis le réseau du ministère. Les chefs de projet devront identifier les offres d'hébergement ministérielles compatibles avec cette exigence.

MI-DEV-PC-CLOIS : cloisonnement postes de travail des développeurs. Les postes de travail des développeurs doivent être dédiés et ne doivent pas pouvoir accéder directement ou indirectement (par le biais d'un proxy) à Internet ou au réseau bureautique du ministère.

3. Applications à risques

Objectif A10-3 : sécurisation des applications à risques. Accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles.

MI-DEV-FILT-APPL : mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque. Devant les applications à risques exposées à l'extérieur du ministère, il est nécessaire de faire usage d'une solution tierce de filtrage applicatif. Ceci est recommandé pour les applications à risques de l'intranet.