

## DEVELOPPEMENT SECURISE

### RÈGLES DE SÉCURITÉ

Référence	SSI-REG-DEVS_Développement sécurisé_V1.0
Clef GED	262087
Version	V1.0
Classification	Restreint
Date	05/01/2017
État	Validé
Auteur(s)	Filière Sécurité des SI
Approbateur(s)	Sylvain Lambert
Validation	Direction de la Maîtrise des Risques

Identification du document		
Référence	Titre du document	
SSI-REG-DEVS_Développement sécurisé_V1.0	Développement sécurisé	
Version	État du document	Auteurs
1.0	Final	Filière Sécurité des SI

Classification	
Niveau	Diffusion
Restreint	Le personnel <u>de la DSI</u> de Pôle Emploi et à ses tiers formellement autorisés (ayant signé une convention, charte de sécurité, clause de confidentialité)

Mises à jour		
Version	Date	Nature de la modification
0.10	09/12/2016	Création du document dans le cadre de la refonte du référentiel initiée en 2016
0.11	26/12/2016	Maj : prise en compte vulnérabilités OWASP
1.0	05/01/2017	Version finale Pôle emploi

Relectures et validations				
Version	Relu par	Direction	Date	Statut
1.0	RSSI Sylvain Lambert	DSI	05/01/2017	validé
1.0	Robert Laupy	DGA-QMR	09/01/2017	validé

Documents de référence	
Référence	Titre du document
[1] Colibri 196557	Demande de dérogation
[2] Colibri 208129	Guide de développement sécurisé
Colibri 72639	Projets Informatiques

## SOMMAIRE

<b>1.</b>	<b>PRÉAMBULE .....</b>	<b>5</b>
1.1.	Principes fondateurs de la Politique Générale de Sécurité des SI .....	5
1.2.	Enjeux et objectifs du document.....	5
1.3.	Champ d'application .....	5
<b>2.</b>	<b>RÔLES ET RESPONSABILITÉS.....</b>	<b>6</b>
<b>3.</b>	<b>REGLES .....</b>	<b>7</b>
3.1.	Environnement de développement et tests .....	7
3.2.	Formation .....	9
3.3.	Vérification des développements.....	10
3.3.1.	Du ressort du développeur .....	10
3.3.2.	Du ressort du chef de projet .....	14
3.3.3.	Du ressort de la maîtrise d'ouvrage sécurité .....	14
<b>4.</b>	<b>ANNEXES.....</b>	<b>15</b>
4.1.	Liste des règles.....	15
4.2.	Glossaire .....	16

### Règles typographiques

Les termes écrits en vert et soulignés, sont définis dans le glossaire de ce document thématique.

Les règles de la thématique « Développement Sécurisé » sont préfixées par le sigle « **DEVS-** » et sont numérotées par ordre d'apparition. Elles sont définies dans un encart bleu clair comme figuré ci-dessous :

#### *Définition de la règle*

Pour certaines règles, des préconisations, recommandations, commentaires ou des évolutions prévisibles sont détaillés au-dessous de la règle.

#### **Préconisations :**

La maîtrise d'œuvre est orientée vers une solution pour couvrir la règle de sécurité.

#### **Recommandations :**

L'utilisateur est orienté vers un comportement, un usage, afin de respecter la règle de sécurité.

#### **Commentaires :**

Des précisions sont apportées afin d'éclairer la règle énoncée.

## 1. PRÉAMBULE

---

### 1.1. PRINCIPES FONDATEURS DE LA POLITIQUE GÉNÉRALE DE SÉCURITÉ DES SI

Les Systèmes d'Information hébergent de nombreuses données qui revêtent un caractère stratégique et qui constituent un patrimoine essentiel que Pôle Emploi a l'obligation de protéger efficacement.

Pour ce faire, la Direction adopte une Politique Générale de Sécurité des SI qui s'inscrit dans le cadre de la politique de gestion des risques ; cette politique protège les informations et leurs traitements ainsi que les ressources hébergées par les Systèmes d'Information de Pôle Emploi.

### 1.2. ENJEUX ET OBJECTIFS DU DOCUMENT

De par les informations sensibles et les données à « caractère personnel » qui constituent le patrimoine de Pôle Emploi, le développement sécurisé est un thème important de la sécurité des SI.

En effet, une application non sécurisée peut présenter de nombreux vecteurs d'attaque qui pourraient porter atteinte à la Disponibilité, l'Intégrité et la Confidentialité du SI de Pôle Emploi, et plus globalement de son patrimoine informationnel.

Le présent document définit les règles de sécurité relatives au développement sécurisé dans les projets. Il se compose d'un ensemble de règles accompagnées d'un document thématique sur les projets informatiques.

Cet ensemble de règles vient compléter la démarche qualité entreprise par Pôle Emploi dans le domaine du développement d'applications.

### 1.3. CHAMP D'APPLICATION

Le présent document présente les règles à respecter dans le cadre du développement sécurisé dans les projets informatiques du Pôle Emploi, quels que soient la localisation géographique des intervenants et les moyens utilisés.

Ce document s'adresse au personnel (agents) de la DSI de Pôle Emploi et à l'ensemble des tiers fournissant des services de développement informatique.

En cas de non-applicabilité d'une des règles du présent document, une procédure de dérogation doit être engagée. Cette demande de dérogation [1] sera transmise au Responsable Sécurité des Systèmes d'Information.

## 2. RÔLES ET RESPONSABILITÉS

---

Le présent chapitre a pour but de définir les fonctions intervenant dans les processus de définition, d'application et de contrôle des règles de sécurité de Développement Sécurisé.

- **Le Chef de Projet Maîtrise d'ouvrage (MOA)**
  - ▶ Identifie, classe et protège les informations propres du Projet.
  - ▶ Conduit la classification du produit cible du projet, et pilote la définition et la mise en œuvre des mesures de protection appropriées.
  - ▶ Emet des exigences en termes de sécurité des informations propres au Projet et du produit cible du Projet.
  - ▶ Réalise les déclarations CNIL en relation avec le CIL (si nécessaire).
- **Le Chef de Projet Maîtrise d'œuvre (MOE)**
  - ▶ Prend en charge la sécurité informatique du Projet tout au long de sa durée de vie.
  - ▶ Garantit la qualité et la sécurité du Projet conformément aux besoins de sécurité et aux exigences exprimées par la Maîtrise d'Ouvrage. En particulier, décline les exigences de sécurité de la Maîtrise d'Ouvrage en mesures techniques permettant d'assurer un niveau de protection conforme à la classification du produit cible, et de maîtriser les risques identifiés.
- **Les Développeurs**
  - ▶ Toute personne (Pôle Emploi ou tout prestataire) participant au développement informatique de Pôle Emploi.
  - ▶ Elaborent du code dans le respect des règles de l'art en matière de qualité et de sécurité du code.

## 3. REGLES

---

### 3.1. ENVIRONNEMENT DE DÉVELOPPEMENT ET TESTS

#### DEVS- 01 Stockage sécurisé du code source

Tout code source stocké sur une solution de gestion de développement de logiciels (dépôts) doit être accessible uniquement par des personnes habilitées.

#### DEVS- 02 Disponibilité de l'application

Pour garantir la disponibilité de l'application, un livrable issue de la **Gestion de Configuration Logiciel Unifiée (GCLU)**, sous forme de code précompilé de l'application doit être archivé.

**Recommandations :**

Les documents suivants peuvent être également archivés :

- La documentation du projet,
- Les règles fonctionnelles de l'application.

En complément, le code source doit être compréhensible, par l'usage de noms de fonctions / méthodes autoportées.

#### DEVS- 03 Restriction d'accès aux données

L'accès aux données doit être restreint au seul périmètre de l'application ou de la fonction applicative, en appliquant le principe du « moindre privilège ».

**Préconisations :**

- La séparation de la base de données en environnement de production et en environnement hors production (test ou développement) doit être mise en place.
- Dans le cadre d'une maintenance, l'accès en lecture seule à la base de données en production peut être toléré.

## DEVS- 04 Extraction des données hors environnement de production

Dans la mesure du possible, toute donnée qui est amenée à être extraite de l'environnement de production doit être anonymisée.

Dans le cas où le processus d'anonymisation n'est pas possible, les intervenants accédant aux environnements de non-production contenant des données de production doivent posséder les habilitations ad-hoc et signer une charte comprenant un engagement de confidentialité.

### **Préconisations :**

À titre d'exemples, le processus d'anonymisation peut consister à :

- Mélanger des données pour rendre l'information inconsistante,
- Masquer des données (exemple : masquage du mot de passe)



## 3.2. FORMATION

### DEVS- 05 Formation des agents Pôle Emploi

Les développeurs internes Pôle Emploi doivent se maintenir à niveau en matière de bonnes pratiques de développement sécurisé (sensibilisation, formation...).

### DEVS- 06 Formation des tiers

Les tiers doivent s'engager de manière contractuelle à maintenir à niveau leurs développeurs, intervenant pour le compte de Pôle Emploi, en matière de bonnes pratiques de développement sécurisé.

### 3.3. VÉRIFICATION DES DÉVELOPPEMENTS

La phase de vérification doit permettre d'atteindre deux objectifs clés :

- Aider l'entreprise à développer et à maintenir des applications sécurisées,
- Permettre à la DSI de vérifier le niveau de sécurité de l'application.

#### 3.3.1. Du ressort du développeur

En complément des règles ci-dessous qui prennent en considération les 10 vulnérabilités majeures des applications Web citées par l'OWASP (Open Web Application Security Project), il est impératif de suivre les recommandations décrites au sein du document « Guide de développement sécurisé » [2] du tome 3 de la politique de sécurité.

Le développeur peut s'appuyer sur l'usage d'outil afin de contrôler la bonne mise en œuvre de ces référentiels de bonnes pratiques.

#### DEVS- 07 Usage de requêtes paramétrées

Ne pas faire d'accès direct aux bases de données et privilégier les requêtes paramétrées.

**Commentaires :**

L'injection SQL est une des failles les plus répandues dans les applications Web.

**Préconisations :**

Les Requêtes Paramétrées sont la meilleure protection pour les empêcher. Elles regroupent les requêtes préparées et les procédures stockées.

#### DEVS- 08 Usage de données encodées

Les données manipulées par l'application doivent être encodées afin d'éviter les failles XSS.

**Commentaires :**

Le principe de la faille Cross Site Scripting (XSS) est d'injecter un script dans un site vulnérable afin qu'il soit exécuté par le navigateur de la victime.

**Préconisations :**

L'encodage des données, c'est-à-dire le fait de transformer des chaînes de caractères malicieuses en chaînes purement littérales et non interprétables par le navigateur, permet de s'en prémunir.

## DEVS- 09 Filtrage technique des données échangées avec un client

Les données en entrée de l'application doivent être validées (format, type, taille, encodage, caractères interdits...) afin d'éviter tous les types d'injection (SQL, LDAP, de commande, ...).

Toutes modification/migration doit entrainer un nouveau filtrage technique.

### **Commentaires :**

Une attaque courante consiste à injecter des caractères ou commandes interprétables lors d'une interaction du client avec le serveur.

### **Préconisations :**

Différencier (par leur type) les données fiables des données non fiables.

- Pour un formulaire, définir :
  - ▶ Une liste blanche pour les listes de choix à éléments finis.
  - ▶ Une expression régulière pour les dates.
  - ▶ Une liste de caractères autorisés et une taille maximale pour les champs libres.
- Pour un programme java :
  - ▶ Utilisation de l'API Regex

## DEVS- 10 Protection des données en transit

Il faut protéger les flux sortants et entrants d'un composant applicatif, en utilisant des flux chiffrés pour, assurer la confidentialité des données en transit, l'identité du serveur et l'intégrité des données transportées.

### **Commentaires :**

Un flux peut être intercepté, lu et modifié par un attaquant, Il faut donc les protéger pour s'assurer de l'intégrité et de la confidentialité des échanges entre les deux parties.

## DEVS- 11 Auditabilité des évènements sécuritaires

Tout évènement sécuritaire (opérations effectuées par les fonctions de sécurité quel que soit leur résultat (authentification, gestion de session, habilitation), gestions d'erreur, détections d'intrusion, évènements sensibles) doit être journalisé.

### **Préconisations :**

Lors de la sécurisation d'une application, il est nécessaire de penser à la mise en place de contre-mesures, d'audit, de détection des tentatives d'attaque mais également à la journalisation des évènements de l'application tant pour se protéger que pour réagir à une attaque.

## DEVS- 12 Fonction de sécurité des Framework

Il faut exploiter les fonctionnalités de sécurité des Framework et bibliothèques de sécurité

### **Commentaires :**

Le fait d'utiliser un Framework éprouvé reste la plupart du temps plus fiable que de procéder au développement des fonctionnalités voulues.

### **Recommandations :**

Il existe un ensemble de Framework et de bibliothèques qui aident les développeurs à industrialiser leurs développements et leur permet d'utiliser des fonctions déjà éprouvées. Ces outils comprennent dans la majorité des cas, des fonctionnalités de sécurité qu'il est préférable d'utiliser pour se protéger plus efficacement des attaques.

## DEVS- 13 Vigilance envers l'utilisation de codes tiers

Être vigilant sur les vulnérabilités potentielles des bibliothèques utilisées.

### **Commentaires :**

Les failles ne sont pas exclusives au code que vous écrivez, celui des tiers en est une source pernicieuse. Si les dépendances de votre application ne sont pas connues, ne font pas l'objet d'une veille de sécurité, le code le plus sécurisé reposera sur un socle de sable.

## DEVS- 14 Protéger les moyens d'authentification

Les informations d'authentification du client ne doivent être ni accessibles sur le serveur, ni modifiable par un tiers.  
L'application doit privilégier l'utilisation d'un canal différent et sécurisé pour fournir les données d'authentification.

### **Préconisations :**

Il faut chiffrer les mots de passe avant de les stocker ou s'appuyer sur une authentification extérieure.

Les mesures suivantes sont préconisées lorsque l'authentification n'est pas déléguée à un référentiel tiers tel qu'un annuaire mutualisé :

- Stocker les mots de passe sous forme de condensat (hash de mot de passe) sur le serveur.
- Ré-authentifier l'utilisateur avant tout changement de mot de passe.
- Communiquer les informations par mail sécurisé ou face à face.
- Utiliser plusieurs canaux pour communiquer les informations d'authentification, et ne fournir sur un même canal que des informations partielles d'authentification (ex : Un mot de passe dans un mail chiffré dont la clé de déchiffrement est envoyée par SMS).

## DEVS- 15 Téléchargement de fichiers malicieux

Les téléchargements utilisateurs vers l'application doivent être stockés dans un environnement restreint afin d'empêcher les attaquants de déposer des contenus offensifs sur les serveurs.

### **Commentaires :**

Un attaquant utilisera les fonctions de téléchargement vers vos serveurs pour déposer des contenus offensifs. Il est souvent possible par ces fonctions d'écraser des fichiers côté serveur (directement ou indirectement), de faire du contrôle à distance (Web Shell), ou préparer des attaques vers les usagers.

## DEVS- 16 Vérification de code

Le développeur doit réaliser des contrôles sur le code livré et en fournir la preuve à Pôle emploi.

### 3.3.2. Du ressort du chef de projet

#### DEVS- 17 La sécurité en amont

Prendre en compte la sécurité dès les premières phases du projet.

**Recommandations :**

La sécurité n'est pas qu'une affaire de développement. Lors de la conception, notamment de l'architecture d'un système, la sécurité doit être prise en compte et les mesures de sécurité doivent être adaptées aux besoins de l'application. Il est important de connaître la surface d'attaque, les technologies utilisées, de concevoir une application claire et de savoir où sont les points de confiance / méfiance de l'application.

#### DEVS- 18 Contrôle de deuxième niveau

Lors des phases clés du projet de développement, une évaluation systématique de la sécurité du produit doit être effectuée par le chef de projet Maîtrise d'Œuvre (MOE).

**Préconisations :**

Les contrôles possibles sont :

- Une analyse automatisée des applications via des outils intégrés au framework de développement et d'intégration,
- Un scan de vulnérabilité,
- Un test d'intrusion.

### 3.3.3. Du ressort de la maîtrise d'ouvrage sécurité

#### DEVS- 19 Contrôle de troisième niveau

À chaque évolution du SI, un contrôle de sécurité doit être effectué sur les applications web en production et exposées sur Internet.

**Commentaires :**

Un contrôle de sécurité peut correspondre à un scan de vulnérabilités, un test d'intrusion, etc.

## 4. ANNEXES

---

### 4.1. LISTE DES RÈGLES

DEVS- 01	STOCKAGE SÉCURISÉ DU CODE SOURCE .....	7
DEVS- 02	DISPONIBILITÉ DE L'APPLICATION .....	7
DEVS- 03	RESTRICTION D'ACCÈS AUX DONNÉES .....	7
DEVS- 04	EXTRACTION DES DONNÉES HORS ENVIRONNEMENT DE PRODUCTION.....	8
DEVS- 05	FORMATION DES AGENTS PÔLE EMPLOI .....	9
DEVS- 06	FORMATION DES TIERS.....	9
DEVS- 07	USAGE DE REQUÊTES PARAMÉTRÉES.....	10
DEVS- 08	USAGE DE DONNÉES ENCODÉES .....	10
DEVS- 09	FILTRAGE TECHNIQUE DES DONNÉES ÉCHANGÉES AVEC UN CLIENT .....	11
DEVS- 10	PROTECTION DES DONNÉES EN TRANSIT.....	11
DEVS- 11	AUDITABILITÉ DES ÉVÈNEMENTS SÉCURITAIRES.....	11
DEVS- 12	FONCTION DE SÉCURITÉ DES FRAMEWORK .....	12
DEVS- 13	VIGILANCE ENVERS L'UTILISATION DE CODES TIERS .....	12
DEVS- 14	PROTÉGER LES MOYENS D'AUTHENTIFICATION .....	12
DEVS- 15	TÉLÉCHARGEMENT DE FICHIERS MALICIEUX .....	13
DEVS- 16	VÉRIFICATION DE CODE.....	13
DEVS- 17	LA SÉCURITÉ EN AMONT .....	14
DEVS- 18	CONTRÔLE DE DEUXIÈME NIVEAU.....	14
DEVS- 19	CONTRÔLE DE TROISIÈME NIVEAU.....	14

## 4.2. GLOSSAIRE

### Code précompilé

La compilation est un processus qui transforme un code source écrit en langage de programmation (langage source) facilement compréhensible par l'humain en un autre langage informatique (langage cible) exploitable par la machine.

La pré-compilation ou semi-compilation est un processus qui transforme le langage source en un langage intermédiaire sous forme binaire, avant d'être lui-même interprété ou compilé.

### Confidentialité

La confidentialité est la propriété qui garantit que les informations ne sont accessibles que par des personnes dûment habilitées et que les informations ne peuvent pas être divulguées en dehors des règles établies.

Cette garantie peut être mise en cause par des indiscretions, volontaires ou involontaires, quel que soit le support utilisé (réseau, support physique, etc.).

### Disponibilité

La disponibilité est l'aptitude d'un système d'Information à pouvoir être employé par les utilisateurs (individus, entités, processus...) habilités dans des conditions d'accès et d'usage normalement prévues (conditions d'horaires, de délai, de performances...).

### Données à « caractère personnel »

Au sens de la loi Informatique & Libertés (n°78-17 du 6 janvier 1978 complétée par la loi du 6 août 2004), une donnée à caractère personnel est une information relative à une personne physique identifiée ou identifiable, directement ou indirectement. Il s'agit de tout :

- Élément d'identification directe (ex : prénom, nom patronymique, numéro de sécurité sociale...)
- Élément propre à la personne et/ou permettant indirectement son identification (ex : photo, numéro de téléphone, adresse IP délivrée par un FAI...)

Le traitement de données à caractère personnel est régi et cadré par la loi Informatique et Libertés, qui soumet le responsable du traitement à des obligations vis-à-vis de la CNIL et des personnes intéressées par le traitement.

### Intégrité

L'intégrité est la propriété qui assure qu'une Information n'est modifiée que par les utilisateurs habilités dans des conditions d'accès normalement prévues. L'intégrité doit garantir l'exhaustivité, l'exactitude et la fiabilité de l'Information.

L'intégrité peut être remise en cause par toute altération ou modification non légitime.



---

**Sensible**

La classification des informations repose sur la notion suivante : le propriétaire d'informations classifie ses informations et définit leur niveau de sensibilité (non sensible, Sensible, Critique, Stratégique) duquel est déduit le niveau de protection et de service à mettre en œuvre.

---

**Tiers**

Le terme « Tiers » désigne l'ensemble des stagiaires, des prestataires, des fournisseurs, des partenaires et des travailleurs intérimaires employés à titre individuel par Pôle Emploi ; ces personnels sont amenés à travailler, de manière permanente ou occasionnelle, sur les Systèmes d'Information de Pôle Emploi et, de ce fait, à avoir accès à des informations ou à des ressources de Pôle Emploi.

---

(Fin de document)