Ligne directrice sécurité de l'information et vie privée

Achat, conception, développement et maintenance d'applications

(BLD APPDEV)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie relative à la sécurité de l'information et à la vie privée au sein de la sécurité sociale. Ce document est destiné aux responsables et aux sous-traitants de l'information, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de sécurité sociale (IPSS), aux responsables de projet et à l'ensemble des parties impliquées dans les projets TIC.

Pour une organisation optimale de la protection, il est essentiel que les conditions de sécurité soient définies dès la phase de conception d'un projet.

Le présent document traite les aspects relatifs à la sécurité de l'information et à la protection de vie privée lors de l'achat, de la conception, du développement et de la maintenance dans le cadre des projets TIC.

2. Conditions de sécurité lors de l'achat, de la conception, du développement et de la maintenance d'applications

Toute organisation souscrit les directives suivantes relatives à la sécurité de l'information et à la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation:

2.1. Classification des données

Dans chaque phase d'un projet, une attention particulière sera accordée aux mesures relatives à la sécurité de l'information et à la protection de la vie privée appliquées au traitement des données, manipulées en fonction de leur classification.

Dès le lancement d'un projet il est capital de réaliser une analyse des risques encourus en fonction de la classification des données. A cet égard, l'attention utile sera accordée aux risques relatifs à la sécurité et à la vie privée[1]. Une attention spécifique doit être accordée à la protection des données de base cryptographiques (clés, certificats, ...) qui ne peuvent jamais être sauvegardées dans un système sous une forme non sécurisée (ISP).

Des mesures doivent être prises pour éviter la perte, la modification ou l'abus d'informations échangées avec d'autres organisations.

2.2. Exigences réglementaires

2.2.1. EU GDPR et loi BCSS

Il y a lieu de veiller au respect des conditions légales et des exigences relatives à la sécurité auxquelles les systèmes d'information utilisés sont soumis.

2.2.2. Autorisations du Comité sectoriel

Une autorisation du Comité sectoriel compétent est requise pour permettre à une organisation d'exploiter des données à caractère personnel lorsqu'elle n'est pas le propriétaire de ces données.

[1] L'évaluation des risques permettra par exemple de déterminer la nécessité de méthodes cryptographiques pour la préservation de la confidentialité, de l'authenticité et de l'intégrité des données. Ces techniques peuvent aussi contribuer à la non-réfutabilité des transactions.

2.2.3. Force probante

Si la force probante est requise, le dossier doit être soumis aux instances compétentes. Le contexte de la force probante est défini dans des arrêtés royaux[2].

2.2.4. Dossier unique

Au sein de la sécurité sociale, une procédure a été instaurée pour contrôler les aspects légaux, les aspects relatifs à la sécurité et à la vie privée lors de la mise en service (mise en production) d'une application. Cette validation est formalisée dans un « dossier unique » (aspects légaux lors de la mise en production d'une nouvelle application). Ce dossier est obligatoire pour les applications hébergées sur le portail de la sécurité sociale et la Plate-forme eHealth. Ce dossier centralise les informations nécessaires permettant aux gestionnaires du système de la sécurité sociale de mettre en production une application, conformément à la législation relative à la sécurité de l'information et à la protection de la vie privée.

2.2.5. Autorisations BCSS

Si des services électroniques (tels des services web) de la BCSS sont utilisés, il faut demander l'autorisation à cet effet en temps utile.

2.3. Directives

Les points suivants sont imposés par les directives relatives à sécurité de l'information et à la protection de la vie privée telles que fixées par le Comité sectoriel de la sécurité sociale et de la santé. Dans la mesure où il existe une directive spécifique qui correspond au sujet, cette directive doit être respectée et appliquée.

2.3.1. Communication

Une communication efficace et constructive doit être établie entre les différentes parties concernées par le projet (en ce compris avec les clients et les fournisseurs), en particulier envers le(s) conseiller(s) en sécurité. Ceci doit garantir un niveau adéquat de sécurité de l'information et de vie privée connu de tous.

De même, ces acteurs doivent être informés quant à leurs responsabilités personnelles telles que décrites dans le « Code de bonne conduite pour les gestionnaires d'information » ou dans un code déontologique inhérent à leur fonction spécifique:

- la limitation de consultation de données confidentielles à des fins strictement professionnelles
- le secret des données confidentielles.

2.3.2. Gestion des accès

Tous les collaborateurs et en particulier les collaborateurs externes (tels les consultants, les contractants, les intérimaires, les stagiaires, les étudiants-jobistes) qui utilisent des outils TIC mis à la disposition par l'institution le font sur la base d'autorisations limitées à l'exécution de leur tâche.

Lors du développement de la protection des accès, il est essentiel de tenir compte des systèmes de gestion des accès déjà opérationnels (tels l'UAM) ainsi que de leurs évolutions. L'utilisation de ces systèmes garantira l'indépendance entre ce système de gestion et le système développé.

Les exigences relatives à la sécurisation des accès (identification, authentification, autorisation) doivent être définies, documentées, validées et communiquées. Le niveau de sécurisation des accès (tel la nature du moyen d'authentification) doit être adapté en fonction de l'application (p.ex. degré de confidentialité des données traitées) et de la menace (p.ex. accès via des réseaux publics) sur la base d'une analyse des risques. Ces accès font l'objet d'une prise de traces.

[2] https://www.ksz-bcss.fgov.be/fr/force-probante-nouvelle-approche-pour-le-controle-des-dossiers-en-vue-de-lobtention-dune-agreation

Sachant que dans le cadre d'une application, des groupes différents d'utilisateurs peuvent détenir des droits distincts (p.ex. lecture, écriture, modification) en fonction des degrés de confidentialité des données, il est nécessaire de tenir de la granularité de l'accès aux données.

Il y a lieu d'éviter dans toute la mesure du possible la gestion des accès dans une application. Dans des cas exceptionnels, il faut disposer de procédures formelles permettant de gérer l'ensemble des phases du cycle de vie de la protection des accès (introduction, contrôle sur la base d'un inventaire, mutation, suppression) (ISP).

Lorsqu'un programme est développé dans lequel l'institution de sécurité sociale reprend un numéro de programme dans un message qu'elle adresse à la BCSS, bien qu'une personne physique soit à l'origine de ce message, cette organisation doit être en mesure d'établir elle-même la relation entre ce numéro de programme et l'identité de la personne physique qui envoie ce message.

2.3.3. Sous-traitance à des tiers

En cas de sous-traitance d'activités TIC, une attention particulière est consacrée aux risques relatifs à la sécurité et à la protection de la vie privée. Il est crucial de fixer ces aspects dans un contrat. Il y a lieu de prévoir des clauses de confidentialité et de continuité.

2.3.4. Check-list

Le chef de projet doit toujours prévoir une liste de contrôle. Sur cette base, il peut s'assurer que l'ensemble des directives relatives à la sécurité de l'information et à la protection de la vie privée sont correctement évaluées et sont, si nécessaire, mises en œuvre durant la phase de développement du projet.

2.3.5. Contrôle avant la mise en production

Lors de la mise en production du projet, le responsable du suivi, à savoir le chef de projet, doit s'assurer que les conditions relatives à la sécurité et à la protection de la vie privée qui ont été fixées au début du projet sont effectivement mises en œuvre.

2.3.6. Approche structurée

Les dispositifs de développement, de test et/ou d'acceptation et de production sont scindés et le partage des responsabilités qui en découle est réalisé dans le cadre du projet. Le tout se fait sous la supervision du chef de projet.

2.3.7. Gestion des logs

Dans les spécifications d'un projet, il y a lieu de préciser comment l'accès et l'utilisation des systèmes et des applications seront logs, afin de contribuer à la détection d'anomalies par rapport aux directives relatives à la sécurité de l'information et à la vie privée. Les logs doivent être conçus de manière conforme à la directive logging.

Il y a lieu de tenir compte des systèmes de log existants lors de l'évaluation des besoins de logging dans le cadre du présent projet. Ceci afin d'éviter qu'un système de logging spécifique ne soit développé par projet. Ce qui permet également de garantir l'indépendance entre le système de log et le projet.

2.3.8. Sauvegarde/restauration

Le chef de projet doit s'assurer que le projet puisse être intégré dans le système de gestion des sauvegardes de l'organisation comme imposé dans les directives. Ceci concerne non seulement les données qui sont traitées mais aussi la documentation qui y a trait (code source, programmes, documents techniques, ...). La sauvegarde doit régulièrement être testée au moyen d'un exercice de restauration (« restore ») afin de vérifier que les informations puissent effectivement être récupérées et de déterminer le délai nécessaire pour cette mission de reprise.

2.3.9. Gestion de la continuité

Au cours du développement du projet, les besoins relatifs à la continuité de la prestation de services doivent être formalisés, conformément aux attentes de l'organisation.

Les points suivants doivent être respectés:

- Les programmes doivent intégrer des points de redémarrage clairement définis afin de faire face à des problèmes opérationnels . Ces informations font partie du dossier d'exploitation.
- Au cours du développement d'un projet, il y a lieu d'accorder une attention particulière à une sauvegarde et à une restauration (« restore ») des informations.
- Dans l'environnement de production, il y a lieu de tenir compte des exigences de l'institution en ce qui concerne la tolérance aux problèmes et la redondance de l'infrastructure
- Le plan de continuité et les procédures y afférentes, en ce compris les tests de continuité, doivent être actualisés en fonction de l'évolution du projet.

En fonction de l'analyse des risques réalisée au début du projet, il y a lieu de définir des procédures d'urgence. Celles-ci concernent notamment les aspects suivants.

- Le fonctionnement en cas de disponibilité réduite des systèmes d'information
- La description de systèmes d'information alternatifs, en ce compris le déploiement, les modalités d'exploitation et le développement éventuel de systèmes d'urgence
- Les tâches et procédures clés en cas d'interruption du système
- Les tâches, les rôles clés et les moyens à mettre en œuvre afin de garantir une disponibilité optimale.

2.3.10. Gestion des incidents

Les procédures relatives à la gestion des incidents doivent être formalisées et validées au cours du développement d'un projet. Ceci doit permettre d'intégrer le système développé dans le système de gestion standard des incidents de l'organisation. Le conseiller en sécurité doit être informé des incidents relatifs à la sécurité et à la vie privée.

2.3.11. Documentation

La documentation (technique, procédures, manuels, ...) doit être actualisée au cours de la durée de vie du projet.

2.3.12. Inventaire

Tous les actifs, en ce compris les systèmes acquis ou développés, doivent être ajoutés au système de gestion des moyens opérationnels (inventaire).

2.3.13. Audit

La collaboration appropriée à des fins d'audit interne et externe sera apportée sous la forme de mise à la disposition du personnel, de la documentation, de la gestion des traces et des autres informations qui sont raisonnablement disponibles.

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description de la modification	Date approbation	Date entrée en vigueur
2007	JC	V2007	Première version	10/10/2007	01/11/2007
2011	PB	V2011	Deuxième version	29/03/2011	01/04/2011
2017	M. Vael	V2017	Intégration UE GDPR	07/03/2017	07/03/2017
2018	Groupe de travail policy	V2018	Adaptation suite à modification dans BLD LOG	06/02/2018	01/01/2019

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 p.
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 p.
- ISO, "ISO/IEC 27034:2011 Security Techniques – Application Security", November 2011, 67 p.
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 p.

Ci-dessous figurent les références aux sites web qui ont service de source d'inspiration pour le présent document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- https://www.iso.org/standard/44378.html
- http://www.isaca.org/cobit
- https://www.owasp.org
- http://www.webappsec.org/
- http://www.ccb.belgium.be/fr/work
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

Annexe C: Secure project lifecycle

Initialisation

Non seulement les exigences du projet mais aussi les conditions relatives à la sécurité et à la protection de la vie privée doivent être examinées et définies en concertation avec le donneur d'ordre dès le début du projet. Le(s) conseiller(s) en sécurité et le DPO du (des) donneur(s) d'ordre et de l'organisation ou des organisations concernées doivent être impliqués à cet effet.

Planification

Le planning du projet doit tenir compte du temps et des moyens nécessaires afin d'aussi réaliser les aspects relatifs à la sécurité et à la vie privée.

Il y a lieu d'éviter de contourner les directives relatives à la sécurité et à la vie privée afin de privilégier d'autres aspects du projet (par exemple, par manque de temps ou pour des raisons budgétaires). S'il y a tout de même un contournement, celui-ci doit être argumenté et confirmé formellement sur la base d'une analyse des risques. Toutes les dérogations doivent faire l'objet de mesures correctrices afin d'atteindre les objectifs initiaux en matière de sécurité et de protection de la vie privée.

Réalisation

- ***Développement et test***

Lors du développement et des tests, il y a lieu de tenir compte des faiblesses susceptibles d'être exploitées pour compromettre les applications.

Un programme de formation, adapté aux différentes responsabilités, doit est prévu. L'attention nécessaire doit être accordée aux risques relatifs aux applications et aux contre-mesures.

Il est dès lors capital de vérifier que les collaborateurs aient suivi la formation nécessaire pour prendre conscience des menaces existantes et de l'importance de la sécurité de l'information et de la vie privée et qu'ils aient à leur disposition les moyens, connaissances et aptitudes adéquats pour protéger les systèmes contre ces menaces.

L'attribution des rôles et droits d'accès spéciaux et critiques pendant la phase de développement (p.ex. pour la gestion des versions logicielles) doit être limitée et leurs utilisations contrôlées.

- Les méthodes d'authentification (telles les mots de passe/phrases de passe) et les niveaux d'autorisation (tels celui d'administrateur) doivent être gérés au moyen d'une procédure formelle.
- Les collaborateurs doivent être sensibilisés à leur responsabilité quant au maintien d'une protection des accès effective.

Lors du développement de systèmes, une attention particulière doit être accordée à l'intégrité des données, par exemple par la validation des données dès leur introduction, par la sécurisation du traitement interne et par la validation des données en sortie. Des traces auditables doivent être intégrées.

Lors du développement de systèmes, il doit être tenu compte des points faibles de sécurité (et de protection de la vie privée) inhérents aux langages de programmation. La vérification des logiciels par des tiers, autres que les développeurs, constitue une méthode pour réduire ces risques. Si un tiers se charge de la vérification, il y a lieu de vérifier sa déontologie.

Pendant le développement, l'intégrité et la cohérence du logiciel sont garanties par une gestion procédurale des versions du logiciel et la sécurisation des accès aux bibliothèques logicielles (ISP).

Des mesures maximales doivent être prises pour éviter que des canaux de communication secrets (« cover channels »)[3] et des chevaux de Troie[4] ne se cachent dans les logiciels développés.

[3] Ces canaux de communication secrets permettent d'utiliser par la suite ces logiciels à mauvais escient.

En vue de la gestion de la continuité, les programmes contiennent des points de redémarrage clairement définis pour faire face à des problèmes opérationnels.

L'accès à ces systèmes et l'utilisation de ces systèmes doivent être contrôlés afin de détecter des dérogations à la politique d'accès ou des anomalies.

La documentation des développements de nouveaux systèmes et de la maintenance de systèmes existants est obligatoire. Ceci permet aux successeurs des développeurs initiaux de gagner du temps précieux.

Ceci comprend la réalisation par le chef de projet d'une cartographie fonctionnelle et d'une cartographie technique. Chacune de ces cartographies décrit jusqu'au niveau adéquat les divers flux de données, les différents éléments pertinents (serveurs, ...) et leur rôle dans le projet (serveurs applicatifs, banque de données, ...).

Il y a lieu de manipuler les données de test avec précaution afin d'éviter la compromission de données professionnelles, confidentielles et sensibles. A des fins de développement, seules des données de test spécialement prévues à cet effet seront utilisées. Il y a lieu de donner une approbation explicite chaque fois que des données de production sont copiées dans d'autres environnements (de test). À cet effet, soit les données de production sont dépersonnalisées, soit l'autre environnement (de test) hérite des mêmes conditions relatives à la sécurité de l'information et à la protection de la vie privée qui sont valables dans l'environnement de production. Les informations provenant d'autres environnements (de test) doivent être supprimées directement dès que les tests sont terminés. Il faut disposer d'un aperçu central de l'ensemble des flux d'information entre les environnements de production, d'entraînement, de pré-production, de référence, d'intégration, d'acceptation, de test et de développement. Cet aperçu doit pouvoir permettre de déterminer quelles données se trouvent dans quel environnement et quelles données sont protégées de quelle manière. Il y a lieu de rédiger, de valider, de communiquer et d'appliquer des procédures pour un transfert sécurisé des données entre l'environnement de production et les autres environnements.

- ***Mise en production***

A ce stade, il faudrait traiter, analyser et valider les aspects suivants avec les personnes responsables de la mise en production et de l'exploitation, et ce conformément aux exigences des utilisateurs.

- La désignation d'un collaborateur ayant le rôle de « propriétaire de l'application » qui est responsable pour le système développé (évolution, documentation, point de contact, ...).
- La fourniture par le chef de projet d'une version définitive de la cartographie technique et fonctionnelle (as built). Ces documents permettent aux gestionnaires systèmes (gestionnaires réseau, gestionnaire banque de données, ...) d'actualiser leur propre cartographie.
- La conformité du projet et des flux de données associés aux autorisations accordées par le Comité sectoriel.
- La conformité du projet aux nécessités de continuité de services définis.
- La disponibilité de la documentation et de manuels (p.ex. le dossier de production).
- La définition des données à archiver, du support d'enregistrement, des délais de conservation, du chiffrement éventuel
- Le respect des conditions relatives à la sécurité de l'information et à la vie privée dans l'environnement de production (confidentialité, intégrité, disponibilité, force probante)
    - Conditions de confidentialité:
        - Identification
        - Authentification forte
        - Autorisation
        - Chiffrement
        - Contrôle d'accès
        - Traçage et surveillance de l'accès
    - Conditions d'intégrité (authenticité):
        - Traitement de données dans les applications

[4] Le cheval de Troie est le terme général utilisé pour désigner un type de logiciel illicite qui fait exécuter des fonctions autres que celles initialement prévues par le logiciel autorisé (dans lequel ce logiciel illicite est caché).

- Contrôles d'intégrité
- Traçage et surveillance des activités

- Conditions de disponibilité:
  - Redondance système
  - Plans de sauvegarde et de restauration (« restore »)

- Les moyens pour réaliser un certain archivage doivent être préparés. Il y a lieu d'accorder une attention particulière à la définition des données à archiver, au support d'enregistrement, aux délais de conservation, au chiffrement éventuel, ...
  Remarque: en vue du respect des dispositions légales relatives à la conservation et à l'utilisation de données archivées, il y a lieu de vérifier à chaque évolution de l'infrastructure informatique et du système informatique qui a un impact sur l'archivage, si les données archivées, les supports d'enregistrement et les applications nécessaires à leur exploitation sont toujours en adéquation.
- Par ailleurs, les méthodes décrites dans le dossier relatif à la force probante doivent, le cas échéant, être scrupuleusement respectées.
- Pour l'approbation d'une application jusqu'à sa mise en production sur le portail de la sécurité sociale, il y a lieu de suivre une procédure stricte de la BCSS (dossier unique).
- Les moyens et compétences nécessaires doivent être mis à la disposition pour une intervention urgente en cas de problèmes au cours de la phase de production.

Clôture

Le responsable du projet, le responsable d'exploitation des données ainsi que le responsable du traitement des données doivent veiller ensemble à ce que le système livré soit en phase avec l'autorisation accordée (p.ex. flux à ouvrir).

Annexe D: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Sécurité des ressources humaines	
Gestion des actifs	
Protection de l'accès	
Cryptographie	**Oui**
Sécurité physique et environnementale	
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	**Oui**
Relations avec les fournisseurs	
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	

***** FIN DU DOCUMENT *****