SOMMAIRE D'UN PLAN D'ASSURANCE SECURITE

v 1.0 (Mai 2023)

Table des Matières

1.1 INTRODUCTION ET OBJET DU DOCUMENT 3
1.2 POSITIONNEMENT DU DOCUMENT DANS LE REFERENTIEL DOCUMENTAIRE SSI 3
1.3 PERIMETRE D'APPLICATION ET ACTEURS CONCERNES 4
1.4 DUREE DE VALIDITE DE LA PSSIO, MODE DE REVISION ET DE MODIFICATION 4
2 CHAPITRES ATTENDUS D'UN PAS POUR ONF 5
2.1 DEFINITION 5
2.2 PERIMETRE ET ACTEURS 5
2.3 CHAPITRES ATTENDUS 5
2.4 AUTRES ELEMENTS (FACULTATIF) 7

	Rédacteur	Vérificateur	Approbateur
Fonction	Responsable de Sécurité des Systèmes d'Information de BPF	Responsable de Direction Sécurité & Réseaux	Responsable des Systèmes d'Information
Nom	ZYCHOWSKI G.	KOLOCZEK D.	COMBETTES A.
Signature			

Stockage

Traduction

Table des évolutions

Date d'application	Indice de Révision	Nature de la révision	N° des chapitres modifiés
15/06/2023	1.0	Création	

1.1 Introduction et objet du document

Ce document décrit les éléments qui doivent être présents dans un Plan d'Assurance Sécurité (PAS) document contribuant à garantir le niveau de sécurité d'un fournisseur et corollaire à l'analyse de risque de celui-ci, le cas échéant.

1.2 Positionnement du document dans le référentiel documentaire SSI

Le présent document fait partie du référentiel documentaire SSI de l' Office National des Forêts structuré de la manière suivante :

- Niveau 1 : Il s'agit du document chapeau définissant les cadres déontologiques et réglementaires dans le domaine de la Sécurité des Systèmes d'Information et de Poursuite d'Activité de Office National des Forêts;
- Niveau 2 : Il est constitué d'une série de politiques techniques de sécurité définies par thèmes éventuellement complétées de Directives de Sécurité de l'ANSSI, applicables à ONF;
- Niveau 3 : Il est constitué des documents dits de support et d'accompagnements qui précisent les règles, les procédures et les processus communs et/ou transverses à respecter qui favorisent un déploiement cohérent des dispositifs de sécurité et de poursuite d'activité. Ces

documents sont destinés aux opérationnels qui doivent respecter les procédures et méthodes qui y sont définis.

Le présent document est un document de niveau 3 qui doit être lu et connu des personnels ayant le besoin d'en connaître ou des opérationnels devant respecter les procédures et méthodes qui y sont définies, en fonction de leur rôle dans la sécurité des SI de Office National des Forêts.

1.3 Périmètre d'application et acteurs concernés

1.3.1 Applicabilité

Cette politique est applicable dans toutes les entités françaises et étrangères de Office National des Forêts. D'éventuels compléments peuvent y être apportés, sous forme d'addendum dans des documents indépendants, pour chacune des entités à l'étranger qui aurait à respecter une règlementation locale dont les enjeux en termes de maîtrise des risques portant sur les Systèmes d'Informations seraient plus exigeants.

1.3.2 Qui doit connaître cette politique de niveau 3

Elle s'adresse essentiellement aux :

- Réseau SSI de ONF ;
- Réseau SSI DT-DR (via les RIT et SSR);
- Auditeurs et corps de contrôle ;
- Toutes les équipes de la DSI de ONF ;
- Tout collaborateur de l'ONF, , ses filiales, ses succursales ou tout autre partenaire dans lequel ONF détient au moins 51% des parts, en France et à l'étranger et qui intervient dans les projets SI.

1.4 Durée de validité de la PSSIO, Mode de Révision et de Modification

1.4.1 Durée de validité de la PSSIO

Les trois niveaux de documentation constituant la PSSIO (PSSI de l'ONF) ont une durée de validité pérenne, afin d'en garantir l'adéquation avec les problématiques de sécurité. Ils sont soumis à une périodicité de révision et en cas de besoin de modification. Ce document de PSSI de niveau 3 fait partie du corpus global de la PSSIO, qui est donc soumis à cette temporalité.

1.4.2 Révision et modification de la PSSIO

La périodicité de révision et de modification des 3 niveaux de documents constituant la PSSIO est variable en fonction du niveau :

- **Niveau 1** : la PSSIO de niveau 1 fait l'objet d'une révision annuelle qui pourra ou non, selon le cas, donner lieu à des modifications ;
- **Niveau 2** : compte tenu du nombre de Politiques de niveau 2, elles ne pourront pas faire l'objet d'une révision annuelle. Elles seront révisées tous les 3 ans par tranches de 4 ou 5 documents, pour tenir compte notamment des évolutions techniques ou fonctionnelles. Selon les évolutions constatées, elles feront l'objet des modifications correspondantes ;
- **Niveau 3** : les procédures, modes opératoires, etc., constituant le corpus des Politiques de niveau 3, seront révisés et modifiés en fonction des évolutions techniques, fonctionnelles, organisationnelles, etc., chaque fois que cela s'avèrera nécessaire.

2 CHAPITRES ATTENDUS D'UN PAS POUR ONF

2.1 Définition

Dans le cadre de la démarche de cadrage sécurité des projets de ONF, et notamment vis-à-vis des projets en liaison avec un ou plusieurs fournisseurs externe, un Plan d'Assurance Sécurité, aussi nommé PAS, doit désormais accompagner les éléments documentaires fournis par ce dernier dans le cadre de la prestation envisagée. Le Plan d'Assurance Sécurité (PAS) doit être élaboré et annexé au contrat.

2.2 Périmètre et acteurs

Ce document doit permettre aux équipes de la DSI de ONF, et notamment au RSSI de ONF, d'obtenir une vue consolidée des principaux dispositifs de sécurité que le fournisseur met en œuvre dans la protection des biens opérés ou fournis pour le compte de ONF. Il constitue la réponse du fournisseur aux exigences de sécurité demandées par ONF. Un point formel peut être organisé entre le RSSI de l'ONF et la personne en charge de la sécurité côté fournisseur pour valider la conformité du PAS aux attendus indiqués ci-dessous.

2.3 Chapitres attendus

Dans la suite du document, nous mentionnons les chapitres attendus dans le PAS. Pour chacun d'entre eux on précise s'il est obligatoire ou facultatif suivant la prestation.

2.3.1 Introduction (obligatoire)

Objectif du document, documents applicables dont PSSI du fournisseur et tout autre document établissant les standards de sécurité en vigueur chez le fournisseur, processus de mise à jour du document, glossaire et définitions des termes utilisés.

2.3.2 Structuration du document (obligatoire)

Description précise de chaque chapitre abordé dans le document.

2.3.3 Modalités de révision du PAS (obligatoire)

Le Plan d'Assurance Sécurité doit être revu régulièrement en tenant compte notamment : de l'évolution des lois et règlementations, des évolutions des prestations délivrées, qu'elles soient organisationnelles ou techniques, de l'évolution des risques, notamment pour prendre en compte les éventuels incidents.

Ce chapitre mentionnera les modalités et fréquence de révision du PAS.

2.3.4 Organisation de la Sécurité de l'information (obligatoire)

Description d'un éventuel SMSI chez le fournisseur, méthodologie d'analyse de risque utilisée, rôles et responsabilités dans le cadre de la prestation, pilotage opérationnel de la sécurité, gestion et déclaration des incidents de sécurité, gestion des évolutions techniques, ou organisationnelles le cas échéant…

2.3.5 Gestion des biens/données du client (obligatoire)

Maitrise des configurations, sécurité des données confiées par le client, sécurité des données crées par l'applicatif, localisation des données et des centres d'exploitation dans lesquels elles sont traitées.

2.3.6 Sécurité des RH (obligatoire)

Contrôles à l'embauche, engagement de confidentialité, sensibilisation à la sécurité, processus de terminaison, les modalités d'appel à de la sous-traitance par le fournisseur.

2.3.7 Sécurité physique et environnementale (obligatoire)

Principales mesures de sécurité des sites du fournisseur, y compris ceux existants dans les Datacenter opérés par ou pour le compte du fournisseur ; description du ou des mécanismes de sauvegarde/restauration des données du client, algorithme de sauvegarde choisi (GFS, etc..) et durée de rétention définie…

2.3.8 Gestion de l'exploitation et télécoms (obligatoire)

Protection contre les codes malveillants, protection des environnements de travail, des réseaux, sauvegardes-restaurations, surveillance des journaux, politique de gestion de vulnérabilités,

La localisation de l'exécution des prestations et celle de ses centres de traitement de données, les modalités d'appel à de la sous-traitance par le fournisseur.

Ce chapitre intégrera également les points suivants à expliciter :

- la description du ou des mécanismes de sauvegarde/restauration des données du client, algorithme de sauvegarde choisi (GFS, etc..) et durée de rétention définie…

- Les principes de durcissement adoptés et le périmètre choisi : base de données, serveurs, réseaux et développements informatiques dans le cadre de la prestation choisie

- les principes retenus pour la gestion du changement (cf. norme ITIL)

- le principe des règles de calcul pour le dimensionnement de l'architecture (et l'adaptation des besoins au client).

Dans ce chapitre sera également mentionnée l'obligation pour le fournisseur d'informer BPF de tout changement de localisation des data center où sont exploitées les données de BPF.

2.3.9 Contrôle d'accès physique (obligatoire)

Description des mécanismes de contrôle des accès des sites du fournisseur, y compris les Datacenter opérés par ou pour le compte du fournisseur, revues de droits des populations à privilèges, etc…

2.3.10 Contrôle d'accès logique (obligatoire)

Description des moyens de contrôle d'accès logique, en mode Saas description des profils d'accès à l'application.

2.3.11 Acquisition, développement et maintenance des SI du fournisseur (suivant solution)

Principes de développements sécurisés utilisés, test et audit de code déroulés sur l'applicatif ou les procédures mises en œuvre

2.3.12 Gestion du Plan de Continuité d'Activité (obligatoire)

Description de l'approche retenue concernant la continuité d'activité : plan de secours informatique, plan de poursuite d'activité, plan de reprise d'activité suivant la gravité de l'impact ; définition des indicateurs de reprise (RTO, RPO) applicables à la solution proposée.

2.3.13 Conformité et audits (obligatoire)

Exigences légales, certifications obtenues par le fournisseur qui entrent dans le champ de la prestation, tests d'intrusion et demandes d'audit par les corps de contrôle du client ou ses organisations internes.

Dans ce chapitre sera également explicité l'obligation pour le fournisseur de permettre des audit mandaté ou piloté par BPF.

2.3.14 Réversibilité (suivant solution)

Description des moyens proposés pour la récupération des données de BPF en fin de vie du contrat ou en cas de rupture de celui-ci (moyen technique, délai, suppression des données du client, garantie d'effacement…)

2.3.15 Recensement et référencement des procédures opérationnelles liées à la prestation sous l'angle Sécurité des SI (obligatoire)

Le document indiquera également le responsable chargé de la mise en œuvre de ces mesures et les modalités de suivi du bon déploiement de ces mesures.

2.3.16 Organisation du suivi, KPI et tableaux de bord (obligatoire)

Description des indicateurs de suivi de la sécurité en conformité avec les modalités accordées entre les parties et les tableaux de bord doivent être publiés.

2.4 Autres éléments (facultatif)

Description des éléments spécifiques à la prestation pour prendre en compte une spécificité non mentionnée dans les autres chapitres du PAS ; on y trouvera notamment la réponse du fournisseur aux obligations réglementaires (ex. GDRP)

Réponse du fournisseur aux risques résiduels identifiés par l'analyse de risque menée initialement entre l'ONF et le fournisseur.