

NomProjet

Plan d’assurance sécurité (PAS)

Date :

Version :

Référence : PAS-cadre-de-reponse.odt

Suivi du document :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Date | Auteur | Vérification | Approbation | Modifications |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Diffusion :

|  |  |  |
| --- | --- | --- |
| Prénom Nom | Organisation / Direction / Service | Fonction |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Sommaire

[1 Objet 3](#__RefHeading___Toc19264_560750809)

[1.1 Objet du document 3](#__RefHeading___Toc19259_560750809)

[1.2 Documents de référence 3](#__RefHeading___Toc19261_560750809)

[1.3 Description du système 3](#__RefHeading___Toc19266_560750809)

[1.4 Rappel des exigences 3](#__RefHeading___Toc19268_560750809)

[2 Organisation de la sécurité 4](#__RefHeading___Toc19270_560750809)

[2.1 Organisation générale de la sécurité 4](#__RefHeading___Toc23327_560750809)

[2.2 Chaîne de sécurité du candidat 4](#__RefHeading___Toc23329_560750809)

[2.3 Relation avec des groupes de travail spécialisés 4](#__RefHeading___Toc23366_560750809)

[3 Présentation du PAS 5](#__RefHeading___Toc19272_560750809)

[3.1 Responsabilités liées au PAS 5](#__RefHeading___Toc19284_560750809)

[3.2 Procédure d’évolution du PAS 5](#__RefHeading___Toc19278_560750809)

[3.3 Applicabilité du PAS 5](#__RefHeading___Toc19280_560750809)

[4 Mesures de sécurité 7](#__RefHeading___Toc19282_560750809)

[4.1 Sécurité et ressources humaines 7](#__RefHeading___Toc23297_560750809)

[4.2 Gestion des actifs 7](#__RefHeading___Toc23299_560750809)

[4.3 Sécurité physique et environnementale 8](#__RefHeading___Toc23333_560750809)

[4.4 Sécurité des communications 8](#__RefHeading___Toc23335_560750809)

[4.5 Contrôle d’accès logiques 8](#__RefHeading___Toc23337_560750809)

[4.6 Sécurité liée à l’exploitation 9](#__RefHeading___Toc23339_560750809)

[4.7 Acquisition, développement et maintenance des systèmes 10](#__RefHeading___Toc23343_560750809)

[4.8 Relation avec les fournisseurs 10](#__RefHeading___Toc23345_560750809)

[4.9 Gestion des incidents liés à sécurité numérique 10](#__RefHeading___Toc23347_560750809)

[4.10 Gestion de la continuité d’activité 11](#__RefHeading___Toc23349_560750809)

[4.11 Conformité 11](#__RefHeading___Toc23351_560750809)

[4.12 Cryptographie 11](#__RefHeading___Toc23353_560750809)

[4.13 Indicateurs de sécurité 11](#__RefHeading___Toc23355_560750809)

[4.14 Réversibilité 11](#__RefHeading___Toc23357_560750809)

[5 Matrice de couverture des exigences de sécurité 12](#__RefHeading___Toc23359_560750809)

[6 Suivi de la documentation sécurité 12](#__RefHeading___Toc23361_560750809)

[7 Glossaire 12](#__RefHeading___Toc23688_560750809)

# Objet

## Objet du document

Ce document décrit les dispositions que <*À compléter – nom du prestataire*> s’engage à mettre en œuvre pour répondre aux exigences de sécurité d’Angers Loire Métropole, de la ville d’Angers ou de son CCAS. Il définit en particulier l’organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet d’externalisation et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre.

## Documents de référence

Ce paragraphe liste les documents de référence pour le Plan d’Assurance Sécurité.

À titre d’exemple, les documents applicables peuvent être les suivants :

* le contrat ;
* le cahier des charges, incluant les exigences de sécurité ;
* le plan d’assurance qualité ;
* etc.

*À compléter par le prestataire / documents applicables*

## Description du système

Présentation succincte du système faisant l’objet de l’opération d’externalisation, en rappelant les points qui justifient la mise en œuvre de mesures de sécurité.

*À compléter par le prestataire*

## Rappel des exigences

Rappel des exigences de sécurité d’Angers Loire Métropole, de la ville d’Angers ou de son CCAS.

*À compléter par le prestataire*

# Organisation de la sécurité

## Organisation générale de la sécurité

Organisation proposée pour gérer la sécurité dans le projet.

Maître d’ouvrage, prestataire, co-traitants, sous-traitants, fournisseurs.

Comité de suivi de la sécurité

Diffusion du PAS et des documents de suivi

Audits, contrôles réalisés par la maîtrise d’ouvrage

…

*À compléter par le prestataire*

## Chaîne de sécurité du candidat

Groupes : rôles et fonctions

Contacts et alertes

Objectif : information de qualité, non ambiguë, avec des termes précis et exacts. Afin d’éviter les interprétations, incompréhensions, ou informations partielles.

*À compléter par le prestataire*

## Relation avec des groupes de travail spécialisés

Veille juridique et réglementaire, revue de presse, suivi des bulletins ou des alertes…

*À compléter par le prestataire*

# Présentation du PAS

La rédaction du PAS s’appuie sur :

* Les normes et standards reconnus (ISO 27001, ISO 27002) ;
* Les recommandations de l’ANSSI ;
* Les recommandations de l’OWASP ;
* Les bonnes pratiques en matière de sécurité SI.

Le titulaire, au travers de son responsable de la sécurité désigné, est responsable de la rédaction, de l’évolution et de l’application du Plan d’Assurance Sécurité.

## Responsabilités liées au PAS

Responsabilités pour la rédaction, l’évolution et l’application du PAS

*À compléter par le prestataire*

## Procédure d’évolution du PAS

Situations susceptibles d’entraîner une modification du PAS. Par ex :

* évolution du SI
* évolution de l’environnement du SI (locaux, personnels, procédures)
* évolution du périmètre
* évolution au-delà d’une certaine durée

Vérification du besoin de modification, rédaction, validation

*À compléter par le prestataire*

## Applicabilité du PAS

Applicable à l’ensemble des acteurs du projet.

*À compléter par le prestataire*

### Surveillance et suivi

Vérifications et contrôles

Suivi à l’aide d’indicateurs

Bilans, état d’avancement de mise en œuvre

*À compléter par le prestataire*

### Procédure à suivre en cas de non-application du PAS

Information, rapport, correction, pénalité

*À compléter par le prestataire*

### Dérogation à l’application du PAS

En cas d’impossibilité à appliquer l’ensemble des clauses par un acteur du projet

Modèle de demande de dérogation

Traitement de la demande de dérogation

*À compléter par le prestataire*

# Mesures de sécurité

Description des mesures destinées à assurer la sécurité du système cible de l’opération d’externalisation pendant les différentes phases contractuelles : phase de transfert, phase d’exploitation, phase de réversibilité ou fin de contrat.

## Sécurité et ressources humaines

### Avant l’embauche

Recrutement, formation

Personnel permanent et non permanent

*À compléter par le prestataire*

### Pendant la durée du contrat

Chartes

Sensibilisation

*À compléter par le prestataire*

### Rupture, terme ou modification du contrat

Mise à jour des droits d’accès

Gestion des départs

*À compléter par le prestataire*

## Gestion des actifs

### Inventaire des actifs

Ressources informatiques : inventaire, propriété, utilisation correcte, restitution

Cartographie physique, logique, de l’administration, applicative (incluant les flux associés).

(listes des cartographies, outils, périodicité des mises à jour…)

*À compléter par le prestataire*

### Classification de l’information

Classification, marquage, manipulation

*À compléter par le prestataire*

### Manipulation des supports

Supports amovibles, mise au rebut, transfert physique

Sécurité des documents papier

*À compléter par le prestataire*

## Sécurité physique et environnementale

### Zones sécurisés

Cartographie : zones sécurisées et sensibles, zones internes, zone d’accueil…

Hébergement des équipements

Contrôle d’accès physiques aux salles serveurs

Sécurité environnementale des salles serveurs

Protection d’accès aux locaux techniques

*À compléter par le prestataire*

### Matériels

Maintenance du matériel

Sécurité du câblage

Mise au rebut des supports de données

*À compléter par le prestataire*

## Sécurité des communications

### Gestion de la sécurité des réseaux informatiques

Sécurité des réseaux, architecture des SI et cloisonnement réseau, sécurité périmétrique

Réseaux sans fil

Sécurité des accès Internet

Réexamen des règles de filtrage

*À compléter par le prestataire*

### Transfert d’information

politique, chiffrement, échange automatisés

*À compléter par le prestataire*

### Appareils mobiles

Attribution, configuration sécurisé, chiffrement, utilisation professionnelle / personnelle, surveillance, matériels personnels, sauvegarde

*À compléter par le prestataire*

## Contrôle d’accès logiques

### Exigences métier en matière de contrôle d’accès

Politique d’habilitation

*À compléter par le prestataire*

### Gestion de l’accès utilisateur

gestion des comptes, politique de mots de passe, réexamen des droits d’accès

*À compléter par le prestataire*

### Responsabilité des utilisateurs

Protection des codes d’accès, et de la session de travail

*À compléter par le prestataire*

### Contrôle de l’accès aux systèmes et aux applications

Authentification

Accès distants

Protections

Comptes à privilèges

*À compléter par le prestataire*

## Sécurité liée à l’exploitation

### Procédure et responsabilités liées à l’exploitation

Documentation, procédure, gestion des changements

*À compléter par le prestataire*

### Protection contre les codes malveillants

### Sauvegarde

politiques, tests, supports de sauvegarde

*À compléter par le prestataire*

### Journalisation et surveillance

### Maîtrise des logiciels en exploitation

(Accès aux) outils d’administration, contrôle de la configuration

*À compléter par le prestataire*

### Gestion des vulnérabilités

Installations, maîtrise des vulnérabilités techniques, gestion de l’obsolescence

*À compléter par le prestataire*

## Acquisition, développement et maintenance des systèmes

### Exigences de sécurité applicables aux systèmes d’information

Expression des besoins de sécurité

Sécurisation des services d’application sur les réseaux publics

Protection des transactions

*À compléter par le prestataire*

### Sécurité des processus de développement et d’assistance technique

Sécurité des développements, bonnes pratiques, respect de règles, contrôles, audit du code, recette, gestion des versions

Environnement de développement

Gestion des développements externalisés ou des acquisitions

*À compléter par le prestataire*

### Données de test

Gestion des données et environnements de test, qualification, recette.

Anonymisation

*À compléter par le prestataire*

## Relation avec les fournisseurs

### Sécurité de l’information dans les relations avec les fournisseurs

Sécurité dans les contrats

Envoi de données (sensibles ou à caractère personnel)

*À compléter par le prestataire*

### Gestion de la prestation du service

Engagements de services, suivi

Gestion des changements,

Accès des fournisseurs aux SI

*À compléter par le prestataire*

## Gestion des incidents liés à sécurité numérique

Gestion des incidents

Dispositif d’alerte

Gestion de crise

*À compléter par le prestataire*

## Gestion de la continuité d’activité

### Continuité de la sécurité de l’information

Procédures dégradées

Continuité des opérations et organisation des compétences SI

Reprise d’activité

Exercices de test des plans de continuité, et des plans de reprise.

*À compléter par le prestataire*

### Redondances

Redondance des composants SI

Test des redondances

*À compléter par le prestataire*

## Conformité

### Conformité aux obligations légales et réglementaires

Identification et respect des exigences légales, réglementaires…

*À compléter par le prestataire*

### Revue de la sécurité de l’information

Revue de la sécurité, contrôles, audits.

*À compléter par le prestataire*

## Cryptographie

Politique et mécanismes cryptographiques, gestion des clés

*À compléter par le prestataire*

## Indicateurs de sécurité

Surveillance et mesure de l’efficacité

ex : taux de formation, ratio de systèmes obsolètes, incidents de sécurité importants ou graves…

*À compléter par le prestataire*

## Réversibilité

Assistance durant le période de migration : transfert des moyens de sécurité matériels et logiciels

Maintien du niveau de sécurité durant la phase de transfert

Conservation des journaux après la fin du contrat

*À compléter par le prestataire*

# Matrice de couverture des exigences de sécurité

Cf tableur joint.

# Suivi de la documentation sécurité

Recensement de l’ensemble de la documentation concernant la sécurité fournie au titre du projet.

PAS, dossier de sécurité, plan de secours, plan de gestion des incidents, comptes-rendu…

# Glossaire

|  |  |
| --- | --- |
| Terme | Définition |
| ALM | Angers Loire Métropole |
| SSI | Sécurité des systèmes d’information |
| PAS | Plan d’assurance sécurité |
| *À compléter* |  |
|  |  |