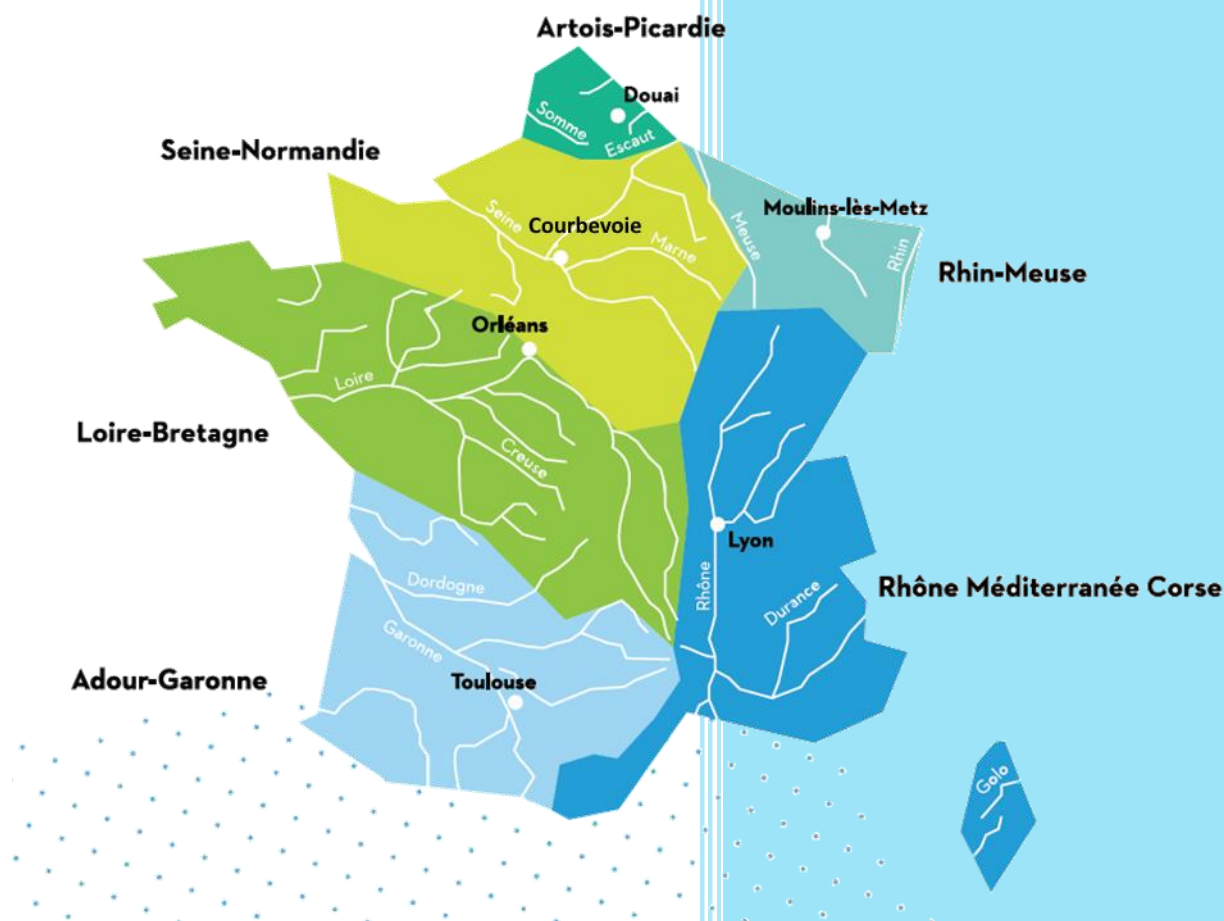


PLAN D'ASSURANCE SECURITE DES AGENCES DE L'EAU



Le présent Plan d'Assurance Sécurité (PAS) spécifie les exigences de sécurité applicable dans le cadre du contrat établie entre les agences de l'eau et le ou les prestataires intervenant dans le projet

Projet : XXXXXXXXXXXX

Les agences de l'eau
Prestataire(s)

Date : XX/XX/XXXX

Version : XX.XX



1 SUIVI DES REVISIONS

1.1 REVISIONS

Version	Date	Acteur	Description de la révision
1.0	10/04/2025	P. Veinante	Création du modèle

1.2 VALIDATIONS

Version	Etape	Date	Acteurs	Visa
1.0	Rédaction			
	Vérification LADE			
	Approbation prestataires			
	Rédaction			
	Vérification LADE			
	Approbation prestataires			

1.3 DIFFUSION

Entreprise	Destinataires	Pour action	Pour Information

1	Suivi des révisions	2
1.1	Révisions	2
1.2	Validations	2
1.3	Diffusion	2
2	Définitions	7
3	INTRODUCTION	9
3.1	Objectif du document	9
3.2	Applicabilité du présent Plan d'Assurance Sécurité	9
3.3	Documents Applicables	9
3.4	Cycle de vie du PAS	10
3.4.1	Rédaction du PAS	10
3.4.2	Dérogation à l'application du PAS	10
3.4.3	Procédure en cas de non-application du PAS	10
3.5	Description du contexte du projet	11
3.5.1	Rappel du cadre du projet	11
3.5.2	Les risques identifiés sur le projet	11
4	Gouvernance de la sécurité	12
4.1	Politiques de sécurité de l'information	12
4.2	Rôles et responsabilités en matière de sécurité des SI	13
4.2.1	Rôle et responsabilité dans les agences de l'eau	13
4.2.2	Rôle et responsabilité chez le prestataire	13
4.3	Séparation des tâches	14
4.4	Relation avec les autorités	14
4.5	Contacts avec des groupes d'intérêt spécifiques	14
4.6	Sécurité de l'information dans la gestion de projet	15
4.7	Les indicateurs (KPI) Sécurité	15
5	Gestion des actifs	16
5.1	Inventaire des informations et autres actifs associés	16
5.2	Restitution des actifs	16
5.3	Emplacement et protection du matériel	16
5.4	Sécurité des actifs hors des locaux	16
5.5	Supports de stockage	16
5.6	Maintenance du matériel	16
5.7	Elimination ou recyclage sécurisé du matériel	16
6	Gestion et protection de l'information	17
6.1	Classification des informations	17

6.2	Marquage des informations	17
6.3	Transfert des informations	17
6.4	Utilisation correcte des informations et autres actifs associés	17
6.5	Suppression d'information	17
6.6	Masquage des données	17
6.7	Prévention de la fuite de données	17
6.8	Informations de test	17
6.9	Protection des systèmes d'information pendant les tests d'audit	17
6.10	Protection des enregistrements	17
6.11	Protection de la vie privée et des données à caractère personnel (DCP)	17
7	<i>Gestion des ressources humaines</i>	18
7.1	Sélection des candidats	18
7.2	Termes et conditions du contrat de travail	18
7.3	Sensibilisation, enseignement et formation en sécurité de l'information	18
7.4	Processus disciplinaire	18
7.5	Responsabilités après la fin ou le changement d'un emploi	18
7.6	Accords de confidentialité ou de non-divulgence	18
8	<i>Gestion des comptes et des accès</i>	19
8.1	Contrôle d'accès	19
8.2	Gestion des identités	19
8.3	Informations d'authentification	19
8.4	Droits d'accès	19
8.5	Droits d'accès privilégiés	19
8.6	Restriction d'accès aux informations	19
8.7	Authentification sécurisée	19
9	<i>Protection physique</i>	20
9.1	Périmètres de sécurité physique	20
9.2	Les entrées physiques	20
9.3	Sécurisation des bureaux, des salles et des installations	20
9.4	Surveillance de la sécurité physique	20
9.5	Protection contre les menaces physiques et environnementales	20
9.6	Travail dans les zones sécurisées	20
9.7	Bureau propre et écran vide	20
9.8	Services support	20
9.9	Sécurité du câblage	20

10	Mesures technologiques	21
10.1	Terminaux utilisateurs	21
10.2	Télétravail	21
10.3	Protection contre les programmes malveillants (malware)	21
10.4	Gestion des vulnérabilités techniques	21
10.5	Renseignement sur les menaces	21
10.6	Utilisation de programmes utilitaires à privilèges	21
10.7	Sécurité des réseaux	21
10.8	Sécurité des services réseau	21
10.9	Cloisonnement des réseaux	21
10.10	Filtrage web	21
11	Sécurité des applications	22
11.1	Accès au code source	22
11.2	Cycle de développement sécurisé	22
11.3	Exigences de sécurité des applications	22
11.4	Principes d'ingénierie et d'architecture des systèmes sécurisés	22
11.5	Codage sécurisé	22
11.6	Test de sécurité dans le développement et l'acceptation	22
11.7	Développement externalisé	22
11.8	Séparation des environnements de développement, de test et opérationnels	22
11.9	Gestion des changements	22
12	Gestion des configurations	23
12.1	Gestion de la configuration	23
12.2	Installation de logiciels sur des systèmes opérationnels	23
12.3	Utilisation de la cryptographie	23
13	Continuité d'activité et maintien en condition opérationnelle	24
13.1	PRA PCA	24
13.2	Sécurité de l'information pendant une perturbation	24
13.3	Préparation des TIC pour la continuité d'activité	24
13.4	Procédures d'exploitation documentées	24
13.5	Dimensionnement	24
13.6	Sauvegarde des informations	24
13.7	Redondance des moyens de traitement de l'information	24
14	La chaîne d'approvisionnement	25
14.1	Sécurité de l'information dans les relations avec les fournisseurs	25

14.2	La sécurité de l'information dans les accords conclus avec les fournisseurs	25
14.3	Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC	25
14.4	Surveillance, révision et gestion des changements des services fournisseurs	25
14.5	Sécurité de l'information dans l'utilisation de services en nuage	25
15	Conformités et exigences légales	26
15.1	Exigences légales, statutaires, réglementaires et contractuelles	26
15.2	Droits de propriété intellectuelle	26
15.3	Revue indépendante de la sécurité de l'information	26
15.4	Conformité aux politiques, règles et normes de sécurité de l'information	26
16	Gestion des événements et des incidents	27
16.1	Planification et préparation de la gestion des incidents liés à la sécurité de l'information	27
16.2	Evaluation des événements liés à la sécurité de l'information et prise de décision	27
16.3	Réponse aux incidents liés à la sécurité de l'information	27
16.4	Enseignements des incidents liés à la sécurité de l'information	27
16.5	Collecte de preuves	27
16.6	Déclaration des événements liés à la sécurité de l'information	27
16.7	Journalisation	27
16.8	Activités de surveillance	27
16.9	Synchronisation des horloges	27

2 DEFINITIONS

Afin de limiter les interprétations de certains termes clés, une définition applicable au présent document est donnée ci- après pour certains mots, sigles ou abréviations.

Accès privilégiés : Un compte utilisateur ayant des accès privilégiés dispose de droits d'accès supérieur à ceux attribués à un compte ordinaire. Ces accès privilégiés permettent de réaliser certaines opérations considérées comme sensibles ou exceptionnelles sur les systèmes d'information (ex : Installation de briques logicielles, un Système d'exploitation...).

Actif :

Administrateur : Toute personne habilitée par la Direction des Systèmes d'Information et des Usages Numériques (DSIUN) à assurer le fonctionnement et la sécurité des moyens informatiques. Il dispose à ce titre de droits d'accès privilégiés. L'administrateur est soumis aux chartes utilisateurs et administrateur des agences de l'eau.

Agence : Terme qui désigne dans le présent document, les différents entités juridiques et sites (sièges et délégations territoriales) des agences de l'eau.

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information - <https://cyber.gouv.fr/>

CNIL : Commission Nationale de l'Informatique et des Libertés - <https://www.cnil.fr/>

DPD : Le Délégué à la Protection des Données est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'agence qui l'a désigné

DSIUN : La Direction des Systèmes d'Informations et des Usages Numériques, a été créée en septembre 2020. Ses agents sont répartis dans les 6 agences de l'eau. Ses principales missions sont de garantir le maintien en conditions opérationnelles des services numériques existants et de construire le système d'information mutualisé pour le compte des 6 agences de l'eau.

OCEAN : Application interne aux agences de l'eau. Elle permet la gestion de tickets des demandes et incidents des utilisateurs, accessible depuis l'intranet ou via l'adresse suivante : <https://ocean.lesagencesdeleau.eu/wm/>

PAS : Plan d'Assurance Sécurité

PSSI : Politique de sécurité des Système d'Information. Ce document, disponible sur Res'eau, précise le plan d'action pour maintenir un certain niveau de sécurité. Cette politique reflète la vision stratégique de la direction des agences de l'eau en matière de sécurité des systèmes d'information (SSI)

RGS : Référentiel Général de Sécurité <https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs>


RSSI : Responsable de la Sécurité des Systèmes d'information des agences de l'eau

S.I. : Un Système d'Information est constitué d'informations (données, documents, vidéo...) et de systèmes informatiques (ordinateur, serveur, réseaux...)

SSI : Sécurité des Systèmes d'Information

RGPD : Le Règlement Général sur la Protection des Données n° R (UE) 2016/679 établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données :

[Règlement - 2016/679 - FR - rgdp - EUR-Lex](#)

TLP GREEN :  Diffusion libre au sein des agences de l'eau et de ces prestataires

TLP AMBER :  Diffusion limitée à quelques entités identifiées, liées par un engagement

✓ **TLP :** Marquage indiquant le degré de partage autorisé du contenu dans un document

✓ Pour plus d'information, consulter le site de l'ANSSI :

[Politique de partage et d'utilisation des informations à caractère opérationnel - CERT-FR](#)

Utilisateur : Terme générique qui désigne toute personne, autorisée par l'agence à utiliser de façon permanente ou temporaire les moyens informatiques qu'elle met à disposition. Notamment :

- L'ensemble des personnels de l'agence quel que soit leur statut (agent, membre de commission, stagiaire, apprenti, fonctionnaire, contractuel en CDD ou CDI, intérimaire...)
- Les personnels prestataires extérieurs (société de service) autorisés à travailler sur site
- Les syndicats représentants du personnel, Amicale et Association Sportive
- Et tous les personnels tiers aux agences (visiteurs occasionnels se connectant au réseau Wifi public)

VPN : Virtual Private Network ou Réseau Privé Virtuel permet de créer un lien direct sécurisé entre un ordinateur distant et le réseau de l'agence.

3 INTRODUCTION

3.1 OBJECTIF DU DOCUMENT

Les agences de l'eau mettent en œuvre des systèmes d'Information et de communications nécessaires à l'exercice de leurs missions. Le présent Plan d'Assurance Sécurité a pour objet de définir les exigences de sécurité de l'information dans le cadre du contrat **XXXXXXXX**. Ce document répond aux exigences de sécurité de l'information des agences de l'eau.

Il définit en particulier l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre.

Il vient en complément des clauses contractuelles, en particulier le chapitre sécurité du CCTP, qui ne seront pas reprises ici dans leur contenu.

Chaque nouvelle version du plan d'assurance sécurité est soumise au circuit d'approbation décrit infra.

Le PAS et ses éventuelles annexes, sert de référence en cas d'audit demandé par les Agences de l'eau, l'un des prestataires intervenant sur le contrat ou par une tierce partie.

Ces documents servent aussi de référence aux mesures de sécurité mises en œuvre dans le cadre de la protection des données à caractère personnel.

3.2 APPLICABILITE DU PRESENT PLAN D'ASSURANCE SECURITE

Le présent PAS, une fois validé, est applicable à l'ensemble des agents des agences de l'eau ainsi qu'à l'ensemble des personnels des prestataires intervenant dans le cadre du contrat mentionné supra.

3.3 DOCUMENTS APPLICABLES

Sont listés dans le tableau ci-dessous les documents de référence applicables dans le cadre du contrat.

Référence du document	Description du document
DCE *	Dossier de consultation des entreprises
PAQ *	Plan d'Assurance Qualité
PAS	Plan d'Assurance Sécurité
DAT *	Dossier d'architecture technique
DEX	Dossier d'Exploitation
PCA*	Plan de Continuité d'Activité

* si prévu au contrat

3.4 CYCLE DE VIE DU PAS

3.4.1 Rédaction du PAS

Le PAS est mis à jour par le prestataire à partir du modèle fourni par le RSSI des agences de l'eau.

Le directeur de projet du titulaire est responsable de la rédaction, de l'évolution et de l'application du Plan d'Assurance Sécurité par l'ensemble de ses équipes (sous-traitants éventuels inclus).

Le directeur de projet des agences de l'eau est responsable de la rédaction, de l'évolution et de l'application du Plan d'Assurance Sécurité par l'ensemble des équipes internes (sous-traitants éventuels inclus).

Le Pas doit être approuvé par le RSSI des agences de l'eau.

La cohérence de l'ensemble des mesures pourra être analysée et réévaluée lors des comités de pilotage ou en cas d'incident ou dysfonctionnement

Il est à noter que la version du PAS fourni dans les dossiers de consultation des entreprises (marché public) peut différer de la version fournie en début du projet par le RSSI des agences de l'eau, afin de prendre en compte notamment les évolutions réglementaires et les besoins opérationnels afin de prendre en compte les nouvelles menaces.

3.4.2 Dérogation à l'application du PAS

En cas de non-application des dispositions du PAS, une demande de dérogation justifiée doit être faite par le prestataire auprès du représentant des agences de l'eau sur le projet (en règle générale le directeur ou chef de projet).

Si la dérogation est justifiée et approuvée par le comité de pilotage, elle est soumise pour approbation au RSSI des agences de l'eau.

Toute dérogation est tracée et suivie en comité de pilotage ou en comité de sécurité s'il existe.

3.4.3 Procédure en cas de non-application du PAS

Toute non-application du PAS par un des membres des équipes des agences et du prestataire doit immédiatement être signalée auprès des membres du comité de pilotage et du RSSI des agences de l'eau. Ce signalement devra être tracé et suivi tout comme les actions correctives qui seront mises en place.

3.5 DESCRIPTION DU CONTEXTE DU PROJET

3.5.1 *Rappel du cadre du projet*

Rappeler ici le cadre du projet (Objectifs, Périmètre, limite, parties prenantes...)

3.5.2 *Les risques identifiés sur le projet*

Rappeler ici les risques identifiés ainsi que les moyens de maitrises s'il sont définis

4 GOUVERNANCE DE LA SECURITE

4.1 POLITIQUES DE SECURITE DE L'INFORMATION

Placées sous la tutelle du Ministère de la Transition écologique, les agences de l'eau perçoivent des redevances en provenance de tous les usagers de l'eau selon le principe du « pollueur-payeur » et « préleveur-payeur ». Chaque euro prélevé est réinvesti sous forme d'aides aux collectivités, acteurs économiques et agricoles pour financer des actions favorisant la reconquête du bon état de l'eau.

Nos missions : aider les collectivités, les industriels, les agriculteurs, les associations de pêche et de protection de la nature dans le financement, l'accompagnement et la valorisation de tous projets et initiatives visant à préserver la ressource en eau et la biodiversité dans chaque bassin hydrographique sous climat changeant.

Chaque agence a mis en place un système d'information autonome qui prend une place de plus en plus prépondérante en fournissant aux agents les outils et services essentiels à la réalisation de leurs missions. Dans un contexte de mutualisation, ces Systèmes d'Information (SI) sont amenés à être gérés de manière commune par la Direction des systèmes d'information et des usages numériques (DSIUN) tout en conservant l'autonomie de chacune des six agences de l'eau.

Conscient des risques pesant sur les SI, un responsable de la sécurité des systèmes d'information (RSSI) unique a été nommé afin d'uniformiser, coordonner et renforcer les mesures de sécurité au sein des six agences.

La sécurité de l'information est un enjeu stratégique pour les agences ainsi qu'une source de confiance dans leurs relations avec les usagers, avec les agents et entre les Agences. La DSIUN met en œuvre une démarche de sécurisation des SI défini dans sa PSSI qui identifie les enjeux et les contraintes de sécurité des SI (SSI) et définit les principales orientations de sécurité. Elle précise également l'organisation, les rôles et les responsabilités de l'ensemble des acteurs en matière de sécurité de l'information.

Les directions des agences de l'eau soutiennent à différents niveaux la définition et l'application de la dite PSSI en :

- ✓ Nommant un responsable de la sécurité des systèmes d'information (RSSI) garant du respect des règles édictées dans ce document.
- ✓ Assurant un suivi régulier des plans d'actions engagées et de la maîtrise des risques
- ✓ Allouant des budgets de mise en œuvre et de maintien de la politique de sécurité

La PSSI est révisée régulièrement par le responsable de la sécurité des systèmes d'information (RSSI) afin de prendre en compte les éventuels changements intervenant dans l'organisation, les systèmes d'information ou la législation en vigueur.

4.2 ROLES ET RESPONSABILITES EN MATIERE DE SECURITE DES SI

4.2.1 Rôle et responsabilité dans les agences de l'eau

Les agences de l'eau ont mis en place une organisation de la gestion de la sécurité conformément aux dispositions de la PSSI. Le tableau suivant présente les différents acteurs.

Acteur	Description
RSSI	Il est le garant de la définition et de la mise en œuvre du système de management de la sécurité des agences de l'eau. Il accompagne les autres acteurs de la sécurité dans l'élaboration des PAS et dans l'application de la PSSI. En cas d'incident Cyber, il assure la coordination de la cellule de crise et les réalisations avec l'ANSSI et le CSIRT du ministère
DPD	Il est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'agence. Il est le garant de l'application de la loi « informatique et libertés » et du « RGPD ». Il enregistre toutes les déclarations de traitements internes et externes, dans son registre et assure les échanges avec la CNIL
Directeur de projet	Il est responsable des projets qu'il pilote. Sur ces projets, il est le garant du respect des mesures de sécurité par les équipes internes aux agences de l'eau.
Chef de projet	Il travaille sous l'autorité fonctionnelle du DP et peut piloter un ou plusieurs sous projets. Sur ces sous-projets, il est le garant du respect des mesures de sécurité par les équipes internes aux agences de l'eau.
Responsable de site	Il coordonne la sécurité physique des actifs et des personnes du site dont il est responsable.

4.2.2 Rôle et responsabilité chez le prestataire

A préciser par le prestataire

Acteur	Description

4.3 SEPARATION DES TACHES

Les rôles et responsabilités doivent être définis afin qu'une séparation des tâches soit effective visant à limiter les possibilités de modification, d'usage non autorisé ou involontaire des ressources des SI.

Les intervenants des agences de l'eau et du prestataire interviennent dans le respect des prérogatives de leurs rôles dans le projet.

Un RACI peut être défini si besoin.

A préciser si un RACI est nécessaire. Si c'est le cas, il faut l'ajouter au paragraphe.

4.4 RELATION AVEC LES AUTORITES

Le RSSI des agences de l'eau est en relation avec l'Agence Nationale de Sécurité des Systèmes d'Information (l'ANSSI) ainsi qu'avec le CSIRT du ministère de l'Environnement.

Il se charge de signaler les incidents de sécurité, partager des informations sur les menaces et répondre aux demandes d'informations.

Le DPD des agences de l'eau est en relation avec la Commission National de l'Informatique et des Libertés (CNIL). Il se charge de déclarer les traitements opérés sur les données ainsi que les incidents de sécurité en lien avec le RGPD. Il répond également aux demandes d'informations de cette entité.

Le prestataire s'engage à informer sans délai le RSSI et le DPD des agences de l'eau sur tout incident de sécurité constaté sur le périmètre de projet sur lequel il intervient, mais également sur les incidents intervenus dans ses propres SI qui pourraient avoir un impact direct ou indirect sur les données ou les SI des agences de l'eau.

Le prestataire précisera son organisation

4.5 CONTACTS AVEC DES GROUPES D'INTERET SPECIFIQUES

Afin de faire face aux cybermenaces, les agences de l'eau peuvent recourir à des prestations d'expertise et s'abonner à des services comme le CERT.

Le RSSI des agences de l'eau est enregistré comme interlocuteur principal auprès du CSIRT du ministère de l'Environnement qui assure une veille sur les menaces cyber.

Les experts de la DSIUN sont également affiliés à des groupes d'expertise et assurent entre eux une veille technique.

Le prestataire précisera son organisation

4.6 SECURITE DE L'INFORMATION DANS LA GESTION DE PROJET

La direction de projet (Agence de l'eau et prestataire) s'assure de la prise en compte et de l'application de la politique de sécurité des Agences de l'eau tout au long du projet pour les parties qui les concerne.

Pour se faire, il maintienne à jour et réalise un suivi régulier de l'analyse des risques et des exigences du projet.

Aussi, des échanges réguliers doivent être établis entre les agences de l'eau et le prestataire au sein d'instance comme les comités de pilotage ou les Comité de Sécurité. Durant ces échanges, un suivi à minima des points suivants doit être réalisé :

- ✓ Gestion des actifs
- ✓ Les menaces et vulnérabilités identifiées (moyens de maitrise)
- ✓ Suivi de la maitrise des risques
- ✓ KPI relatifs à la sécurité
- ✓ Evènements et incidents de sécurité rencontrés ou évités
- ✓ Respect du PAS

Préciser ce qui est retenu dans le cadre du projet (point en comité de pilotage ou comité de sécurité) ainsi que la fréquence, l'ordre du jour et les participants.

4.7 LES INDICATEURS (KPI) SECURITE

L'élaboration d'indicateurs de sécurité puis leurs communications sous la forme de tableaux de bord permet aux agences de l'eau d'évaluer le niveau de sécurité respecté sur le projet.

Préciser les indicateurs de sécurité retenu sur le projet.

5 GESTION DES ACTIFS

De manière générale, les agences de l'eau assurent la gestion de leurs propres actifs. Il en est de même pour le prestataire.

5.1 INVENTAIRE DES INFORMATIONS ET AUTRES ACTIFS ASSOCIES

5.2 RESTITUTION DES ACTIFS

5.3 EMBLACEMENT ET PROTECTION DU MATERIEL

5.4 SECURITE DES ACTIFS HORS DES LOCAUX

5.5 SUPPORTS DE STOCKAGE

5.6 MAINTENANCE DU MATERIEL

5.7 ELIMINATION OU RECYCLAGE SECURISE DU MATERIEL

6 GESTION ET PROTECTION DE L'INFORMATION

6.1 CLASSIFICATION DES INFORMATIONS

6.2 MARQUAGE DES INFORMATIONS

6.3 TRANSFERT DES INFORMATIONS

6.4 UTILISATION CORRECTE DES INFORMATIONS ET AUTRES ACTIFS ASSOCIES

6.5 SUPPRESSION D'INFORMATION

6.6 MASQUAGE DES DONNEES

6.7 PREVENTION DE LA FUITE DE DONNEES

6.8 INFORMATIONS DE TEST

6.9 PROTECTION DES SYSTEMES D'INFORMATION PENDANT LES TESTS D'AUDIT

6.10 PROTECTION DES ENREGISTREMENTS

6.11 PROTECTION DE LA VIE PRIVEE ET DES DONNEES A CARACTERE PERSONNEL (DCP)

7 GESTION DES RESSOURCES HUMAINES

7.1 SELECTION DES CANDIDATS

7.2 TERMES ET CONDITIONS DU CONTRAT DE TRAVAIL

7.3 SENSIBILISATION, ENSEIGNEMENT ET FORMATION EN SECURITE DE L'INFORMATION

7.4 PROCESSUS DISCIPLINAIRE

7.5 RESPONSABILITES APRES LA FIN OU LE CHANGEMENT D'UN EMPLOI

7.6 ACCORDS DE CONFIDENTIALITE OU DE NON-DIVULGATION

8 GESTION DES COMPTES ET DES ACCES

8.1 CONTROLE D'ACCES

8.2 GESTION DES IDENTITES

8.3 INFORMATIONS D'AUTHENTIFICATION

8.4 DROITS D'ACCES

8.5 DROITS D'ACCES PRIVILEGIES

8.6 RESTRICTION D'ACCES AUX INFORMATIONS

8.7 AUTHENTIFICATION SECURISEE

9 PROTECTION PHYSIQUE

9.1 PERIMETRES DE SECURITE PHYSIQUE

9.2 LES ENTREES PHYSIQUES

9.3 SECURISATION DES BUREAUX, DES SALLES ET DES INSTALLATIONS

9.4 SURVEILLANCE DE LA SECURITE PHYSIQUE

9.5 PROTECTION CONTRE LES MENACES PHYSIQUES ET ENVIRONNEMENTALES

9.6 TRAVAIL DANS LES ZONES SECURISEES

9.7 BUREAU PROPRE ET ECRAN VIDE

9.8 SERVICES SUPPORT

9.9 SECURITE DU CABLAGE

10 MESURES TECHNOLOGIQUES

10.1 TERMINAUX UTILISATEURS

10.2 TELETRAVAIL

10.3 PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS (MALWARE)

10.4 GESTION DES VULNERABILITES TECHNIQUES

10.5 RENSEIGNEMENT SUR LES MENACES

10.6 UTILISATION DE PROGRAMMES UTILITAIRES A PRIVILEGES

10.7 SECURITE DES RESEAUX

10.8 SECURITE DES SERVICES RESEAU

10.9 CLOISONNEMENT DES RESEAUX

10.10 FILTRAGE WEB

11 SECURITE DES APPLICATIONS

11.1 ACCES AU CODE SOURCE

11.2 CYCLE DE DEVELOPPEMENT SECURISE

11.3 EXIGENCES DE SECURITE DES APPLICATIONS

11.4 PRINCIPES D'INGENIERIE ET D'ARCHITECTURE DES SYSTEMES SECURISES

11.5 CODAGE SECURISE

11.6 TEST DE SECURITE DANS LE DEVELOPPEMENT ET L'ACCEPTATION

11.7 DEVELOPPEMENT EXTERNALISE

11.8 SEPARATION DES ENVIRONNEMENTS DE DEVELOPPEMENT, DE TEST ET OPERATIONNELS

11.9 GESTION DES CHANGEMENTS

12 GESTION DES CONFIGURATIONS

12.1 GESTION DE LA CONFIGURATION

12.2 INSTALLATION DE LOGICIELS SUR DES SYSTEMES OPERATIONNELS

12.3 UTILISATION DE LA CRYPTOGRAPHIE

13 CONTINUITE D'ACTIVITE ET MAINTIEN EN CONDITION OPERATIONNELLE

13.1 PRA PCA

13.2 SECURITE DE L'INFORMATION PENDANT UNE PERTURBATION

13.3 PREPARATION DES TIC POUR LA CONTINUITE D'ACTIVITE

13.4 PROCEDURES D'EXPLOITATION DOCUMENTEES

13.5 DIMENSIONNEMENT

13.6 SAUVEGARDE DES INFORMATIONS

13.7 REDONDANCE DES MOYENS DE TRAITEMENT DE L'INFORMATION

14 LA CHAÎNE D'APPROVISIONNEMENT

14.1 SECURITE DE L'INFORMATION DANS LES RELATIONS AVEC LES FOURNISSEURS

14.2 LA SECURITE DE L'INFORMATION DANS LES ACCORDS CONCLUS AVEC LES FOURNISSEURS

14.3 GESTION DE LA SECURITE DE L'INFORMATION DANS LA CHAÎNE D'APPROVISIONNEMENT TIC

14.4 SURVEILLANCE, REVISION ET GESTION DES CHANGEMENTS DES SERVICES FOURNISSEURS

14.5 SECURITE DE L'INFORMATION DANS L'UTILISATION DE SERVICES EN NUAGE

15 CONFORMITES ET EXIGENCES LEGALES

15.1 EXIGENCES LEGALES, STATUTAIRES, REGLEMENTAIRES ET CONTRACTUELLES

Les agences de l'eau et le prestataire s'engage à respecter à minima les obligations légales et réglementaires suivantes :

- ✓ Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (dite « loi informatique et libertés »), telle que modifiée par la loi n° 2018-493 du 20 juin 2018, ses ordonnances et décrets
- ✓ Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique (dites loi Godfrain)
- ✓ Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (dites loi LCEN),
- ✓ L'ordonnance no 2005-1516 dite « ordonnance RGS », vise à instaurer la confiance numérique dans les échanges électroniques.
- ✓ La jurisprudence de la CNIL et des cours et tribunaux français
- ✓ Le Règlement Général de Protection des Données (RGPD), 2016/679
- ✓ Instructions et recommandations interministérielles provenant de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)
- ✓ European Cyber Resilience Act (CRA) (20 novembre 2024)
- ✓ La directive Network and Information Security (NIS) 2
- ✓ Dispositions relevant du code de la propriété intellectuelle

15.2 DROITS DE PROPRIETE INTELLECTUELLE

15.3 REVUE INDEPENDANTE DE LA SECURITE DE L'INFORMATION

15.4 CONFORMITE AUX POLITIQUES, REGLES ET NORMES DE SECURITE DE L'INFORMATION

16 GESTION DES EVENEMENTS ET DES INCIDENTS

16.1 PLANIFICATION ET PREPARATION DE LA GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

16.2 EVALUATION DES EVENEMENTS LIES A LA SECURITE DE L'INFORMATION ET PRISE DE DECISION

16.3 REPONSE AUX INCIDENTS LIES A LA SECURITE DE L'INFORMATION

16.4 ENSEIGNEMENTS DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

16.5 COLLECTE DE PREUVES

16.6 DECLARATION DES EVENEMENTS LIES A LA SECURITE DE L'INFORMATION

16.7 JOURNALISATION

16.8 ACTIVITES DE SURVEILLANCE

16.9 SYNCHRONISATION DES HORLOGES
