



SOLUTIONS NUMÉRIQUES TERRITORIALES  
INNOVANTES

**POLITIQUE DE SECURITE DU  
SYSTEME D'INFORMATION  
ET DE COMMUNICATION**

17/12/2020



SOLUTIONS NUMÉRIQUES TERRITORIALES  
INNOVANTES



## HISTORIQUE DES MISES A JOUR DU DOCUMENT

Ce document a été créé puis mis à jour par les personnes suivantes :

Version	Date	Motif	Rédacteur	Validateur
2.0	15/11/2017	Rédaction initiale	Damien ALEXANDRE	Benoît LIENARD
3.0	10/11/2020	Révision avec Diane GERMAIN et Casimir DECAS	Damien ALEXANDRE	Benoît LIENARD
3.1	09/12/2020	Remarques de Benoît LIÉNARD	Damien ALEXANDRE	Benoît LIENARD

## LISTE DE DIFFUSION

Ce document est diffusable aux personnes suivantes :

Destinataire	Responsabilité	Date de diffusion
Autorité d'homologation	Décision d'homologation	
Commission d'homologation	Avis sur l'homologation	
Groupe de travail sécurité	Réflexion sur les usages	
Agents de SOLURIS	Mise en application	
Fournisseurs	Mise en application	

# TABLE DES MATIERES

<b>1. POLITIQUE DE SECURITE</b>	5
R1.1 Engagement	5
R1.2 Contenu	5
<b>2. ORGANISATION DE LA SECURITE</b>	6
R2.1 Gouvernance	6
R2.2 Responsable de la Sécurité du Système d'Information	6
<b>3. SECURITE DES RESSOURCES HUMAINES</b>	8
R3.1 Diffusion de l'information	8
R3.2 Gestion des habilitations : ouverture des droits	8
R3.2 Gestion des habilitations : fermeture des droits	8
R3.3 Sensibilisation	8
R3.4 Information sur la PSSIC	8
<b>4. GESTION DES ACTIFS</b>	10
R4.1 Gestion des actifs	10
R4.2 Cycle de vie des ordinateurs et des smartphones	10
<b>5. CONTROLE D'ACCES</b>	11
R5.1 Compte de session au domaine	11
R5.2 Politique de mot de passe du compte du domaine	11
<b>6. CRYPTOGRAPHIE</b>	12
R6.1 Inventaire des certificats	12
R6.2 Gestionnaire des certificats	12
R6.3 Conformité des certificats	12
<b>7. SECURITE PHYSIQUE</b>	13
R7.1 Local Technique Informatique (LTI)	13
R7.2 Suivi des accès	13
R7.3 Coordination des interventions	13
<b>8. SECURITE LIEE A L'EXPLOITATION</b>	15
R8.1 Documentation	15
R8.2 Usages	15
R8.3 Conformité	15
R8.4 Gestion des vulnérabilités	15
<b>9. SECURITE DES COMMUNICATIONS</b>	16
R9.1 Filtrage et prévention des intrusions	16
R9.2 Cloisonnement	16

<b>10. ACQUISITION, DEVELOPPEMENT, ET MAINTENANCE DES SYSTEMES D'INFORMATION.....</b>	<b>17</b>
R10.1 Gestion des projets.....	17
R10.3 Gestion des contrats.....	17
<b>11. RELATION AVEC LES FOURNISSEURS.....</b>	<b>18</b>
R11.1 Plan d'Assurance Sécurité (PAS).....	18
R11.2 Gestion des fournisseurs .....	18
<b>12. GESTIONS DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION .....</b>	<b>19</b>
R12.1 Gestion des incidents de sécurité.....	19
<b>13. CONTINUITE D'ACTIVITE .....</b>	<b>20</b>
R13.1 Externalisation des sauvegardes .....	20
R13.2 Modes dégradés .....	20
<b>14. CONFORMITE .....</b>	<b>21</b>
R14.1 RGS.....	21
R14.2 RGPD.....	21

Ce document contient **22** pages.

## PREAMBULE

La Politique de Sécurité du Système d'Information et de communication (PSSIC) est rédigée sur la base des 14 chapitres de la norme ISO27002-2014.

Elle a pour objectif de préciser les attentes du Directeur de SOLURIS en matière de sécurité.

Le Plan d'Assurance Sécurité reprend certains éléments de la PSSIC afin d'informer les tiers des règles à respecter à minima dans le cadre de leurs interventions chez SOLURIS.

# 1. POLITIQUE DE SECURITE

**Objectif**

Disposer d'un référentiel de mesures de sécurité, aligné sur les activités de l'entreprise, conforme aux lois et règlements en vigueur et soutenu par la direction.

## R1.1 Engagement

Le Directeur de SOLURIS en tant que propriétaire du processus « sécurité globale du système d'information » définit ses attentes en matière de respect des pratiques de sécurité dans le présent document.

Ce document n'est pas exhaustif de l'ensemble des bonnes pratiques de sécurité mais constitue le socle minimal commun à respecter.

**Statut** : Opérationnelle

## R1.2 Contenu

Le présent document contient les mesures de sécurité applicables à SOLURIS. Cette politique est revue une fois par an lors de la révision de l'homologation ou lorsque cela s'avère nécessaire dans un principe d'amélioration continue.

**Statut** : Opérationnelle

## 2. ORGANISATION DE LA SECURITE

### Objectif

Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'entreprise.

Assurer la sécurité dans l'utilisation d'appareils mobiles.

### R2.1 Gouvernance

La sécurité globale de SOLURIS est pilotée par la commission d'homologation renommée « commission confiance numérique » composée des membres du Conseil de Direction et de trois membres du bureau syndical désigné par le Président de SOLURIS.

Les responsabilités de la gouvernance sont :

- Arbitrer le plan de traitement proposé et valider la PSSI ;
- Contrôler la réalisation du plan de traitement ;
- Donner un avis triennal au Président de SOLURIS pour lui permettre de définir le cadre de l'homologation formelle de SOLURIS ;
- Réviser annuellement l'homologation formelle de sécurité et donner un avis au Président de SOLURIS pour le maintien ou le retrait de cette homologation.

**Statut** : Opérationnelle

### R2.2 Responsable de la Sécurité du Système d'Information

Le RSSI est désigné par le propriétaire du processus sécurité globale, le Directeur de SOLURIS.

Les missions du RSSI sont :

1. Piloter le processus sécurité globale
2. Organiser la réunion annuelle de la commission d'homologation ;
3. Organiser l'évaluation des risques dans les projets dès la conception ;
4. Organiser le suivi des services numériques sensibles (impact fort) ;
  - a. Participer aux réunions de pilotage
  - b. Organiser un point annuel avec les gestionnaires
  - c. Définir et contrôler les préalables à la mise en production (tests, développements, accès, habilitations, politique de mot de passe)
5. Contrôler le suivi des incidents sur la base des process ITIL mis en place par SOLURIS;
6. Contrôler l'application de la PSSIC ;
7. Assurer une veille réglementaire ;

8. Proposer et animer un plan de sensibilisation des agents de SOLURIS pour la durée de l'homologation formelle ;
9. Organiser les audits internes et externes

**Statut** : Opérationnelle



### 3. SECURITE DES RESSOURCES HUMAINES

**Objectif**

Réduire les risques d'erreur, de vol, de fraude ou de mauvais usage du système d'information

#### R3.1 Diffusion de l'information

La Direction des Ressources (DR) définit et met en œuvre une procédure qui informe le service Territoires Numériques des arrivées, des changements de poste et des départs des salariés, stagiaires ou sous-traitants ;

Et ce en collaboration avec la Direction des Services Numériques (DSN).

**Statut** : En cours

#### R3.2 Gestion des habilitations : ouverture des droits

La Direction des Ressources (DR) définit et met en œuvre une procédure qui informe le service Territoires Numériques des modifications des habilitations sur les services numériques en cas de changement de poste d'un agent ;

Et ce en collaboration avec la Direction des Services Numériques (DSN).

**Statut** : En cours

#### R3.2 Gestion des habilitations : fermeture des droits

Le service Territoires Numériques définit et met en œuvre une procédure qui garantit la fermeture des comptes d'accès au domaine, à la messagerie, à l'accès distant (vpn), au contrôle d'accès et à l'alarme après le départ de l'utilisateur dans un délai maximum de 2 jours après le départ de la personne ;

**Statut** : En cours

#### R3.3 Sensibilisation

La Direction des Ressources (DR) s'assure que tout collaborateur de SOLURIS est sensibilisé aux 05 règles de bonne conduite de la charte comportementale.

**Statut** : En cours

#### R3.4 Information sur la PSSIC

La Direction des Ressources (DR) s'assure que tout collaborateur de SOLURIS reçoit dès son arrivée un exemplaire de la PSSIC.

**Statut** : En cours



## 4. GESTION DES ACTIFS

### Objectif

Bien connaître le système d'information et garantir un niveau approprié de sécurité à chaque information.

#### R4.1 Gestion des actifs

Le service Territoires Numériques définit et met en œuvre une procédure qui garantit l'établissement et la mise à jour d'un inventaire des actifs matériels et logiciels.

**Statut** : En cours

#### R4.2 Cycle de vie des ordinateurs et des smartphones.

Le service Territoires Numériques définit et met en œuvre une procédure qui garantit le remplacement au bout de 3 ans à minima et 5 ans à maxima des équipements des agents par des équipements neufs.

**Statut** : En cours

## 5. CONTROLE D'ACCES

### Objectif

Prévenir les accès logiques non autorisés au système d'information

#### R5.1 Compte de session au domaine

Tout utilisateur possède un identifiant nominatif et un mot de passe de qualité pour accéder au domaine. Les exceptions sont connues et tracées.

**Statut** : Opérationnelle

#### R5.2 Politique de mot de passe du compte du domaine

Le mot de passe pour être de qualité doit comporter 12 caractères alphanumériques et comprendre à minima 1 minuscule, 1 majuscule, 1 chiffre, 1 caractère spécial.

Le service Territoires Numériques définit et met en œuvre une procédure qui garantit la fréquence de changement du mot de passe à 1 an. Les exceptions sont connues et tracées.

**Statut** : En cours

## 6. CRYPTOGRAPHIE

### Objectif

Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

#### R6.1 Inventaire des certificats

Le service Territoires Numériques définit et met en œuvre une procédure qui garantit l'établissement et la mise à jour d'un inventaire des certificats RGS.

**Statut** : Opérationnelle

#### R6.2 Gestionnaire des certificats

Le service Territoires Numériques définit et met en œuvre une procédure, selon les process ITIL, qui garantit la continuité des services impactés par l'expiration des certificats RGS.

**Statut** : En cours

#### R6.3 Conformité des certificats

L'ensemble des certificats utilisés en production est conforme au Référentiel Général de Sécurité (RGS). Les exceptions sont connues et tracées.

**Statut** : Opérationnelle

## 7. SECURITE PHYSIQUE

### Objectif

Protéger les environnements physiques qui hébergent le système d'information et protéger les biens sensibles contre la perte de disponibilité, l'endommagement et le vol

### R7.1 Local Technique Informatique (LTI)

Le service Territoires Numériques définit l'ensemble des matériels sensibles comme les serveurs, les systèmes de stockage qui doivent être installés dans des espaces sécurisés (accès réglementé, climatisation, contrôle environnemental, protection électrique, etc.).

**Statut** : Opérationnelle

### R7.2 Suivi des accès

Le services Territoires Numérique définit et met en œuvre, selon les process ITIL, une procédure qui garantit l'établissement et la mise à jour d'un registre où les accès au LTI sont consignés et qui permet de tracer :

- Date et heure d'arrivée ;
- Date et heure de départ ;
- Nom de l'entreprise ;
- Nom de l'intervenant ;
- Objet de l'intervention ;
- Bilan de l'intervention.

La consignation fait l'objet d'une signature par les deux parties.

**Statut** : En cours

### R7.3 Coordination des interventions

Le service Territoires Numériques définit et met en œuvre une procédure, selon les process ITIL, qui garantit la coordination des interventions avec la Direction des Ressources pour les domaines pouvant avoir un impact sur la disponibilité ou l'intégrité du SIC :

- Ascenseur ;
- Climatisation ;
- Electricité
- Contrôle d'accès au bâtiment ;

- Local Technique Informatique.

**Statut** : Opérationnelle

## 8. SECURITE LIEE A L'EXPLOITATION

### Objectif

S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.

### R8.1 Documentation

Les Procédures d'Exploitation Sécurisées suivantes sont documentées :

- La gestion des sauvegardes
- La gestion des codes malveillants
- La gestion du pare-feu
- La gestion des vulnérabilités techniques publiées

**Statut** : Opérationnelle

### R8.2 Usages

L'usage de logiciels, de matériels ou d'équipements mobiles par les utilisateurs, hors parc géré par le service Territoires Numériques, est soumis à l'autorisation écrite du responsable du service Territoires Numériques.

**Statut** : Opérationnelle

### R8.3 Conformité

Tout ordinateur, tablette, ordiphone utilisant le réseau de SOLURIS doit disposer d'un antivirus déployé par le service Territoire Numérique.

Tout utilisateur utilisant les ressources du domaine doit en respecter les usages définis par le responsable du service Territoires Numériques.

**Statut** : Opérationnelle

### R8.4 Gestion des vulnérabilités

Tout ordinateur, tablette, ordiphone utilisant le réseau de SOLURIS doit faire l'objet d'un suivi des vulnérabilités et de mise à jour des ses composant en conformité avec les préconisations du RSSI.

**Statut** : En cours



## 9. SECURITE DES COMMUNICATIONS

### Objectif

Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.

### R9.1 Filtrage et prévention des intrusions

Un dispositif de filtrage légal et de prévention des intrusions contrôle la navigation Internet des utilisateurs des accès internet de SOLURIS.

**Statut** : Opérationnelle

### R9.2 Cloisonnement

Le service Territoire Numérique a identifié les zones de sécurité spécifiques et en assure l'isolation réseau :

- Salle de préparation et de tests ;
- Salle de formation ;
- Salles de réunion ;
- Local Technique Informatique.

**Statut** : Opérationnelle

## 10. ACQUISITION, DEVELOPPEMENT, ET MAINTENANCE DES SYSTEMES D'INFORMATION

### Objectif

Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut notamment des exigences spécifiques pour les systèmes d'information fournissant des services sur les réseaux publics.

### R10.1 Gestion des projets

Le RSSI pilote l'évaluation des risques en valorisant les conséquences en termes de Disponibilité, Intégrité, Confidentialité.

**Statut** : Opérationnelle

### R10.3 Gestion des contrats

L'ensemble des matériels et logiciels en production doit faire l'objet d'un contrat de maintenance avec un niveau de service adapté aux besoins métiers (sur la base de l'évaluation des conséquences).

Les exceptions sont connues et listées.

**Statut** : Opérationnelle

## 11. RELATION AVEC LES FOURNISSEURS

### Objectif

Garantir la protection des actifs de l'organisation accessibles aux fournisseurs. Maintenir un niveau convenu de sécurité de l'information et de prestations de services, conformément aux accords conclus avec les fournisseurs.

#### R11.1 Plan d'Assurance Sécurité (PAS)

Un Plan d'Assurance Sécurité doit être signé par les cotraitants, les prestataires de maintenance, et les partenaires qui interviennent sur le système d'information ou accèdent au Local Technique Informatique.

**Statut** : En cours

#### R11.2 Gestion des fournisseurs

Le contrôle des signatures du PAS est assuré par le RSSI en coordination avec les responsables des pôles gestionnaires.

**Statut** : En cours

## 12. GESTIONS DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

**Objectif**

Garantir un traitement rapide et efficient des incidents de sécurité du SI

### R12.1 Gestion des incidents de sécurité

Le service Territoires Numériques définit et met en œuvre une procédure de gestion des incidents, basée sur ITIL, qui permet l'établissement de l'inventaire des incidents et leur analyse.

Le suivi des incidents de sécurité fait l'objet d'un point mensuel avec le RSSI, le DGS, la Direction des Services Numériques.

**Statut** : Opérationnelle

## 13. CONTINUITE D'ACTIVITE

### Objectif

Anticiper sur les mesures à prendre en cas d'interruption de processus métier critiques afin d'en limiter les impacts

### R13.1 Externalisation des sauvegardes

Le service Territoires Numériques est garant de l'externalisation des sauvegardes en cohérence avec le plan de sauvegarde qui prévoit :

- la sauvegarde locale journalière des machines virtuelles ;
- l'externalisation mensuelle des machines virtuelles ;
- l'externalisation journalière de Teampass.

**Statut** : Opérationnelle

### R13.2 Modes dégradés

La Direction des Solutions Numériques définit et établit, selon les résultats des révisions de l'homologation, les modes dégradés pour les services numériques sensibles :

- Teampass
- Gedeon & AFC

**Statut** : En cours

## 14. CONFORMITE

### Objectif

Etre conforme aux dispositifs réglementaires et à sa propre politique de sécurité du SI

#### R14.1 RGS

SOLURIS doit disposer d'un RSSI nommé et formé, en charge de garantir l'homologation de sécurité de l'établissement au Référentiel Général de Sécurité.

**Statut** : Opérationnelle

#### R14.2 RGPD

SOLURIS doit disposer d'un Délégué à la Protection des Données (DPO) nommé et formé au plus tard pour le 25 mai 2018, en charge de garantir la conformité de l'établissement au Règlement Général de Protection des Données.

**Statut** : Opérationnelle