Guide d'accueil des nouveaux élus

Soluris, votre partenaire de confiance

Vous êtes adhérent.e Soluris et venez d'être élu·e dans votre collectivité.

À l'occasion de ce nouveau mandat, nous souhaitons attirer votre attention sur un **enjeu devenu central pour les collectivités** : **le numérique**.

Le numérique est au **cœur du fonctionnement des collectivités** : gestion des collectivités, services à la population, administration numérique, cybersécurité, matériels sécurité et hébergement.

Soluris, un syndicat informatique créé par les élus pour les élus

Soluris en tant qu'Opérateur Public de Service Numérique **(OPSN**) basé à Saintes, **accompagne 545 collectivités (Charente-Maritime et Deux-Sèvres) dans la mise en œuvre d'une stratégie numérique cohérente et adaptée à vos besoins.**

Notre rôle est de vous permettre de :

- Disposer d'un **interlocuteur de proximité** et de confiance ;
- **Garantir la sécurité et la conformité de vos données** : Soluris est le délégué à la protection des données mutualisé de ses adhérents ;
- Bénéficier d'**offres adaptées** selon la taille de votre collectivité et à l'évolution de vos besoins.
- Être **acteur des choix stratégique de Soluris** (chaque collectivité adhérente dispose d'un droit de vote au Comité Syndical).
- Accéder à des **solutions mutualisées** pour optimiser vos coûts.

L'adhésion à notre **modèle mutualisé** permet à votre collectivité de **bénéficier de nombreux services et solutions selon vos besoins**. Cela passe par une par une **cotisation annuelle**, et selon vos besoins, vous pouvez opter pour un ou deux forfaits :

- **Forfaits Métiers** : assurer vos besoins fonctionnels et réglementaires.
- **Forfaits Technologiques** : pour répondre aux obligations de sécurités.

En tant que **membre du réseau national Déclic regroupant les OPSN**, Soluris s'inscrit dans une dynamique nationale d'innovation numérique de partage d'expertises entre acteurs publics, afin de **défendre vos intérêts** et d'**anticiper les évolutions.**

Bien cordialement,
Hubert COUPEZ, Président de Soluris

FOCUS

Dates à retenir :

- Désignation des délégués titulaires et suppléants : délibération à envoyer à Soluris avant **le 7 mai 2026**
- Date limite de dépôt de liste pour siéger au Bureau Syndical : **22 mai 2026**
- 1er Comité Syndical : **le 11 juin 2026**

Table des matières

Les fiches pratiques

Fiche 1 - Usage d'une boîte mail professionnelle par les élus

Préconisation

Chaque élu doit **utiliser exclusivement une adresse mail professionnelle** fournie par la collectivité pour tout échange lié à son mandat (communications internes, échanges avec les administrés, partenaires, services, etc.).

Il est recommandé de :

> **Ne jamais utiliser une adresse personnelle** (Gmail, Yahoo, etc.) pour des sujets liés au mandat.
> **Séparer strictement les usages** (professionnel vs personnel).
> **Activer les dispositifs de sécurité** (mot de passe robuste, MFA si disponible)
> **Archiver les échanges** selon les règles en vigueur.

Motif juridiques

> **Responsabilité du traitement (RGPD)** : les données personnelles traitées dans le cadre du mandat relèvent de la responsabilité de la collectivité (responsable de traitement).
> **Obligation de sécurité (RGPD)** : la collectivité doit garantir la confidentialité, l'intégrité et la disponibilité des données.
> **Traçabilité et archivage** : les échanges professionnels peuvent relever du droit administratif (documents communicables, archives publiques).
> **Responsabilité de la collectivité** : l'usage de messageries personnelles empêche la maîtrise des traitements et expose à des non-conformités.

Risques sécurité

> **Compromission de compte (phishing / hameçonnage)** : utilisation d'adresses personnelles plus vulnérables pour des accès frauduleux aux échanges sensibles.
> **Perte de confidentialité des données** : hébergement sur des services non maîtrisés (hors cadre contractuel, parfois hors UE).
> **Absence de supervision et de journalisation** : impossible pour la collectivité de détecter un incident ou d'investiguer (pas de logs).
> **Fuite d'informations stratégiques** : décisions politiques, données d'administrés ou informations internes exposées.
> **Risque de fraude** (ex : fraude au président / faux ordres) Usurpation d'identité facilitée via messagerie non sécurisée.
> **Perte d'accès aux données** : en cas de changement de mandat ou perte du compte personnel.

Fiche 2 - Éviter les usages mixtes (pro / perso) du matériel

Préconisation

Le **matériel informatique** fourni par la collectivité (ordinateur, smartphone, tablette) doit être **utilisé uniquement dans le cadre des activités liées au mandat.**

Il est recommandé de :

> Ne pas installer d'applications personnelles non validées.
> Ne pas stocker de données personnelles sur les équipements professionnels.
> Ne pas utiliser le matériel pour des usages privés (réseaux sociaux personnels, achats, etc.)
> Utiliser des équipements distincts pour les usages personnels
> Respecter les politiques de sécurité (mises à jour, antivirus, verrouillage).

Motif juridiques

> **Principe de minimisation (RGPD) :** limiter les données traitées aux stricts besoins professionnels.
> **Sécurité des systèmes d'information (RGPD) :** obligation de protéger les équipements et les données.
> **Responsabilité de la collectivité :** le matériel reste sous sa responsabilité juridique.
> **Protection des données personnelles :** mélange des usages = risque de traitement non maîtrisé.
> **Cadre de la commande publique :** les équipements sont financés pour un usage professionnel.

Risques sécurité

> **Introduction de logiciels malveillants** Applications personnelles, téléchargements ou navigation non maîtrisée.
> **Exfiltration de données** Synchronisation automatique avec des clouds personnels (Drive, iCloud, etc.).
> **Contournement des politiques de sécurité** Installation d'outils non validés entrainant une perte de contrôle du SI.
> **Fuite de données en cas de perte/vol** Données professionnelles accessibles sans cloisonnement.
> **Mélange des environnements** Difficulté à distinguer ce qui relève du mandat d'erreurs d'envoi ou de partage.
> **Propagation d'incident au système d'information** Un équipement compromis peut servir de point d'entrée au SI de la collectivité.
> **Atteinte à la réputation** Usage inapproprié (réseaux sociaux, contenus) depuis un équipement officiel.

Fiche 3 - Mise à jour des informations dans le logiciel MADIS

Préconisation

- **Les informations relatives :**
  - au **responsable de traitement** (élu en charge).
  - au **référent RGPD / DPD.**

doivent être **tenues à jour en permanence dans le logiciel MADIS**.

- **Il est recommandé de :**
  - **Mettre à jour ces informations** à chaque **changement d'élu ou d'organisation**.
  - Vérifier les données au **minimum une fois par an.**
  - **S'assurer de la cohérence avec les autres documents** (registre RGPD, mentions légales, site web).
  - **Formaliser la mise à jour** (traçabilité interne).

Motif juridiques

> **Responsabilité (RGPD)** : identification claire du responsable de traitement et responsabilité ("accountability").
> **Désignation (RGPD)** : le référent RGPD est votre DPD de proximité qui est formé et échange avec votre DPD Mutualisé SOLURIS.
> **Obligation d'information des personnes concernées** : les administrés doivent pouvoir identifier un interlocuteur.
> **Principe de transparence (article 5 RGPD)** : exactitude et mise à jour des informations.
> **Exigence CNIL** : capacité à démontrer la gouvernance RGPD (pilotage, responsabilités identifiées).

Risques sécurité

> **Défaut de gouvernance des données :** absence d'identification claire des responsables entrainant des décisions non maîtrisées.
> **Non-gestion des incidents (violation de données) :** mauvais interlocuteur ou coordonnées obsolètes pouvant entrainer un retard de notification à la CNIL.
> **Non-conformité réglementaire :** informations erronées dans les mentions RGPD constituant un manquement aux obligations légales.
> **Perte de confiance des administrés** Impossibilité de contacter le bon interlocuteur pour l'exercice des droits (accès, rectification...).
> **Risque contentieux** : difficulté à démontrer la responsabilité en cas de litige.
> **Désorganisation interne** Mauvaise orientation des demandes (droits RGPD, sécurité, incidents).

Une mise à jour de vos informations sera réalisée par le DPD Mutualisé SOLURIS auprès de la CNIL à partir de mi-septembre sur la base des informations contenues dans MADIS.

Fiche 4 - Sauvegarde des données

Préconisation

L'objectif est de garantir l'intégrité et la disponibilité des données en appliquant strictement la règle d'or.

> **La Règle 3-2-1** : posséder 3 copies de vos données (l'originale + **2 sauvegardes**), sur 2 supports différents (disque dur, NAS, clé USB, bande, cloud), avec **1 copie externalisée** (hors du site principal).
> **La Règle 3-2-1-0** : la règle du 3-2-1 constitue la bonne pratique minimale pour réduire au maximum le risque de perte de ses données mais nous vous conseillons de réaliser ou de faire réaliser au moins un test de restauration par an.
> **Immuabilité et Déconnexion** : pour contrer les cyberattaques, votre sauvegarde sur clé ou disque dur doit être déconnectée (ne pas laisser le support branché en permanence sur votre ordinateur).
> **Chiffrement de bout en bout** : les données externalisées par Soluris sont chiffrées avant même de quitter votre infrastructure, ceci afin d'éviter toute fuite en cas de compromission du lien de transfert.

Motif juridiques

Une sauvegarde n'est utile que si elle est exploitable. L'organisation doit encadrer l'aspect humain et temporel.

> **Automatisation et Fréquence** : les sauvegardes externalisées sont automatisées pour éviter l'oubli humain. La fréquence a été définie avec vos services. Vos sauvegardes sur support doivent être réalisées en fonction de votre niveau d'acceptation de perte en nombre de jours de travail.
> **En cas de modification organisationnelle** : si vous modifiez votre arborescence de données, il est nécessaire que vous preniez contact avec nos services pour modifier le jeu de sauvegarde externalisé.

Risques sécurité

La mise en place de la **sauvegarde externalisée est effectuée uniquement sur le poste maitre** de votre collectivité ou le serveur.

Nous pouvons vous apporter du conseil pour la sauvegarde des autres postes de votre collectivité.

Nous vous invitons à continuer vos sauvegardes sur support tel que disque dur externe ou clé usb afin d'augmenter votre résilience et respecter la règle d'or.

Soluris vous accompagne dans le choix, l'installation et le suivi de vos postes et logiciels. Nos experts métiers, spécialistes des solutions déployées, vous assurent un accompagnement fiable et adapté.

GESTION DES COLLECTIVITÉS

Un accompagnement global pour optimiser votre organisation et vos outils :

> **Finances et comptabilités**
> **Ressources humaines**
> **Environnement de travail, gestion bureautique, messagerie et agenda collaboratif**
> **SIG (système d'information géographique)**

SERVICES À LA POPULATION

Des solutions numériques pour optimiser les services aux citoyens :

> **Relations citoyens (dont état civil et élections)**
> **Logiciels cimetière et gestion funéraire**
> **Enfance**
> **Bibliothèque**
> **Urbanisme**
> **Gestion des déchets**

ADMINISTRATION NUMÉRIQUE

Nos offres dématérialisées pour simplifier les démarches des concitoyens :

> **Actes : dématérialisation et numérisation**
> **Dématérialisation des marchés publics**
> **Dématérialisation des convocations des assemblées**
> **Passerelle de transmission Chorus**
> **Signature et parapheur électroniques**
> **Site web**

CONFIANCE NUMÉRIQUE

Soluris vous assiste dans la protection des systèmes d'information et la maîtrise de vos obligations :

> **Conseils en cybersécurité** (sensibilisation, accompagnement avec la méthode Cyberisq)
> **Protection de la vie privée :** DPD mutualisé, accompagnements dédiés
> **Sécurité numérique :** sensibilisation, homologation et accompagnement à la conformité (Référentiel Général de Sécurité (RGS), cybersécurité (NIS 2), etc.)
> **Continuité des services face aux risques Cyber :** Plan de Continuité d'Activités (PCA Cyber), Plan Communal de Sauvegarde (PCS Cyber), gestion de crise

MATÉRIELS, SÉCURITÉ ET HÉBERGEMENT

Soluris propose un accompagnement technique de proximité sur site et à distance pour :

> **Matériel informatique :** PC, serveurs, accessoires
> **Logiciels et abonnements :** Adobe, TeamViewer, AutoCAD, etc.
> **Sécurité informatique :** pare-feu, antivirus, protections, etc.

2 rue des Rochers - 17100 Saintes - **www.soluris.fr**
Assistance téléphonique : 05 46 92 39 05 Du lundi au vendredi de 9h à 12h30 et de 14h à 17h30 (16h30 le vendredi)

SOLURIS
SOLUTIONS NUMÉRIQUES TERRITORIALES INNOVANTES