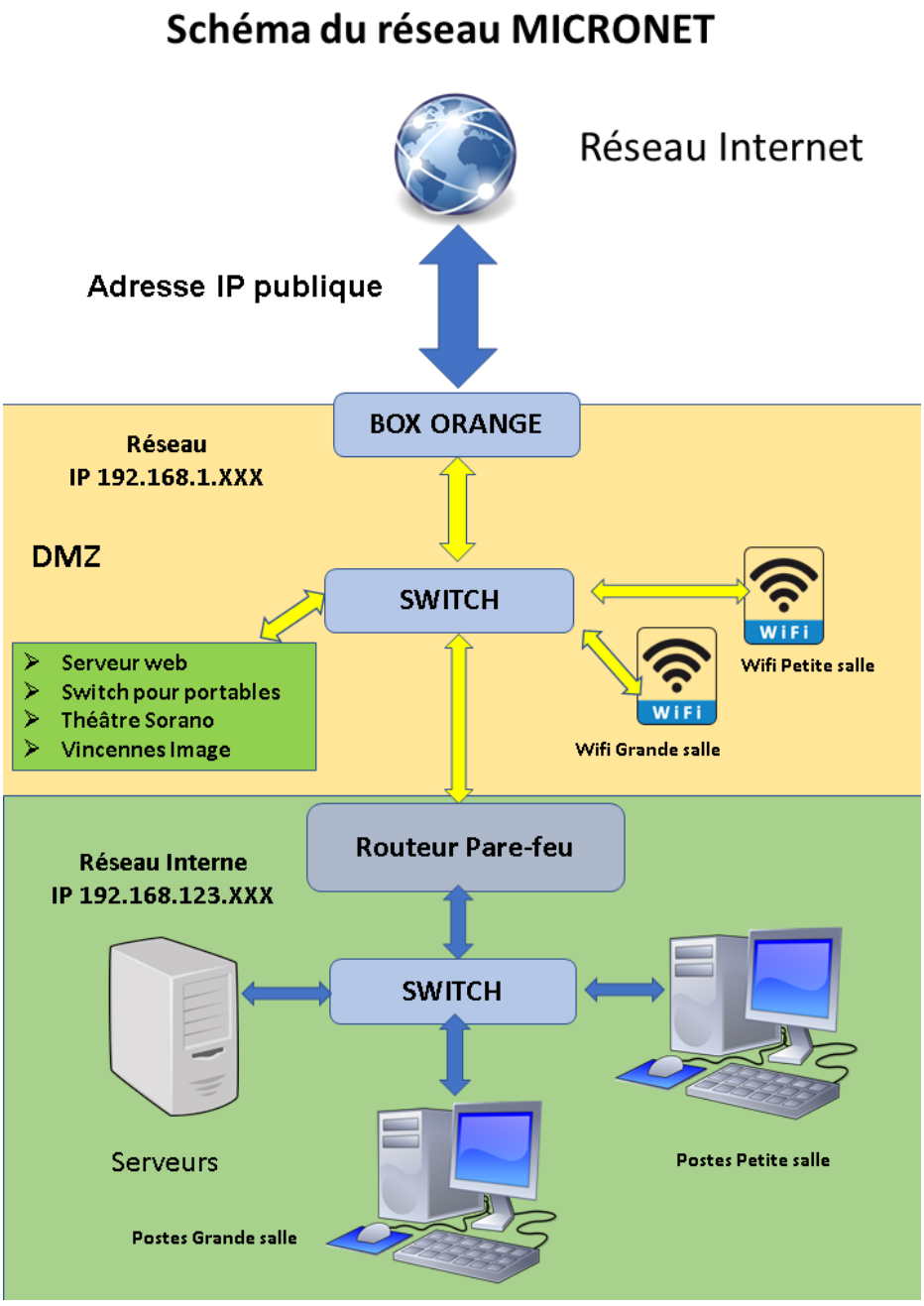
– Charte des données personnelles au club MICRONET.

La loi du 6 janvier 1978 modifiée par la **LOI n° 2016-1321 du 7 octobre 2016,** définit les règles de protection des droits d'accès, de rectification et d'oubli des données personnelles.

Cette procédure décrit les mesures prises pour la protection des données personnelles dans l'association MICRONET.

1 – Réseau informatique et connexion aux ordinateurs.

1 – 1 Schéma du réseau.



Le club est relié à la fibre fournie par Orange. La box Orange alimente un Switch qui partage la connexion entre le réseau interne protégé par un routeur - pare-feu et la zone DMZ (Zone Démilitarisée où sont traitées les données qui n'ont pas besoin d'être dans le réseau interne).Les box Wifi qui y sont connectées sont sécurisées à la norme WPA2.

Sur cette DMZ un adhérent peut connecter son ordinateur portable ou sa tablette après avoir choisi le réseau Wifi Micronet-GS ou Micronet-PS et saisi le mot de passe correspondant. Chaque adhérent se connectant dans cette DMZ sera responsable de la sécurité de son appareil : ordinateur, tablette, smartphone (antivirus, pare-feu, …)

1 – 2 Connexion sur les postes informatiques.

Chaque ordinateur du réseau mis à disposition des adhérents dispose de trois comptes d'accès.

- Compte **MICRONET** : compte local sans propriétés d'administrateur du poste.
- Compte **MICROXXX** : compte local avec propriétés d'administrateur.
- Compte **Install** : réservé aux administrateurs des postes et du réseau.

Chaque compte est protégé par un mot de passe qui sera communiqué par l'animateur.

À chaque démarrage du poste de travail, la partition C: « le disque C : ») est remis à l'état d'origine, le bureau, les connexions, tout fichier ou logiciel installé sont effacés de même que les informations de navigation. Si des logiciels ou des fichiers ont été supprimés, ils sont réinstallés.

Chaque utilisateur devra sauvegarder ses documents sur une clé USB, un disque dur externe ou dans le cloud.

Les règles de sécurité auxquelles chaque adhérent doit se conformer :

- Signaler au service informatique interne tout dysfonctionnement ;
- Ne pas stocker des données personnelles sur le disque **D:\Données** présent sur chaque poste et accessible à toute personne utilisant ce dernier. Ces fichiers peuvent être supprimés à tout moment.
- Respecter les procédures définies par le Club MICRONET afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en respectant les règles de sécurité ;
- Verrouiller son ordinateur dès que l'on quitte son poste de travail et arrêter le poste à la fin des séances des cours ou de travail personnel.

Pour transférer un document en interne à partager avec d'autres adhérents : un raccourci vers un lecteur réseau **¨Dossier-partage¨** est présent sur le bureau de chaque poste ; tout adhérent peut créer un dossier à son nom et y déposer les documents de son choix. Ces dossiers et fichiers sont accessibles à tous les adhérents et ne sont pas protégés : tout le monde peut les supprimer plus ou moins accidentellement. Les responsables informatique se réservent le droit de les supprimer.

2 – Saisie des données personnelles des adhérents.

En application de la loi du 6 janvier 1978 modifiée par la **LOI n° 2016-1321 du 7 octobre 2016**, l'adhérent bénéficie d'un droit d'accès, de rectification et d'oubli des informations qui le concernent. Si l'adhérent souhaite exercer ce droit, il doit s'adresser au responsable de la base de données (ou par défaut au président).

L'enregistrement des données personnelles est effectué par le responsable de saisie de la base de données. Elles sont saisies dans un fichier protégé par un mot de passe.

Elles sont stockées soit dans un espace réservé au responsable, soit sur un support amovible. Dans le cas du lecteur amovible, des sauvegardes devront être faites régulièrement.

Les chèques remis par les adhérents sont scannés et les scans sont sécurisés comme le reste des données.

Les données personnelles des adhérents ne seront transmises en totalité ou en partie qu'aux personnes dûment autorisées :

- En totalité au président
- Partiellement au secrétaire, au trésorier, au directeur technique
- Partiellement au secrétariat de l'Espace SORANO, suivant la procédure mise en place par celui-ci.

Tout incident doit être écrit sur le cahier « Incidents et anomalies » mis à disposition dans chaque salle.

3– Gestion des bulletins d'adhésion.

Les bulletins d'adhésion, contenant toutes les informations sur les adhérents – ainsi que leur signature validant les informations et le droit à l'image, sont conservés dans une armoire fermée à clé (le président, le secrétaire et le trésorier ayant la clé de l'armoire).

4- Durée de stockage des données.

Les scans des chèques sont détruits en fin d'exercice.

Après 6 ans :

- Les données informatiques d'adhésion sont supprimées.
- Les bulletins d'adhésion sont détruits.

Après 10 ans : sont détruits

- Tous les documents comptables (comptes de résultat, bilans, factures clients et fournisseurs, documents bancaires, comptes annuels, livre-comptable, grand livre et livre d'inventaire).
- Les pièces justificatives de la comptabilité : factures, pièces bancaires, etc.,
- **Les contrats passés (le délai prend effet 10 ans après la fin du contrat**).

Remarque : les documents papiers sont broyés avant remise au recyclage.

5- Saisie comptable.

Les données comptables sont entrées exclusivement sur un ordinateur dédié, protégé par un mot de passe, stocké dans une armoire fermée à clé. Seuls le (ou la) comptable et le (ou la) président(e) ont le mot de passe.

Les données comptables sont sauvegardées sur un support amovible chiffré.

6- Mailing liste.

Les mail listes sont gérées par un responsable désigné. La mail liste des adhérents de l'année et les mail listes de diffusion d'informations sont modérées. Seules les mail listes animateur, conseil d'administration et bureau ne sont pas modérées.

Sur les envois par mail liste, figurent la mention et le lien pour se désabonner de cette mail liste. Un adhérent inscrit sur la liste de l'année ne peut se désabonner que s'il a remis par écrit sa démission comme adhérent de l'association. Il n'y aura pas de remboursement de la cotisation au prorata temporis.

Toute la communication (convocation à l'assemblée générale, informations sur la vie de l'association…) se fait uniquement par l'intermédiaire de la mail liste de l'année en cours.

7 – Gestion site Web.

Les codes d'accès à l'administration de l'hébergeur OVH du site Web sont détenus par :

- Compte super administrateur : Président et Secrétaire.
- Accès à la facturation : Trésorier et Président.
- Accès à la base de données, hébergement, ftp : Directeur Technique, Secrétaire et Président
- Sur le gestionnaire du site web : Directeur Technique et Président.
- Rédacteur en chef : Président
- Rédacteur : Secrétaire, responsable communication ou toute autre personne désignée par le bureau de l'association.

8 – Mise à jour des postes de travail et serveurs.

Les mises à jour des systèmes d'exploitation des ordinateurs et serveurs Windows sont faites tous les mois. Régulièrement une vérification des mises à jour des autres programmes installés sur les postes est effectuée. Une mise à jour est lancée si une faille de sécurité est concernée. Si cela n'implique qu'une nouvelle version, la mise à jour est faite au moins annuellement.

9 –Vérification des procédures.

Une vérification des procédures sera effectuée annuellement pour vérifier si d'éventuels changements concernant les données des adhérents respectent la présente charte.

La liste des personnes désignées par leur fonction sur ce document est affichée dans les locaux.