PLAN DE REPRISE D'ACTIVITE INFORMATIQUE APRES SINISTRE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA SANTÉ,
DE LA JEUNESSE,
DES SPORTS
ET DE LA VIE ASSOCIATIVE

SECRÉTARIAT D'ÉTAT
AUX SPORTS,
A LA JEUNESSE ET
A LA VIE ASSOCIATIVE

Version 1.1
2009-01-23

Sujet de stage d'entreprise.
Olivier Houbloup. Stagiaire AFPA 2008-2009

Sommaire

1 Introduction

Ce rapport technique contient des données sensibles à la sécurité de l'information de la DRDJS de Franche-Comté.
Il est donc obligatoire de respecter une stricte confidentialité de lecture, et bien entendu, de non-divulgation.

Ce rapport technique s'adresse à toute personne appelée à intervenir pour une reprise, après sinistre dans les locaux de la DRDJS de Franche-Comté.

Dès lors que la fonction de cette personne contribue en partie à définir, implémenter, maintenir ou garantir la sécurité, ce rapport permet une approche moins fastidieuse de la reprise après incident.

L'élaboration de ce Plan de Reprise d'Activité Informatique après sinistre (PRAI), via des procédures flexibles, vise dans un premier temps à garantir le service minimum requis pour les systèmes d'information.

Afin d'assurer par la suite une continuité d'activité totale, j'ai essayé d'étoffer et de structurer au mieux cette documentation.

Plusieurs niveaux de reprise sont abordés dans ce rapport. J'ai essayé d'ordonner thématiquement les différentes procédures de reprise, à la fois en fonction de la panne plausible et de sa résolution, mais aussi en fonction du type de supports informatiques (stations de travail, serveurs).

Ce document traite uniquement de la partie informatique, et plus précisément de la remise en place du réseau.

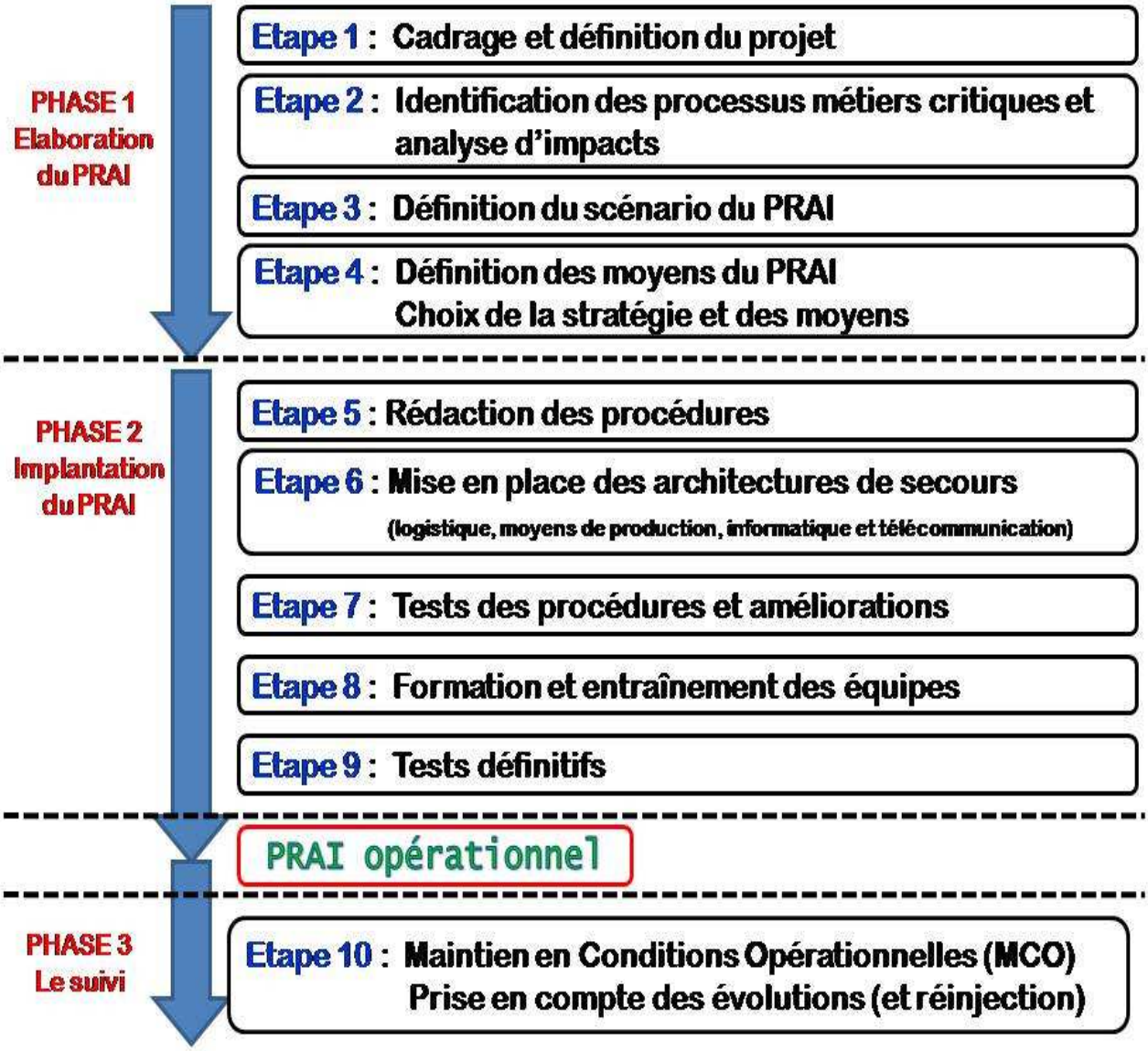
L'informatique évolue très vite. Il n'est pas toujours simple de tenir à jour les nouvelles modifications apportées et leurs effets. Il serait donc souhaitable de tenir à jour ce document autant que possible. Je conseille de prendre le temps, à chaque utilisation de celui-ci, d'introduire toutes les nouvelles procédures et tous les éléments permettant de l'actualiser.

Pour cet usage, sur le serveur de fichiers (___.___.___.___), le répertoire « \\Travail\CIL » contient ce présent document et la totalité des éléments ayant permis sa mise en œuvre (aides, tutoriels, programmes, …)

2 Organisation et annuaire

Notre objectif final est d'être capable d'effectuer en cas d'incidents techniques, un plan secours informatique n'excédant pas plus de 24 heures de problèmes et d'interruption de service.

2.1 Notre démarche conceptuelle d'un projet de PRAI



2.2 Comité de crise

Lieu central de réunion :

Dans l'idéal de la logistique - et si cela est possible, il serait préférable que la structure de crise soit composée au minimum des directions suivantes :

DIRECTIONS	TELEPHONES	FAX
Direction Générale : - -		
Principales Directions utilisatrices : - - -		
Direction des Services Généraux et des Ressources Humaines : - -		
Direction Informatique : - -		
Direction de la Communication : - -		

Responsables du Plan de Secours : - -		

Assistance extérieure : - - -		

2.3 Cellule de coordination :

Lieu central de réunion :

COORDINATEURS	TELEPHONES	FAX
Responsables du Plan de Secours : - -		

Coordinateurs des opérations informatiques : - - -		

Coordinateurs de la logistique : - -		

2.4 Equipe d'intervention

EQUIPE D'INTERVENTION	TELEPHONES	FAX
Equipe logistique (rôle de transport) : - -		
Equipe communication : - -		
Agents de réseau : - -		
Agents de maintenance : - -		

Prestataire Internet : -		
Prestataire téléphonie : -		
Fournisseurs d'énergie : - -		

2.5 L'accès sécurisé aux données protégées

Le coffre fort administratif contient :

- Le code d'ouverture du coffre fort de la salle des serveurs
- le mot de passe de l'administrateur du réseau

Le coffre fort de la salle des serveurs contient :

- Le mot de passe de l'administrateur du réseau
- Le présent Plan de Reprise d'Activité Informatique
- Les CD-ROM d'installation des serveurs
- Les sauvegardes sur bande DLT

2.6 Documentation et matériel

L'anticipation des actions simples est nécessaire pour l'organisation et l'optimisation de la gestion de son temps en cas de sinistre.

2.6.1 Gestion des logiciels originaux et du matériel de remplacement

Selon le cas de reprise après sinistre, les logiciels originaux ne sont pas forcément nécessaires. Néanmoins, il est conseillé de les garder bien à l'abri. Aussi est-il judicieux de les ordonner et de les référencer, en cas d'utilisation imprévue et pour favoriser leur accès facile et rapide. Concernant le matériel dit de remplacement, le même type de prévention doit être appliqué, afin de ne pas perdre de temps au moment opportun.

2.6.2 Matériel à prendre le jour de l'intervention

Pour le moment, cette documentation et son annexe contribuent principalement au plan de secours informatique.

Selon les fonctions de chacun, il peut être nécessaires de penser à :

- Ses codes d'utilisateur et mots de passe personnels
- Ses manuels de mode d'emploi selon les éléments informatiques
- Ses feuillets d'intervention et de résolution de tâches
- Son appareil de communication téléphonique ou tout autre moyen de communication.
- Sa trousse à outils selon le type d'interventions
- Ses supports amovibles de données (clé usb, disques durs)
- …

3 Bilan de l'existant - *OCS inventory*

3.1 Existant matériel et logiciel

La base de données fournit par OCS inventory permet aussi de connaitre le type de matériel et sa date de fin de garantie de service. Chaque matériel sous garantie a la possibilité d'être livré en moins de 24 heures.

3.1.1 Station de travail

Une base de données est régulièrement tenue à jour :
Nom de la base : OCS inventory
Accès : http:
Utilisateur : Mot de passe :

Ensuite, la base de données nous intéressant est celle de la DRDJS de Franche-Comté.

Etablissons une « recherche par multicritères »

Icône en haut à gauche avec une loupe.
Choix du paramètre : nom machine
Dans le champ correspondant à « EGAL » :

Ensuite, sous nom machine, nous pouvons obtenir les détails physiques et les logiciels de chaque station de travail.

Chaque station de travail doit comporter un nom bien précis en fonction des ordres ministériels.
Cf. Référentiel technique pour les systèmes d'information et de télécommunication / version 2.1 / juillet 2008.

3.1.2 Serveurs

Une base de données est régulièrement tenue à jour :
Nom de la base : OCS inventory
Accès : http:
Utilisateur : Mot de passe :

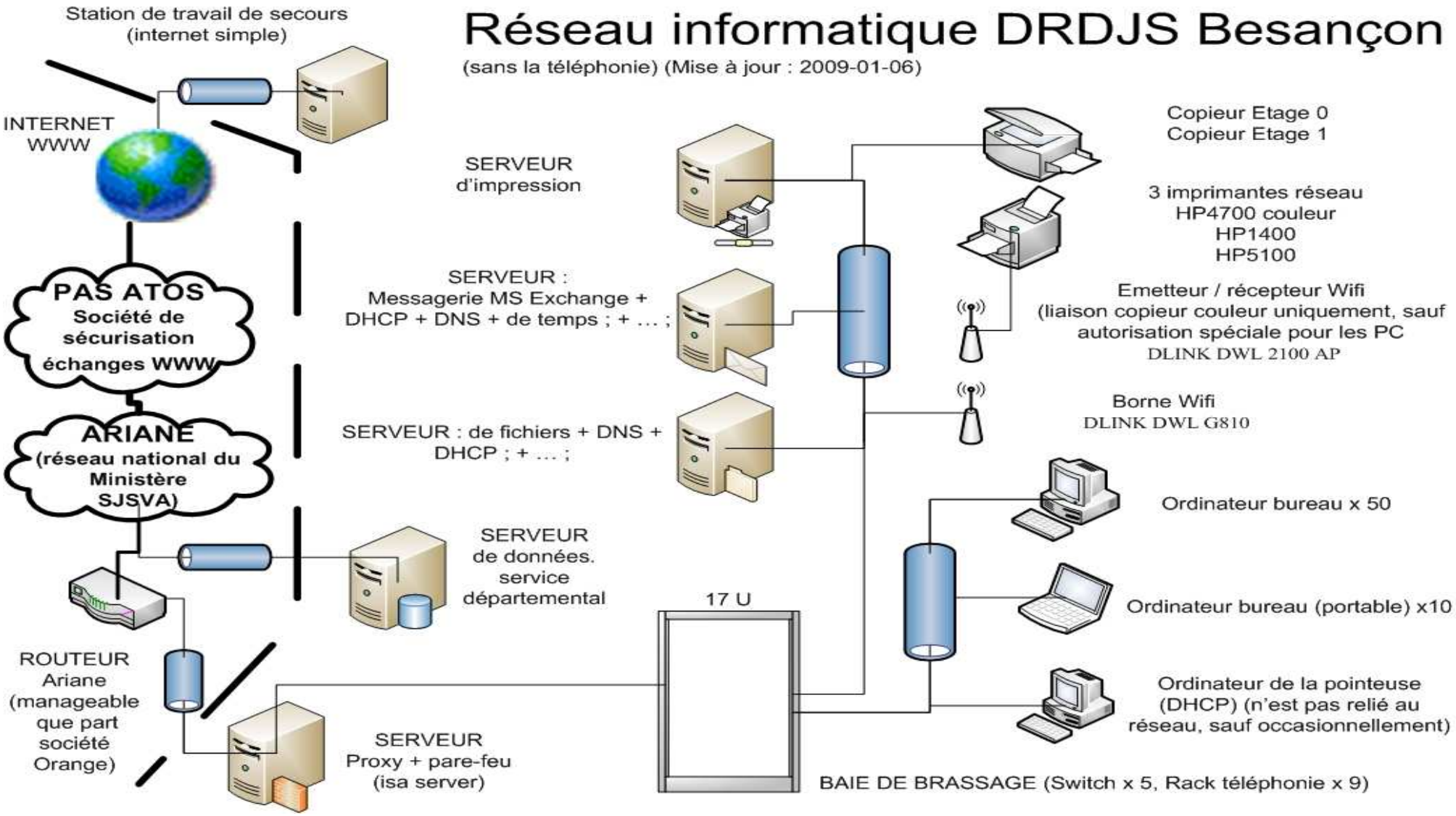
Ensuite, la base de données nous intéressant est celle de la DRDJS de Franche-Comté.

Etablissons une « recherche par multicritères »

Icône en haut à gauche avec une loupe.
Choix du paramètre : serveur
Dans le champ correspondant à « EGAL » :

Ensuite, sous nom machine, nous pouvons obtenir les détails physiques et les logiciels de chaque serveur.

3.1.3 Schéma par création sous le logiciel « Microsoft Visio 2007»



3.2 Classification de l'adressage complet du réseau

Ce tableau, plus précis que les schémas, permet une plus grande souplesse de lecture.

Matériel	Fonctions	Adresse IP	Activé
Boitier noir N°127	Serveur données service départemental 4 services départementaux de comptabilité ont leur accès : Besançon + Lons le Saunier + Belfort + Vesoul		oui
NEC EXPRESS 5800 /120 Eh2	Serveur de fichiers *+ fonction de contrôleur de domaine* *+ Serveur DHCP* +Serveur de temps + serveur DNS (préféré)		oui
NEC TM 800 boitier N°111	Serveur de messagerie Microsoft Exchange		oui
	Serveur DHCP		oui
	+ Serveur DNS (secondaire)		oui
	+ Rôle FSMO + fonction contrôleur de domaine		oui
Boitier Blanc N°89	Serveur Microsoft Windows Server Update Services (WSUS) (A mettre ne place)		oui
	Serveur d'impression		oui
Boitier gris N°101	Serveur proxy. Rôle de pare-feu		oui
Boitier Blanc N°46	Serveur de secours (liaisons internet simple)		non
CANON IR 5055/5065	Copieur multifonctions situé à l'étage 1		oui
CANON IR 5055/5065	Copieur multifonctions situé au rez-de-chaussée		oui
HP LASER JET P4010_P4510 Series	Imprimante située au rez-de-chaussée		oui
HP LASER JET 5100	Imprimante située à l'étage 1		oui
HP Color laser Jet 4700 PCL6	Imprimante couleur située à l'étage		oui
DLINK DWL 2100 AP	Emetteur / récepteur WIFI		oui
DLINK DWL G810	Borne WIFI crypter en WPA ; clé de 40 caractères aléatoire		oui
DLINK DGS 1216T	Switch programmable (baie de brassage)		oui
DLINK DGS 1216T	Switch programmable (baie de brassage)		oui
	PABX programmable		oui
Unités centrales diverses (X50) et portables divers (X10)	Station de travail utilisateur sous Windows XP et 2000. IP donnée par le serveur DHCP		oui

4 Méthodologie de prévention avant sinistre

La prévention d'un sinistre et des incidents doit mettre en avant certains aspects importants.

1) Sécurisation du local informatique
   Local aux normes de sécurité et accès règlementé.

2) Sécurisation des données par du matériel adéquat
   Type de matériel utilisé, type de protection

3) Qualité d'intervention possible et étude de faisabilité
   Sauvegarde et restauration des données sans pertes

4) Remise en question permanente sur les sécurités adoptées : fiabilité et durée de vie.

4.1 Politique actuelle de gestion des serveurs

Pour faciliter la restauration et diminuer l'impact des ennuis sur l'ensemble du fonctionnement de la DRDJS, la politique au niveau des serveurs est de créer plusieurs ordinateurs-serveurs, selon leurs fonctions.

Bien que cette façon de procéder augmente statistiquement le nombre de pannes, cela permet en contrepartie une politique plus souple de gestion de sinistre, et donc « individuelle » selon la fonction ou les fonctions du serveur.
Pour le moment, c'est le meilleur compromis, vu la configuration actuelle.

Actuellement, ces points sont appliqués sur les serveurs :

- Protection électrique des serveurs par des onduleurs
- Serveurs utilisant la technologie RAID pour les données
  - Sur le serveur d'adresse IP ___.___.___.___, les deux disques SCSI sont montés en RAID 1 pour le système d'exploitation et les 3 autres disques SCSI en RAID 5 pour les fichiers des utilisateurs. (il y a en tout 5 disques SCSI)
  - Sur le serveur d'adresse IP ___.___.___.___, les deux disques SCSI sont montés en RAID 1 pour le système d'exploitation et le serveur Exchange
- Sauvegarde quotidienne des fichiers, de la banque d'information du serveur de messagerie, avec rotation sur trois semaines, sauvegarde de la configuration du proxy à chaque modification de celle-ci
- Duplication de certaines configurations (DHCP, DNS)
- La gestion du service d'impression est assurée par le serveur d'adresse IP ___.___.___.___
- Documentation papier sur les configurations et les procédures.

4.1.1 Précision sur les Serveurs d'adresses IP ___.___.___.___ et ___.___.___.___ :

- Au sujet des serveurs DHCP et des serveurs DNS, nous en avons volontairement mis un de chaque en activité sur chaque ordinateur, afin d'augmenter la sécurité et par là même, la facilité d'accès en cas de panne éventuelle de l'un des ordinateurs.
- Sur les mêmes bases de précaution, ces deux ordinateurs assurent chacun les fonctions de contrôleur de domaine. Il est important de savoir que l'Active Directory est répliquée entre ces ordinateurs (contrôleur de domaine) afin de garder toujours la version la plus récente en fonctionnement.

5 La sécurité

5.1 Hiérarchisation d'importance des données

Au niveau du serveur de fichiers, il est important de noter la manière dont les fichiers sont partagés (Fichiers du répertoire travail).

Données très importantes :

- Bases de données production / comptabilité
- Données confidentielles des Directions (DRH, Directeurs, Directeur adjoint, …)
- Données messageries
- Dossiers utilisateurs avec production personnelle

Données importantes :

- Archives utilisateurs
- Configuration bureautique

Données moins importantes :

- Informations téléchargeables
- Documentations partagées avec d'autres centres

5.1.1 Détermination de notre méthode de sauvegarde pour les données

L'étape suivante consiste à déterminer la meilleure méthode pour la sauvegarde de nos données. Les systèmes de sauvegarde offrent pour la plupart une grande variété d'options. Les plus courantes sont les suivantes :

Méthode complète :

Cette méthode transfère sur bande une copie de toutes les données concernées par la sauvegarde, indépendamment de la modification des données depuis l'exécution de la précédente sauvegarde.

Méthode différentielle:

Cette méthode sauvegarde tous les fichiers modifiés depuis la précédente sauvegarde complète, indépendamment de leur modification depuis la dernière opération de sauvegarde, quel que soit son type.

Méthode incrémentale :

Ici se verront transférer sur bande, les seuls fichiers modifiés depuis la dernière opération de sauvegarde, quel que soit son type (complète, différentielle ou incrémentale).

5.1.1.1 Conclusion pour notre méthode actuelle de sauvegarde

Nous utilisons actuellement des bandes DLT. La taille des données utilisateurs ne dépasse pas encore les 70 GO. Pour ces données, nous pouvons garder une méthode complète très fréquente (ex : tous les soirs), avec un cumul de trois semaines des sauvegardes journalières.

Concernant l'ensemble des serveurs, actuellement, toute l'installation et toutes les données ne dépassent pas les 200 GO. Nous pouvons envisager par exemple une méthode complète sur un seul disque dur de 1 TERA, dont la fréquence serait hebdomadaire. Bien entendu, un cumul de 4 sauvegardes hebdomadaires est conseillé.

Il a été abordé entre nous l'utilité de déporter les données sur un site extérieur, en cas d'incendie par exemple. Cette solution n'est actuellement pas envisagée et ne semble pas utile, vu le type de données.

Un coffre fort ignifuge, d'une durée de résistance d'environ 20 minutes, sert actuellement de stockage des bandes DLT.

5.2 Précautions d'usage

Quel que soit le matériel, il faut d'abord déterminer quel est l'élément (ou les éléments) en cause. Cela peut passer par des manipulations précises de test.

Dès qu'il y a possibilité de remplacer un élément défectueux, aussi petit soit-il, il faut donc avoir un listing détaillé de chacun d'entre eux. Ce listing doit comporter les références de l'élément et des personnes (ou sites Internet) à contacter.

Cette manière de procéder a pour objectif de gagner du temps au moment de l'incident.

Prévoir deux types de matériel :

- Celui que l'on doit commander, en connaissant le délai avant rétablissement
- Celui qui existe à disposition immédiate « sans » délai avant rétablissement

Concernant donc la disponibilité avec délais, vérifier dans le contrat de service et de garantie. En général, le délai est de 24 à 48 heures avec jours ouvrés.

Prévoir une manière de tester le matériel :

Il est important de référencer aussi par type de matériel les dates de fin de garantie sur site fournisseur et selon le constructeur. Cela afin d'anticiper un nouvel achat plutôt qu'une impossibilité de remplacement sous garantie. Grâce à OCS inventory (Cf. Bilan de l'existant), ces données sont présentes. La création d'un échéancier peut aussi être utile.

Exemple de canevas d'échéancier pour anticiper le vieillissement technologique :

Matériel	Date de fin de garantie		Estimation du moment d'obsolescence de la technologie	Date de remplacement
	sur site	constructeur		

5.2.1 Anticipations par les utilisateurs

L'intérêt d'un réseau n'existe que s'il y a des individus connectés. Le souci premier est donc cette perte de connexion et par extension technologique, la perte des données plus ou moins centralisées de ces individus. Par la bonne utilisation des ressources informatiques, il est donc important que les utilisateurs puissent se prémunir dans leur champ d'action possible des désagréments d'un sinistre.

Il faut responsabiliser les utilisateurs et ne pas tout faire reposer sur les « gestionnaires » du réseau. Cette anticipation par les utilisateurs a un intérêt double : renforcer leur accès aux données, en épargnant du temps et des manipulations pour les « administrateurs » réseaux.

5.2.2 Anticipation sur manipulation de fichiers et messagerie Outlook 2003

Apprendre aux utilisateurs à manipuler des données (dossiers, fichiers) et les synchroniser. Cela représente certes peu d'intérêt car les données en accès du réseau sont facilement recouvrables. Je me suis ainsi aperçu que des utilisateurs n'étaient pas à l'aise avec simplement les fonctions de copier/coller et même n'avaient pas une vision correcte d'une arborescence à partir de l'explorateur de Windows. Je pense que des formations plus fréquentes dans ce domaine seraient utiles.

L'utilisation de la messagerie sous Outlook 2003 est omniprésente. Beaucoup d'utilisateurs ne savent pas créer et tenir à jour des contacts ainsi que des listes de diffusion!

Même si le logiciel Outlook 2003 est pauvre en convivialité, il serait bon d'obliger les personnes à savoir créer et manipuler un contact.

A la suite des réinstallations, au niveau des serveurs, trop d'utilisateurs se sont plaints de ne plus retrouver un contact sur la simple saisie automatique d'un nom. Il y avait confusion entre saisie automatique des mots dans Windows et création d'un contact. En bilan, beaucoup de temps perdu pour les administrateurs à cause d'un manque de « sérieux » (et/ou de volonté) ou de méconnaissances informatiques des utilisateurs. A mon avis, à ce niveau-là aussi, l'utilité de formations fréquentes est indispensable.

5.3 Amélioration de cette politique de sécurité

Il faut construire cette politique correctement – de manière fiable et efficace, en tenant prioritairement compte des recommandations ministérielles. Par contre, prendre en compte le degré réalisation de cette politique et la réalité de l'utilisation au quotidien de cette sécurité par les utilisateurs est un aspect non négligeable. En effet, l'application des recommandations ministérielles diffèrent des possibilités réelles.

Recommandations tenant compte des utilisateurs :

Chaque station de travail doit être protégé par :
- Un mot de passe utilisateur non devinable par un collègue
- Un mot de passe administrateur

Chaque utilisateur doit avoir en plus du dossier commun, un dossier personnel protégé par un mot de passe unique et personnel.

6 Méthodologie de recouvrement après sinistre

En cas de sinistre nécessitant le recouvrement complet du réseau, il faut tout d'abord agir intégralement au niveau de la fonctionnalité propre du réseau puis agir sur les stations de travail utilisateurs.

6.1 Ordre de priorité de restauration

Toutes les données et tous les serveurs sont importants.
Néanmoins, dans le cas d'une complète remise en service, voici l'ordre de priorité :

1) Le serveur de fichier (50 Go de données) (est contrôleur de domaine)
2) Le serveur proxy (Isa Serveur) avec le pare-feu
    - Est lié à l'Internet et à la messagerie externe
3) Le serveur de messagerie (il est contrôleur de domaine)
4) Microsoft Exchange (3 Go de données)
    - Lié à la messagerie interne et au calendrier partagé
5) Le serveur offrant le DNS et le DHCP (est de toute manière obligatoire pour le réseau)
6) Le serveur d'impression
    - Lié aux imprimantes et copieurs multifonctions

6.2 Incidents matériel

6.2.1 Au niveau de la baie de brassage et autres connectiques

Matériel	Test	Quantité en Disponibilité immédiate	Disponibilité avec délais	Comment contacter ?
Routeur Fournisseur d'accès internet	Appel FAI	Non	Oui	Tél. Opérateur ADSL :
Hub	Voyants et entre PC	Non	oui	Tél. fournisseur :
Switch	Voyants et entre PC	Non	Oui	Tél. fournisseur :
Câble réseaux	Entre deux autres PC	Oui : 2 %	Oui	Tél. fournisseur :

6.2.2 Au niveau des serveurs

- En cas d'arrêt partiel ou total des serveurs, tester les onduleurs.
- Identifier la nature de la panne et évaluer le délai de mise en route.
- Identifier les services utilisables de ceux qui ne le sont pas.
- Prévenir les utilisateurs sur les services utilisables ou non et le temps estimé de retour à la normale, par service si possible.

Matériel	Test	Quantité en Disponibilité immédiate	Disponibilité avec délais	Comment contacter ?
Bande de sauvegarde	A déterminer. Au mieux sur un autre serveur	Non	Oui	Tél. fournisseur :
Carte graphique	Sur autre PC	Oui :	oui	Tél. fournisseur :
alimentation	Sur autre PC	Oui :	oui	Tél. fournisseur :
Carte mère + processeur + RAM	Effectuer test autres composants et déduire !	Non	oui	Tél. fournisseur :
Disques dur et connectique	Accès aux données sur un autre pc si possible ?	Non	oui	Tél. fournisseur :
Lecteur DVD / CD	Sur autre PC si possible ?	Non	Oui	Tél. fournisseur :
Onduleurs	Tester avec un PC non serveur	Non	oui	Tél. fournisseur :

6.2.3 Au niveau des stations de travail des utilisateurs

Matériel	Test	Quantité en Disponibilité immédiate	Disponibilité avec délais	Comment contacter ?
Carte graphique	Sur autre PC	Oui :	oui	Tél. fournisseur :
alimentation	Sur autre PC	Oui :	oui	Tél. fournisseur :
Carte mère + processeur + RAM	Effectuer test autres composants et déduire !	Non	oui	Tél. fournisseur :
Disques dur et connectique	Accès aux données sur un autre pc	Oui :	oui	Tél. fournisseur :
Lecteur DVD / CD	Sur autre PC si possible ?	Non	Oui	Tél. fournisseur :

Pour les périphériques simples comme les claviers, souris, clés usb, …, il suffit d'avoir quelques éléments et de les commander occasionnellement.

Existe aussi la possibilité de garder quelques ordinateurs mis de coté lors du renouvellement de certaines stations de travail par de plus récentes, et ce dans l'idée de dépanner l'utilisateur rapidement et de ne pas interrompre son travail. Ces stations de travail doivent être le plus proche possible de l'état fonctionnel et permettre de gérer une panne occasionnelle.

Au sujet des périphériques d'impression, le nombre suffisant et la disponibilité de plusieurs éléments grâce au serveur d'impression garantissent une certaine pérennité avant remplacement. De plus, les copieurs numériques multifonctionnels sont en général sous contrat de location.

Concernant la téléphonie, il faut se reporter au contrat de service et de maintenance.

6.3 Incidents logiciels

Les incidents logiciels sont multiples et ce sont les plus difficiles à résoudre en général. Et souvent l'impossibilité d'effectuer une manipulation ou un message d'erreur prévient l'utilisateur. La difficulté réside dans l'interprétation de cette erreur.

En cas d'accès à Internet, il peut être souhaitable de vérifier si l'erreur est référencée :

http://support.microsoft.com/gp/errormessage/fr

Dans tous les cas, il vaut mieux partir de la source de l'erreur, c'est-à-dire de l'élément le plus éloigné du réseau où celle-ci se présente, avant d'aller vers l'intérieur du réseau.

Par exemple, un utilisateur ne peut pas se connecter à ses documents sauvegardés sur le serveur de fichiers. En général, c'est un paramétrage au niveau du poste utilisateur qui est source de l'erreur. Inutile alors de commencer par s'interroger sur un éventuel souci du serveur, surtout si c'est un cas isolé. En revanche, si ce problème est commun à tous les utilisateurs, alors c'est probablement une configuration sur le serveur qui est en cause.

L'important est la démarche de réflexion à acquérir. Il serait fastidieux et inutile de référencer toutes les erreurs probables, même si certaines sont très courantes.

6.4 Impacts d'un sinistre : détails par élément de type serveur

Nous avons déjà évoqué précédemment les défaillances matérielles plausibles et leurs solutions palliatives. Néanmoins, nous n'avons pas évoqués leurs champs d'action ni leurs solutions.

D'une manière générale, plus l'élément matériel est commun à l'ensemble du réseau, plus il est jugé vital et susceptible de bloquer le travail des individus.

Etudions le cas où chaque serveur tombe en panne, et les différentes répercussions.
Emettons le postulat que pour chaque situation, il n'y a aucune panne d'origine matérielle.

Si plusieurs serveurs (voir tous) sont arrêtés, il est préférable d'établir un ordre de redémarrage précautionneux. Dans l'idée, redémarrer les serveurs l'un après l'autre (attendre l'accès stabilisé de Windows) plutôt que tous en même temps. Normalement, cela ne change rien, mais cette précaution pourrait éviter une cause possible de dysfonctionnement - et donc un axe de réflexion.

Par exemple :
- serveur Pare-feu
- Serveurs DHCP – DNS – messagerie
- Serveur de fichiers
- Serveur d'impression et de mise à jour.

6.4.1 Les serveurs concernés :

SERVEUR N°	FONCTION en réseau	Impact en cas de défaillance	Solutions plausibles	Temps de réalisation de la solution
1	Serveur de données du service départemental	Impossibilité pour les 4 services départementaux extérieurs de se connecter.	Prendre le temps de réinstaller	3h00
2	Serveur de fichiers	Impossibilité de connexion en local aux fichiers utilisateur	Transférer et rendre disponible sur un autre serveur les fichiers (momentané) Réinstaller le serveur à l'origine	30 min 2h00
3	Serveur de messagerie Microsoft Exchange	Impossibilité de lire ses mails sous Outlook 2003	Réinstallation sur même serveur	1h30
	Serveur DHCP	Certaines stations de travail seront privées de connexion réseau	Réinstallation sur même serveur	1h00
	Serveur DNS	Impossibilité de se connecter aux pages WWW	Réinstallation sur même serveur	45 min
4	Serveur Microsoft Windows Server Update Services (WSUS)	Mise à jour logiciels impossible pour les stations de travail utilisateur	Réinstaller sur le même serveur	1h00
	Serveur d'impression	Impossibilité de d'effectuer une impression en réseau local, distant	Réinstaller sur le même serveur	45 min
5	Serveur proxy	Filtrage absent ; Pas d'internet ; Pas d'application de travail	Réinstaller sur le même serveur	1h00
	Serveur pare-feu	Pas de protection contre les attaques extérieures	Réinstaller sur le même serveur	30 min

7 (Ré)Installation des serveurs

D'emblée, une notion de précaution d'usage très importante est à mettre en place :

Chaque fois que nous faisons une manipulation qui a pour but de changer un état quelconque de fonctionnement, aussi simple soit-elle, prendre le temps de noter précisément ce que l'on a fait. Cela doit permettre (quand c'est possible) d'opérer une manipulation inverse. Cette précaution est à prendre en plus des éventuelles (voir conseillées) sauvegardes juste avant des manipulations suffisamment importantes.

7.1 Notes importantes

1) En cas de réinstallation, une première manipulation consiste à sauvegarder les événements précédents (fichier avec l'extension *.evt).
2) Avoir une solution facile pour le transport des données d'un ordinateur à un autre le cas échéant. Par exemple, un disque dur adéquat avec liaison USB.

3) Avoir facilement accès à tous les logiciels nécessaires à la réinstallation des serveurs :

    - Les O.S. (Operating System). Ex: Windows server 2003 Release 2 + service pack + les mises à jour
    - Les CD-Rom spécifiques aux composants du serveur (drivers, …)
    - Les logiciels spécifiques
    - Les logiciels secondaires pour les applications spéciales
        - CRASKI
        - Logiciels de formation continue
        - Applications sur certains dossiers partagés

4) Posséder du matériel en complément :
    - Carte réseau en PCI + drivers car problème de drivers avec les O.S. par rapport aux nouvelles cartes mères « récentes » avec une carte réseau intégrée.

Compter environ deux heures pour un serveur entièrement installé et complètement à jour.

N.B.
Selon la version à installer de l'O.S., il faut savoir utiliser la commande « adprep »
Celle-ci permet une cohabitation entre les générations de serveurs. Ex : Windows server 2000 vers Windows server 2003.

Mise à jour du schéma « Windows server 2003 » vers « Windows server 2003 R2» :
Utiliser le CD-Rom : \compnent\R2\adprep /adprep/forestprep

Attention :
« adprep/domaine_prep » n'a pas fonctionné dans notre cas la dernière fois.
« \i38\adprep/adprep/forestprep » renvoie une erreur de commande déjà exécutée avant. C'est le cas avec le logiciel Microsoft exchange 2003.

Bilan : utiliser tout de suite la dernière version disponible de Microsoft Windows server 2003. De plus, il est très important de respecter au mieux une homogénéité des versions de Microsoft Windows server installées sur les différents serveurs. Cela réduit les risques d'erreurs et d'incompatibilités.

7.2 Procédures de réinstallation selon le serveur : les grandes lignes

Qu'il s'agisse de réinstallation complète ou partielle, il est important de vérifier les accès utilisateurs encore possibles.

Surtout dans le cas d'une réparation partielle, il peut être important de procéder en dehors des heures de connexion des utilisateurs.

7.2.1 Panne du serveur N°1 :

Serveur avec : Boitier noir N°127 :

Rôle important mais non primordial
Prévenir les utilisateurs concernés des 4 services départementaux
Réinstaller le serveur puis les données de sauvegarde.

7.2.2 Panne du serveur N°2 :

Serveur avec : Boitier NEC EXPRESS 5800/120 Eh2 :

Le rôle de contrôleur de domaine continue d'être assuré par l'autre serveur
Le rôle de serveur DHCP doit être basculé sur le N°3,
Préconfigurer pour cela :
Interdire le serveur DHCP sur le serveur NEC EXPRESS 5800/120 Eh2
Autoriser le serveur DHCP du serveur NEC TM 800 – N° 111
Vérifier le fonctionnement (service DHCP activé)

La bascule du rôle de serveur de fichiers nécessite la restauration, sur l'autre serveur, de la dernière sauvegarde disponible.

Une information doit être faite auprès des usagers sur les modalités particulières d'accès à leurs documents de travail et les problèmes qu'elles posent (lecteurs réseaux déconnectés, publipostages, raccourcis vers applications locales…)

Si la solution de secours doit fonctionner sur une durée supérieure à deux jours, les raccourcis vers les applications locales devront être rétablis, soit par le personnel de l'informatique, soit par les utilisateurs.

7.2.3 Panne du serveur N°3 :

Serveur avec : Boitier NEC TM 800 – N° 111 :

Le rôle de contrôleur de domaine continue d'être assuré par l'autre serveur.

Le rôle de serveur DNS doit être basculé sur l'autre serveur, qui doit être configuré pour cela.

La bascule du rôle de serveur de messagerie nécessite l'installation d'Exchange et sa configuration sur l'autre serveur, puis la restauration de la banque d'information sur ce dernier.

Il faut ensuite intervenir sur chaque poste de travail pour y reconfigurer le client de messagerie.

Il faut mettre en place une solution de sauvegarde provisoire. Le rôle de contrôleur de domaine continue d'être assuré.

7.2.4 Panne du serveur N°4 :

Ce serveur n'a pas de rôle primordial.

Réinstaller ce serveur en prévenant les utilisateurs des conséquences occasionnées.

7.2.5 Panne du serveur N°5 :

La mise en place d'une machine configurée pour cela (Windows 2003 Server, IsaServer2006, installation de la configuration) est nécessaire.

Un serveur de secours pourrait éventuellement exister pour un remplacement immédiat.

Il conviendra de reparamétrer le serveur DHCP et d'intervenir sur les postes de travail pour lesquels le client ISA n'aurait pas été reconfiguré automatiquement.

7.3 Procédure de (ré) installation des serveurs : les détails

1) Installation de l'OS
2) Mise à jour de l'O.S.
3) Mise à jour logiciel des composants matériels
4) Installation des logiciels spécifiques et secondaires
5) Création du domaine :

Manipulation préalable : adéquation du service temps Windows
Permet de résoudre les problèmes de DHCP et de DNS. Problèmes liés aux messages d'erreur en rapport à « Kerberos ».

Menu démarrer → exécuter → mscd → puis écrire les commandes :
net time / sntp: ___.___.___.___ «exemple : ___.___.___.___= adresse du serveur temps »

6) Installer « Microsoft exchange server 2003 » puis effectuer les mises à jour
7) Transfert de toutes les données des utilisateurs depuis le serveur encore fonctionnel si c'est le cas. Attention, débrancher ce dernier du réseau pour éviter les interférences probables en cas d'utilisation d'au moins un fichier par un utilisateur pendant le transfert.
8) Autoriser les droits « administrateur » sur tout le dossier et (fichiers enfants) contenant les données des utilisateurs.
9) Copier les fichiers des utilisateurs sur le nouveau serveur de fichiers.

Une fois les serveurs installés :
Menu démarrer → poste de travail (clic droit) → propriété → utilisation à distance → bureau à distance → cocher : ☑ Autoriser les utilisateurs à se connecter à distance à cet ordinateur.

7.3.1 Création de l'active directory / des utilisateurs / des scripts

Cela concerne les serveurs qui sont contrôleurs de domaine. Une fois ceux-ci installés, nous pouvons procéder dans l'ordre suivant :

Création de l'Active Directory
Création des utilisateurs
Création des scripts

7.3.1.1 Création de l'Active Directory

Un tutoriel est présent en Annexe. Sinon, cf. d'autres tutoriels sur le serveur de fichiers.

7.3.1.2 Création d'une Unité d'Organisation (UO)

1) Créer une Unité d'Organisation (UO)
   Menu démarrer →Outils d'administration → Utilisateurs et ordinateurs Active Directory → _____.local → *Clic droit* → nouveau → Unité d'Organisation → *écrire le nom* puis cliquez *OK*
2) Création des sous Unité d'Organisation en fonction de l'organigramme fonctionnelle de la structure de la DRDJS de Besançon.
   A partir de l'UO créée → *Clic droit* → nouveau → Unité d'Organisation → *écrire le nom* puis cliquez *OK*

7.3.1.3 Création des utilisateurs

A partir de la sous UO créée → *Clic droit* → Nouveau → Utilisateur → …

7.3.1.4 Mise en place des scripts de connexion

Ouvrir le bloc note (Notepad), écrire les commandes ci-dessous, puis enregistrer le fichier avec l'extension *.bat)

net use M: \\...
net use N: \\...
net use O: \\...

Objectif : Chaque utilisateur en se connectant se voit attribuer au moins un lecteur réseau qui est en fait un accès spécifique aux répertoires partagés. Cela permet une plus grande souplesse de l'administrateur des dossiers partagés et une complète transparence pour l'utilisateur.

1) Clic droit sur l'Unité d'Organisation (ou la sous UO selon l'objectif) → Propriétés →Stratégie de groupe → Nouveau → Configuration d'utilisateur →Paramètre Windows → scripts (ouverture/fermeture de sessions)
2) Il faut donc accéder au fichier préalablement enregistré (*.bat)

7.4 Retour d'expériences : cas concrets, astuces et observations

Bien que cette partie soit construite de façon empirique, celle-ci peut parfois aider.

7.4.1 Active directory et réplication

Dans le cas ou nous devrions restaurer un serveur par une image intégrale du disque, il faut évaluer l'impact sur les autres serveurs. Ce cas de figure est d'autant plus vrai, si l'image disque est antérieure à des modifications notables.

L'Active Directory se réplique entre les serveurs. Il faut donc restaurer la banque d'information la plus récente possible et bien prendre en compte qu'une image disque intégrale est antérieure (en général) à la banque d'information.

8 Microsoft Outlook 2003

8.1.1 Les adresses de la messagerie

En cas de changement de nom de domaine :

Les adresses de messagerie en local seront erronées.
Exemple : passage de « _____.local » à « _____.local »
Solution : refaire la liste de diffusion (groupe de destinataires). Attention de ne pas sauvegarder et copier le fichier caché « outlook.nk2 » pour chaque utilisateur. Il est fortement conseillé d'apprendre aux utilisateurs à créer des contacts et des listes de diffusion.

8.1.2 Fonction de calendrier (Le calendrier partagé)

1) Sur chaque station de travail, permettre une autorisation de relecture de chaque calendrier des utilisateurs.
2) Une fois seulement que toutes les stations de travail sont bonnes, permettre d'afficher dès que possible les calendriers de toutes les personnes.
3) Il faut commencer dans l'ordre alphabétique pour chaque contact car Outlook ne permet pas de choisir autrement qu'un à un les contacts et n'autorise pas de classement par ordre alphabétique. (dommage ☺ !)
4) En premier, traiter la station de travail du poste de l'accueil téléphonique.
5) Démarche : bouton « calendrier » → fichier → ouvrir →fichier d'un autre utilisateur

Ci-dessous, la procédure mise en place pour intervenir sur chaque poste utilisateur. Celle-ci est à effectuer une fois l'installation des serveurs et des programmes adéquats complètement finie.

Changement de domaine - Procédure utilisateurs

(Les mots en *italiques* expriment ce qui change en fonction de la situation. Exemple : un *nom_d'utilisateur)*

Nous venons de créer un nouveau domaine : Il faut se rattacher à ce nouveau domaine.

Recommandations :

- Se munir du CD d'OUTLOOK pour certains postes.
- Se munir des manipulations spéciales pour les postes utilisant des logiciels spécifiques
- Se munir des mots de passe utilisateurs (sessions Windows, application de messagerie et autres)

Accorder les droits d'accès utilisateurs de manière égale à celui de l'administrateur permet de raccourcir le temps de certaines manipulations. Par contre, nous avons rencontré des soucis après le retrait de ceux-ci : obligation de remettre les droits d'accès en contrôle total aux éléments du dossier utilisateur et réinstallation sur chaque poste des drivers d'impression. Bilan : 20 minutes par poste.

- Certains ordinateurs lents à démarrer nécessitent le débranchement du câble réseau RJ45

ETAPE 1 : Sauvegarder le contenu des répertoires et fichiers personnels

Depuis l'explorateur Windows : menu « Outils » →Options des dossiers → Affichage → cocher « afficher les fichiers et dossiers cachés » → Ok

Créer un dossier à la racine du disque système : « C:\SVG-*Année-mois-jour* »

Se rendre au dossier utilisateur : « C:\Documents and Settings\
« *identifiant_utilisateur.domaine* »
Copier les dossiers suivants : « Bureau », « favoris », « mes documents » dans le répertoire de sauvegarde

Se rendre au dossier utilisateur
« C:\Documents and Settings\ *identifiant_utilisateur.domaine* \Application Data\Microsoft\Outlook »
Copier le fichier « outlook.nk2 » du répertoire Vers « C:\SVG-*Année-mois-jour* »

ETAPE 2 : Sauvegarder la messagerie OUTLOOK 2003

Démarrer le poste client avec les identifiants habituels (sessions utilisateurs).
Exécuter Microsoft OUTLOOK 2003

Onglet « fichier » → Importer et exporter → exporter des données vers un fichier →
(En cas de demande d'identification, utiliser les données de la session en cours)
Fichiers de fichiers personnels (:pst) → Sélectionner boîte aux lettres utilisateur et cocher « inclure les sous-dossiers» → Suivant → Terminer →

Sauvegarder à la racine dans un répertoire « C:\SVG-*Année-mois-jour* » →(créer un nouveau dossier : clic droit dans la fenêtre →nouveau → dossier → …) →cocher « aucun cryptage »

ETAPE 3 : modifier le domaine

Redémarrer l'ordinateur et s'identifier en tant que :

Utilisateur = Administrateur Mot de passe =
Se connecter à : … (cet ordinateur)

Menu démarrer, propriétés du poste de travail (clic droit → Propriétés)
Onglet « Nom de l'ordinateur » → modifier → domaine : « _____.local »

Sessions = Administrateur mot de passe administrateur =

A l'invite « redémarrer maintenant, répondre « NON » → puis sur les fenêtres ouvertes : Ok → Ok

Menu démarrer →Exécuter →écrire « cmd » → ipconfig /release → « Entrée » → ipconfig /renex → « Entrée »

ETAPE 4 : modifier les droits d'accès du dossier de sauvegarde

Sélectionner le répertoire « C:\SVG-Année-mois-jour » → « Propriétés (clic droit souris), onglet « sécurité » →

Ajouter → emplacement (sessions Administrateur et mot de passe administrateur) →
Avancé →rechercher le « *nom de l'utilisateur* » → … →cocher « contrôle total » →
Paramètres avancés → Cocher « remplacer les entrées … objets enfants » →
Redémarrer l'ordinateur

ETAPE 5 : Connexion au serveur PROXY

Dans la barre des taches (en bas à droite) chercher « server ISA » → configurer (clic droit)

ou partir du menu démarrer : « gestion du client de pare-feu Microsoft »

Onglet « paramètres » → serveur ISA sélectionné manuellement : ……

Bouton « Tester le serveur » et vérifier message et si c'est bon → Ok

ETAPE 6 : paramétrer OUTLOOK 2003 : fonction messagerie (courrier)

Exécuter l'application Outlook 2003 → Suivant → Suivant → cocher « Microsoft exchange Serveur » → Suivant → _____._____._____._____ ou « le_nom_du_serveur » et *nom_utilisateur* = celui de cette connexion
→ et utiliser Vérification du → Suivant → Terminer → …→Onglet « outils » → compte de messagerie → ajouter un nouveau compte de messagerie →pop3 → Suivant
Adresse de messagerie =
Serveur de courrier entrant (Pop3) :
Serveur de courrier sortant (SMTP) :

Nom d'utilisateur et mot de passe : utiliser les identifiants du ministère →
Tester les paramètres du et vérifier que tout est bon.

Paramètres supplémentaires → compte de messagerie = « Messagerie JS » (par exemple) → Onglet « serveur sortant » → cocher « mon serveur sortant … » → Ok → Suivant → Terminer

Dans la barre d'outils en haut utiliser « envoyer/recevoir » pour vérifier que tout est bon
Dans la barre de menu : « outils » → options → messagerie → Envoyer/recevoir
Cocher « planifier un envoi / une réception auto … » et régler le bon temps : 15 min (exemple) → Fermer

Menu « fichier » → importer et exporter → importer à partir d'un autre programme ou fichier → Ok Sélectionner « fichiers de dossiers personnels (.pst) » → Suivant → Suivant → Parcourir et sélectionner le fichier du répertoire « C:\SVG-Année-mois-jour » → Suivant → Terminer

En cas de changement de nom de domaine :

Les adresses de messagerie en local seront erronées.
Exemple : passage de « _____.local » à « _____.local »
Solution : refaire la liste de diffusion (groupe de destinataires). Attention de ne pas sauvegarder et copier le fichier caché « outlook.nk2 » pour chaque utilisateur. Il est fortement conseillé d'apprendre aux utilisateurs à créer des contacts et des listes de diffusion.

Néanmoins il est possible de :

A l'aide l'explorateur, déplacer le fichier « outlook.nk2 » du répertoire « C:\SVG-Année-mois-jour »
Vers C:\Documents and Settings\identifiant_utilisateur.domaine\Application Data\Microsoft\Outlook

ETAPE 7 : Paramétrer OUTLOOK 2003 : fonction calendrier

1) Sur chaque station de travail, permettre une autorisation de relecture de chaque calendrier des utilisateurs.

Fonction « calendrier » (bas / gauche)→partager mon calendrier
Concernant les autorisations d'accès :
compte « anonyme » : supprimer compte « par défaut » : mettre le niveau d'autorisation à « relecteur »

2) Une fois seulement que toutes les stations de travail sont bonnes, permettre d'afficher dès que possible les calendriers de toutes les personnes.

3) Il faut commencer dans l'ordre alphabétique pour chaque contact car Outlook ne permet pas de choisir autrement qu'un à un les contacts et n'autorise pas de classement par ordre alphabétique. (dommage ☺ !)

4) En premier, traiter la station de travail du poste de l'accueil téléphonique.

5) Démarche : bouton « calendrier » → fichier → ouvrir →fichier d'un autre utilisateur

Ci-dessous, la procédure mise en place pour intervenir sur chaque poste utilisateur. Celle-ci est à effectuer une fois l'installation des serveurs et des programmes adéquats complètement finie.

ETAPE 8 : paramétrer l'impression

Menu démarrer →imprimante et télécopieurs → (faire un clic droit sur la bonne imprimante) et définir comme imprimante par défaut →fermer la fenêtre.

ETAPE 9 : Penser à …

Depuis l'explorateur Windows : menu « Outils » →Options des dossiers → Affichage → cocher « ne pas afficher les fichiers et dossiers cachés» → Ok

ETAPE 10 : Optimiser les accès aux données du disque dur (non obligatoire)

Fermer la session, ouvrir en sessions Administrateur et faire une défragmentation du disque C:\

ARRETER L'ORDINATEUR

ETAPE 11 : Manipulation sur les serveurs

Enlever les utilisateurs du domaine des administrateurs selon la méthode employée.

9 Le service d'impression

En cas de changement de domaine, le service d'impression est à mettre en action seulement après avoir effectué la procédure utilisateur de changement de domaine.

La remise en fonctionnement du service d'impression est faite à partir de la sauvegarde du serveur d'impression.

Il faut prévoir les CD-Rom permettant de réinstaller les imprimantes réseaux.

Il faut aussi prévoir les CD-Rom d'installations pour les quelques personnes ayant en plus une ou plusieurs imprimantes locales partagées ou non.

9.1 Mise en place d'un serveur d'impression

En cas de reprise différente, il est conseillé de suivre les indications du § 9.2.2 du référentiel technique pour les systèmes d'information et de télécommunication (version 2.1 – juillet 2008)

Le serveur d'impression permet de partager trois imprimantes et deux copieurs multifonctions.

Modèle de matériel	Drivers utilisé	Adresse IP	Spécificité
CANON IR 5055/5065	PCL 5e		Copieur multifonctions situé au rez-de-chaussée
CANON IR 5055/5065	PCL 5e		Copieur multifonctions situé à l'étage 1
HP LASER JET P4010_P4510 Series	PCL 6		Imprimante située au rez-de-chaussée
HP LASER JET 5100	PCL 5e		Imprimante située à l'étage 1
HP Color laser Jet 4700 PCL6	PCL 6		Imprimante couleur située à l'étage

9.2 Réglages des copieurs multifonctions : paramétrage du scanner

La fonction de scanner offre différentes possibilités, dont celle de scanner au format PDF des documents dans un répertoire de notre choix - par exemple, au nom de l'utilisateur.

1) Touche « ✶ » (avec un contour ressemblant à une tête) (près du pavé numérique)
2) Réglage du carnet d'adresse
3) Mémoriser l'adresse →
4) Mémoriser nouvelle adresse
5) Fichier
6) Nom : « mon_nom » (mon_nom = nom du dossier dans le répertoire du serveur)
7) Protocol : « Windows (SMB) »
8) Nom d'hôtes « \\...
9) Chemin du dossier : « \commun\scanner\mon_nom »
10) Utilisateur : « scanner »
11) Mot de passe : « scanner »

10 La téléphonie

En cas de problèmes de téléphonie, s'adresser à la société de service de sous-traitance. Voir les informations dans le tableau au début de ce PRAI.

Connaître aussi la date de fin de garantie du matériel et du service associé est très utile.

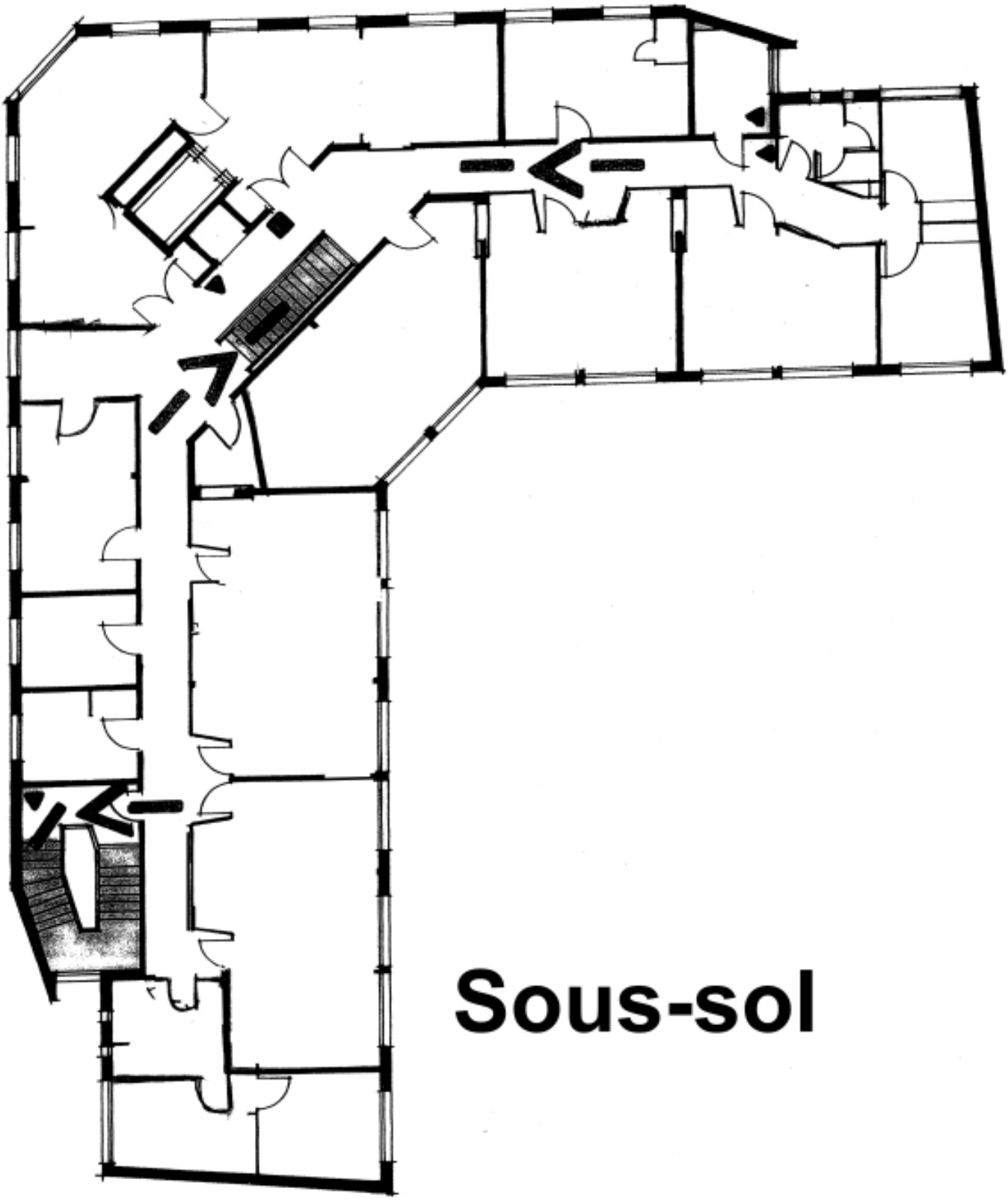
Tables des matières

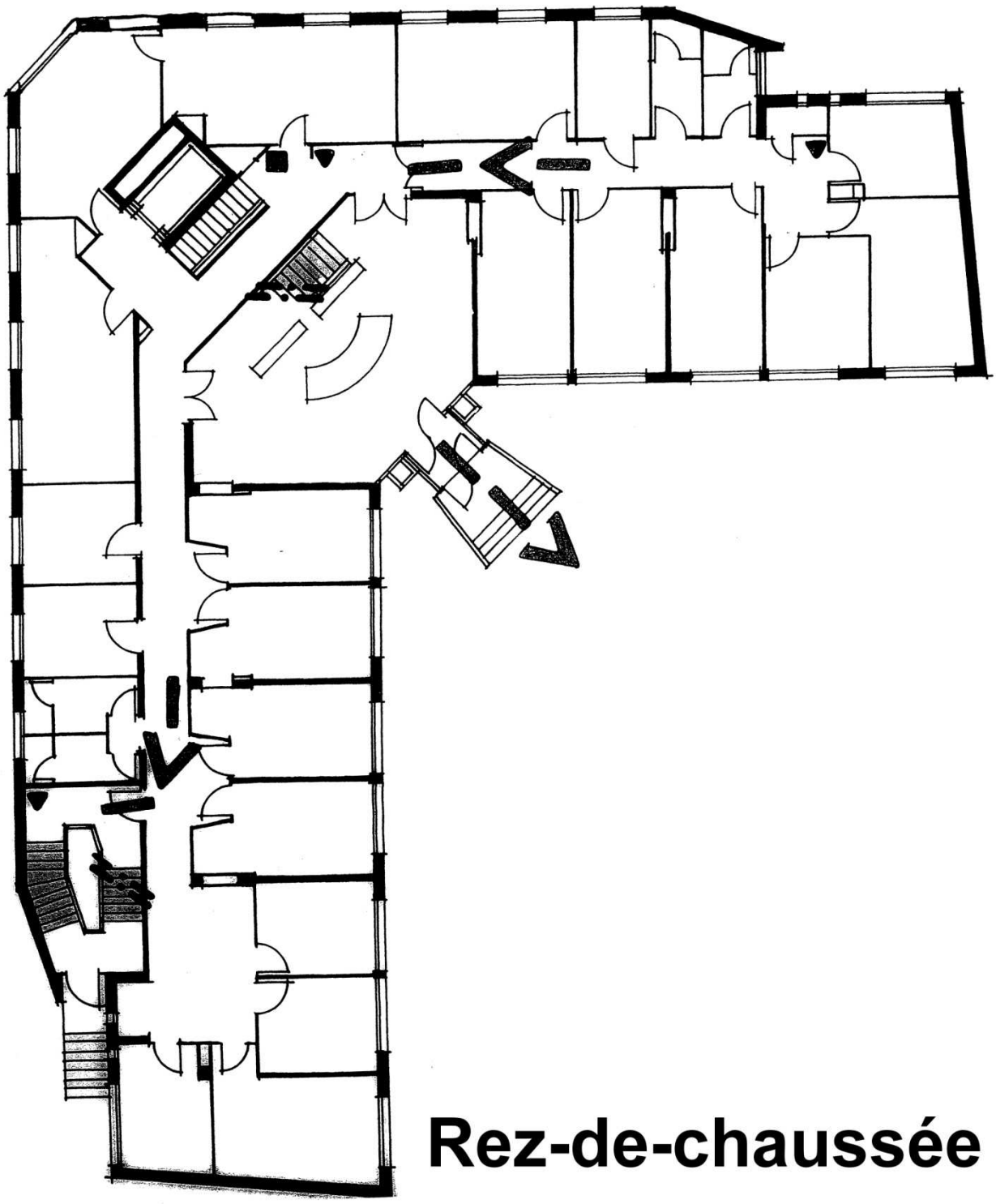
ANNEXES

ANNEXE N° 1 :

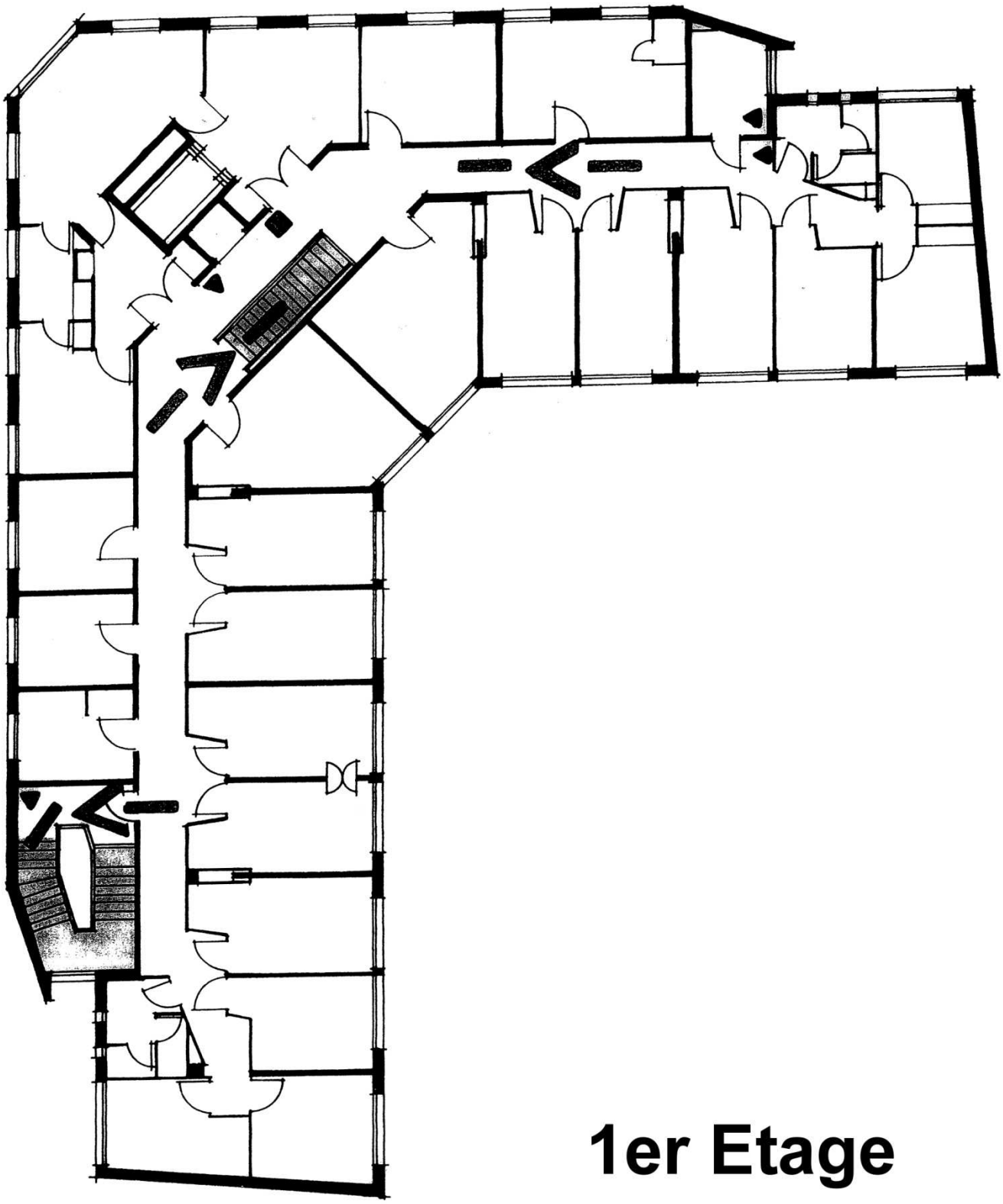
Plan des trois étages. Bâtiment DRDJS

ANNEXE 1 : Plan des trois étages. Bâtiment DRDJS





Rez-de-chaussée



1er Etage

MOT CLES

INFORMATIQUE - RESEAU - PLAN - REPRISE - SINISTRE - CONTINUITE - ACTIVITE - WINDOWS - SERVEUR

Olivier HOUBLOUP

Technicien Supérieur en Réseaux Informatiques et Télécommunications d'Entreprise

RAPPORT DE STAGE
24/10/2008 au 24/01/2009

RESUME

Ce stage s'est déroulé dans un service déconcentré de l'Etat français : la Direction Régionale et Départementale de la Jeunesse et des Sports de Franche-Comté (DRDJS). L'objectif principal a été d'établir un Plan de Reprise d'Activité Informatique (PRAI) après sinistre. Un PRAI est un ensemble de mesures propres à une structure qui doit s'adapter constamment en fonction de l'évolution de l'entreprise. Ce domaine est vaste et génère diverses difficultés. Après présentation de ce service, j'énonce le déroulement et l'analyse d'une première réflexion de PRAI, notamment sur les neuf premières phases d'élaboration, de mise en place des procédures et de tests. A la suite d'un incident technique survenu au niveau de l'Active Directory des serveurs sous Microsoft Windows server 2003, mon maître de stage et moi avons été contraints de réaliser directement un ensemble de procédures permettant de revenir à un niveau normal de production. En annexe, le PRAI remis à l'entreprise contient également l'intégralité de notre démarche de (re)construction d'un réseau complet comprenant divers serveurs (de fichiers, DNS, DHCP, de messagerie, de pare-feu, d'impression…). Ce dossier synthétise aussi mon apport technique et ma réflexion sur les huit semaines de vécu dans un milieu professionnel, vu comme une entreprise. J'ai pu vivre l'interaction entre connaissances théoriques et réalités du terrain, partage des idées pour réparer, problèmes techniques et incidence sur le travail quotidien d'utilisateurs dépendant de la qualité de notre intervention. J'ai apprécié les aspects d'interactivité, de synergie et de contrainte d'un travail urgent et important pour chacun, qui attend une aide rapide et efficace, pour que tout redémarre afin que la structure humaine et technique reprenne son activité normale.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA SANTÉ, DE LA JEUNESSE, DES SPORTS ET DE LA VIE ASSOCIATIVE
SECRÉTARIAT D'ÉTAT AUX SPORTS, A LA JEUNESSE ET A LA VIE ASSOCIATIVE

Direction Régionale et Départementale de la Jeunesse et des Sports

27 Rue Alfred-Sancey
25000 Besançon

afpa
gagnez en compétences

19 Avenue de l'observatoire
25000 Besançon