

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen,Vincent Vandaele,Grégory Orsoni
Année : 2014 -2015		



Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen,Vincent Vandaele,Grégory Orsoni
Année : 2014 -2015		

SOMMAIRE

I Remise en situation.....	3
II Nomenclature.....	3
III Masterisation.....	4-8
IV Procédure en cas de panne.....	9-11
V Charte sur l'utilisation du matériel informatique.....	12-14
VI Conclusion.....	15
VII Annexe.....	.

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

I. Remise en situation

L'entreprise GSB a acheté 480 machines pour ses intervenants qui doivent remplir leur mission sur le terrain. Les visiteurs étant habitués à l'environnement Windows 7, leurs machines ont été dotées de ce système d'exploitation. L'équipement satisfait à des critères spécifiques répondant aux besoins des visiteurs médicaux. Nous nous occuperons du déploiement de ces dernières ainsi que du parc informatique.

II. Nomenclature

Désignation des équipements : **GPTVM_001**

- **G** : Nom de l'entreprise résumé à sa première lettre
- **PT** : Désigne le type. PT pour ordinateur portable, PC pour ordinateur fixe
- **VM** : Désignation de l'utilisateur (Visiteur Médicale)
- **001** : Numéro incrémenté de l'équipement

Cette désignation a pour but de distinguer les ordinateurs entre eux, et aussi de répertorier efficacement le parc informatique.

Ici, nous pouvons savoir quel est le type d'équipement (acheté par GSB ou personnel dans le cadre d'un rajout budgétaire auprès de l'entreprise par exemple), et la fonction de l'utilisateur.

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

Toutes les informations concernant les utilisateurs seront recensées et gérées au sein d'un tableau [Excel](#). Ainsi, à partir du numéro propre à un utilisateur, on effectuera une recherche pour connaître son nom, prénom, numéro de département, logiciels, système d'exploitation, adresse IP (DHCP ou fixe), adresse email, type de Pack Office, antivirus, VPN, sauvegardes...

En cas de départ du visiteur, le PC sera soit envoyé au Siège pour l'intégration d'une image système propre et sera remis à un nouveau visiteur; soit l'administrateur du site s'occupera de l'intégration de la nouvelle image.

Dans le cas d'une mutation, le visiteur pourra garder sa machine. Cependant, les informations concernant le visiteur seront modifiées au niveau du tableau Excel pour mettre à jour le nouveau département.

III. Masterisation

A.Définition

Dans le cadre d'un déploiement de parc informatique, il serait fastidieux et coûteux en terme de productivité et disponibilité d'installer le système d'exploitation, configurer les paramètres réseaux, et installer les logiciels métiers poste par poste.

L'application d'une solution de déploiement d'image disque ou "ghost" serait donc la solution à ces différents problèmes.

On utilisera donc un master qui sera une image qui bénéficiera d'un système propre et le plus optimisé possible.

B.Solutions

A.Disque dur

La première solution consiste à créer une image disque d'un système et de le déployer manuellement grâce à un disque dur. A noter que cette solution sera plus adaptée pour un déploiement des systèmes d'exploitations à très petite échelle car il faudra effectuer l'opération poste par poste.

Avantages : Rapide à mettre en place.

Inconvénients : Pas adapté pour le déploiement d'un grand parc informatique.

B. Type de déploiement avec serveur

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

Il existe différents moyens de déployer des images " ghost " au sein d'un réseau informatique

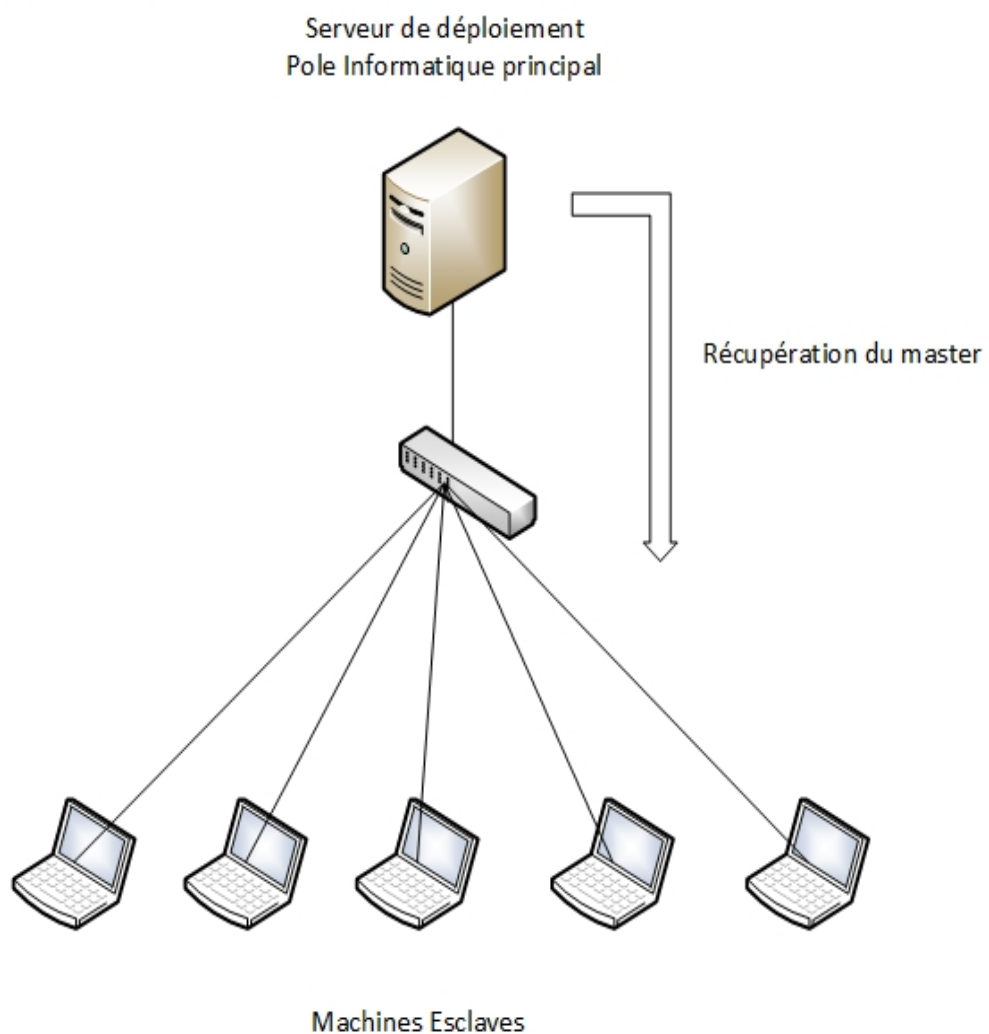
- . Le déploiement en local
- . Le déploiement à distance

Il faut distinguer donc deux choses, la première est la machine dites " Master " ou " Maître ainsi que les machines " Esclave "

Dans la première méthode, le déploiement s'effectue au sein du réseau local de l'entreprise, c'est à dire que toutes les machines hôtes au futur système d'exploitation seront esclave du serveur maître que l'on peut définir également de serveur de déploiement.

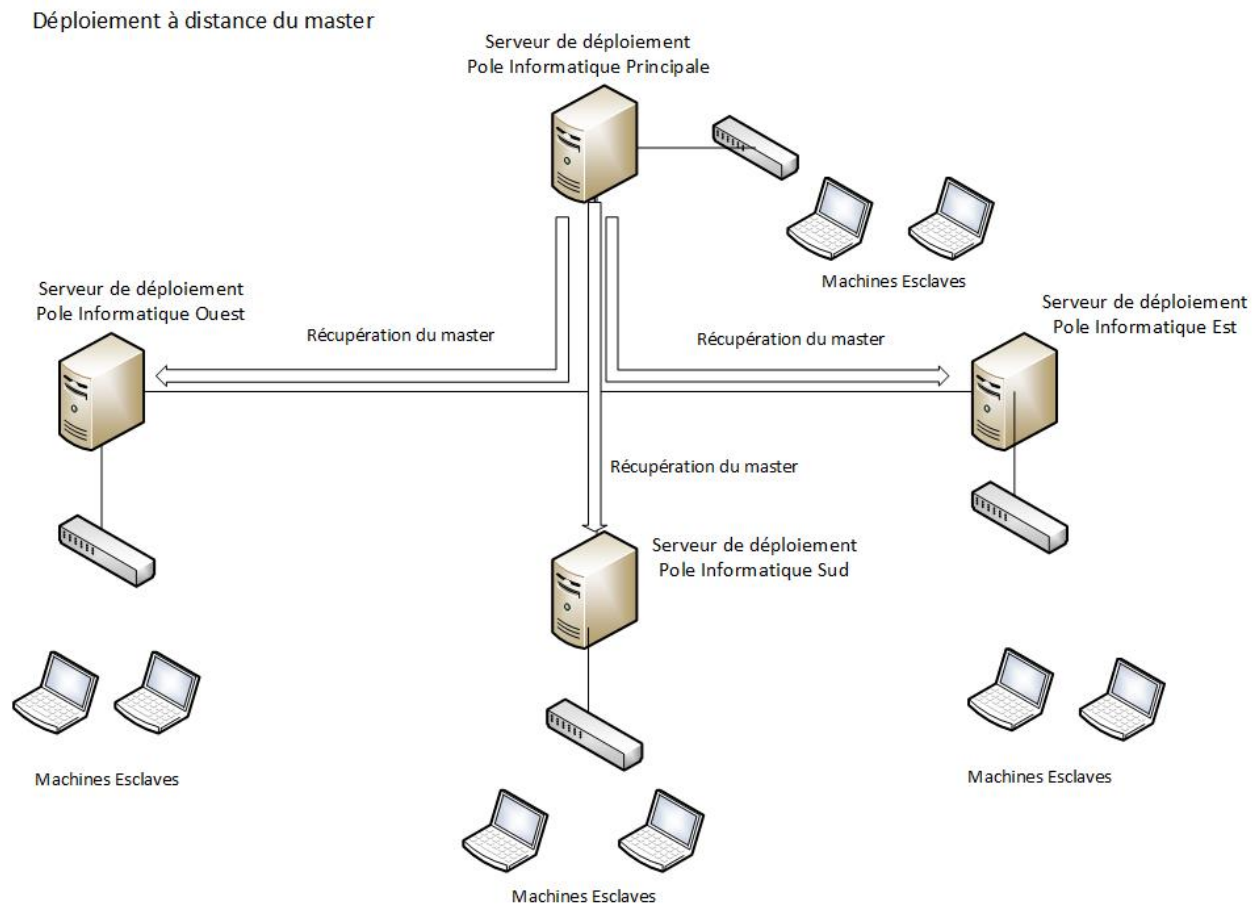
Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen,Vincent Vandaele,Grégory Orsoni
Année : 2014 -2015		

Déploiement en locale du master



Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen,Vincent Vandaele,Grégory Orsoni
Année : 2014 -2015		

La seconde méthode qui elle est basée sur l'éloignement des pôles informatiques qui requiert une machine dans chaque pôle qui fera office de serveur de déploiement pour les machines clientes. Cela évitera de saturer le réseau entre les différents pôles et permettra de répartir au mieux les tâches entre les différents administrateurs réseaux et systèmes.



Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen,Vincent Vandaele,Grégory Orsoni
Année : 2014 -2015		

On utilisera le PxE : Preeboot Exécution Environment pour récupérer les ghost sur le serveur de déploiement, un serveur DHCP, TFTP devra être au préalable installer.

Exemple de boot sur PxE :

```
CLIENT MAC ADDR: 00 24 8C 3C 2C 8C GUID: 002C63CA-5DFA-DD11-AA8A-00248C3C2C8C
CLIENT IP: 10.9.129.102 MASK: 255.255.248.0 DHCP IP: 10.9.129.100

PXELINUX 3.30 2006-09-18 Copyright (C) 1994-2005 H. Peter Anvin
UNDI data segment at: 00094750
UNDI data segment size: 87B0
UNDI code segment at: 0009CF00
UNDI code segment size: 28DA
PXE entry point found (we hope) at 9CF0:0106
My IP address seems to be 0A098166 10.9.129.102
ip=10.9.129.102:10.9.129.100:0.0.0.0:255.255.248.0
TFTP prefix:
Trying to load: pxelinux.cfg/01-00-24-8c-3c-2c-8c
Trying to load: pxelinux.cfg/0A098166
Trying to load: pxelinux.cfg/0A09816
Trying to load: pxelinux.cfg/0A0981
Trying to load: pxelinux.cfg/0A098
Trying to load: pxelinux.cfg/0A09
Trying to load: pxelinux.cfg/0A0
Trying to load: pxelinux.cfg/0A
Trying to load: pxelinux.cfg/0
Trying to load: pxelinux.cfg/default
-
```


Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen,Vincent Vandaele,Grégory Orsoni
Année : 2014 -2015		



C. Comparatif Logiciels

Les solutions retenus seront la solution Libre Clonezilla et le logiciel Symantec Norton Ghost.

Symantec Norton Ghost	Clonezilla
<ul style="list-style-type: none"> + Choix entre l'utilisation de boot via PXE + Déploiement manuels, automatiques, initiés par l'utilisateur ou planifiés. + Gestion du multicast + Support technique - Nécessite l'utilisation d'un serveur de déploiement - Solution payante 	<ul style="list-style-type: none"> + Solution gratuite + Déploiement d'une image sur plusieurs supports à la fois + Utilisation d'un serveur ou non + Déploiement via PXE/Live CD - Le RAID n'est pas supporté - Configuration peu intuitive - Pas de support technique

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

IV.Procédure de mise en place

Etape :	Vérification
Activer le PxE sur le bios	Vérifier qu'il récupère une adresse IP
Mettre le PxE en priorité au boot	Le PxE doit être en haut de la liste
Sur le PxE, lancer norton ghost	Iso bien récupéré et installé

V.Procédure panne dysfonctionnement

Charte de remise en cas de panne, dysfonctionnement ou fin de vie :

En cas de panne détectée par l'utilisateur (problèmes matériels liés à la machine portable), l'équipement devra être déclaré et être remis au Centre Régional. Ces derniers s'occuperont d'envoyer la machine au siège de Paris afin qu'il puisse être examiné et réparé dans les meilleurs délais ou remplacé.

Procédure en cas de panne :

Étape 1 : Signaler tout dysfonctionnement

Par mail ou téléphone au service informatique maintenance pour lancer la procédure. Les détails du problème y seront précisés : panne, vol, casse.

Étape 2 Remise de l'ordinateur endommagé

L'ordinateur doit être retourné en l'état avec tous les accessoires fournis. Une signature sera obligatoire afin d'effectuer la remise du poste.

Étape 3 Mise à disposition d'un ordinateur de remplacement

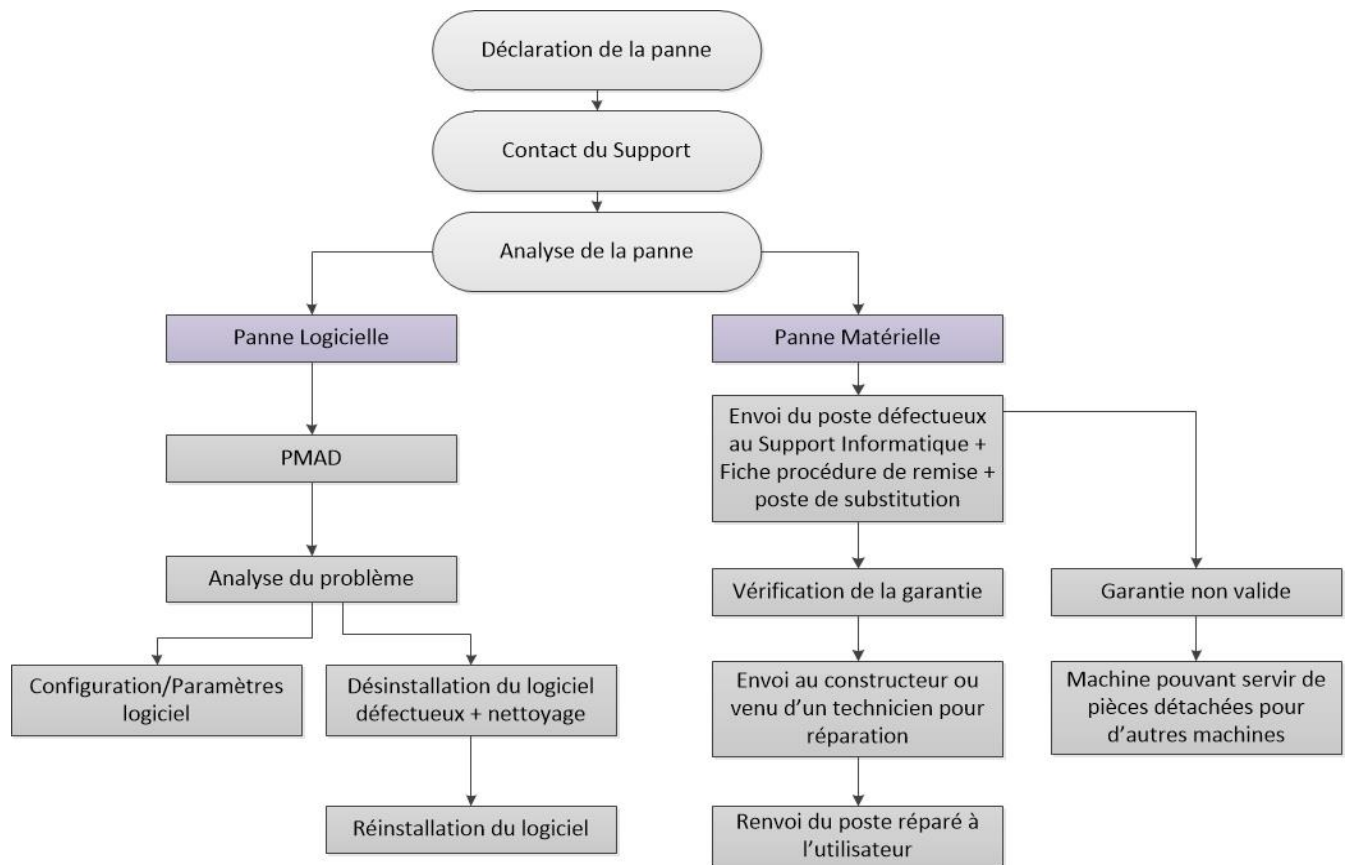
Un poste de substitution sera immédiatement remis pour que le visiteur ne soit pas impacté dans son travail.

Étape 4 Retour du PC au bout de 2 ans

Les ordinateurs seront tous rappelés de manière cyclique au bout de 2 ans, à leur fin de garantie, pour être remplacé selon un roulement.

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen,Vincent Vandaele,Grégory Orsoni
Année : 2014 -2015		

Schéma de solution en cas de panne



Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

Procédure pour distinguer une panne et choisir le moyen approprié	
Date : 10/01/2015	Version : 1.0
Nom : tableau_procedure_panne.csv	Auteur : Service
Pré-requis	Avoir analysé la panne (logiciel ou matériel)
Procédure	Déclarer le sinistre par téléphone ou via mail
Vérification	
Post-opération	Remplissage d'une fiche suivi Aide en ligne pour problème mineur

Procédure de reconditionnement	
Date : 10/01/2015	Version : 1.0
Nom : tableau_procedure_reconditionnement.csv	Auteur : Service
Pré-requis	Récupération d'une machine endommagé
Procédure	Dump en iso le disque dur de la machine endommagé ou reprendre une sauvegarde antérieure
Vérification	
Post-opération	Réinstallation de la sauvegarde sur la nouvelle machine

Numéro de série	Personne	Type de problème	Solution	état
GPTVM_001	Brian Rainbaud	Ralentissement	Dépannage en ligne	Fini
GPTVM_050	Mickael Val	Écran fissure	Remplacement	En Cours

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

Charte sur l'utilisation du matériel informatique

1.Domaine d'application :

Les règles et obligations définies dans cette charte s'appliquent à tout utilisateur des moyens informatiques de l'établissement ainsi que des ressources extérieures accessibles via les réseaux informatiques.

Les ressources informatiques de l'entreprise sont constituées de l'ensemble des outils informatique des outils informatiques : logiciels, serveurs, micro-ordinateurs ainsi que des services destinés à un professionnel : messagerie, connexion internet.

Tout salarié et collaborateur est autorisé à utiliser les ressources informatiques de la société.

2.Règle de bon usage du matériel :

L'utilisation des moyens informatiques mis à disposition est strictement réservée aux seuls besoins de l'entreprise. Tous utilisateur est tenu de respecter le bon usage des ressources communes mises à sa disposition par l'établissement, espaces disques, bande passante réseau , imprimantes, etc. et de respecter les consignes des administrateurs systèmes. Tout utilisateur est tenu de faire preuve de la plus stricte correction à l'égard de ses interlocuteur dans les échanges électronique. Nul ne peut s'exprimer au nom de l'établissement ou l'engager sans y être dûment autorisé de par ses fonctions ou de façon explicite.

3.Gestion de la sécurité :

Chaque collaborateur est responsable de l'usage qu'il fait des ressources informatiques de la société.

Les recommandations fournies par la direction des systèmes d'informations sont les suivantes :

- L'utilisateur doit choisir un mot de passe en mélangeant des caractère alphanumérique et des chiffres ainsi qu'une majuscule.
- Le mot de passe doit être au minimum de 8 caractères.
- Si possible l'utilisateur est prié de changer régulièrement de mot de passe afin d'éviter afin d'éviter d'éventuelle vol.
- Les mots de passe sont personnels est ne doivent pas être communiqués à un tiers.
- Les espaces de stockage des postes de travail et des serveurs doivent être contrôlés par des antivirus.
- L'utilisateur ne doit pas accéder à des ressources (site internet ou autres) qui n'ont aucun rapport avec son activité professionnelle au sein de l'entreprise.

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

- Il doit respecter l'ensemble des lois d'ordre pénal et civil en vigueur, notamment celle relatives :
 - aux publications à caractère raciste, pédophile, injurieux, diffamatoire.
 - au harcèlement sexuel ou moral.
 - à l'utilisation des logiciels.
 - au droit d'auteur.
- Les collaborateurs sont tenus de respecter l'ensemble des directives fournies par les administrateurs système et les responsables informatiques.
- Dans le cadre de son activité professionnelle, le collaborateur doit garder une attention particulière à l'utilisation de sa messagerie. Il doit signaler tout comportement suspect à la direction du système d'information qui prendra les décisions nécessaires.

4. Cas de vol ou dégradation du matériel :

L'utilisation des postes informatiques, personnels comme publics, est sous l'unique et entière responsabilité de l'utilisateur.

En cas de dégradation du matériel mis à la disposition de l'utilisateur, ce dernier engage sa responsabilité personnelle et encourt les sanctions prévues au règlement des espaces ouverts au public auquel il est soumis (exclusion et/ou poursuite judiciaire).

En cas de vol ou de dégradation du matériel mis à disposition de l'utilisateur par GSB, ce dernier est alors tenu d'informer le responsable informatique de son service qui sera libre d'appliquer les sanctions proportionnelles à la faute et devra engager les procédures prévues à cet effet.

5. Règles et sanction :

Les interdictions à respecter par l'utilisateur :

- L'utilisateur ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues à cet effet ou sans y être autorisé par les responsables habilités.
- Il ne doit pas tenter de lire, modifier, déposer ou détruire des données sur un serveur autrement que par les dispositions prévues à cet effet ou sans y être autorisé par les responsables habilités.
- Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède.
- Il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers.
- Il ne doit pas connecter un matériel sur le réseau sans autorisation.
- Il ne doit pas mettre à la disposition de personnes non autorisées un accès aux ressources informatiques de GSB.

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

- Il ne doit pas, par quelque moyen que ce soit, proposer ou rendre accessible aux tiers des informations confidentielles ou contraires à la législation en vigueur.
- Il ne doit pas télécharger ou diffuser des données en violation des lois protégeant les droit d'auteur, quel que soit le domaine (écrits, images, logiciels, bases de données, ..).
- Il ne doit pas contourner les restrictions d'utilisation d'un logiciel.

Le non respect des règles énoncé si- dessus peut entraîner les sanctions de la nature suivante :

- Disciplinaire : Les responsables fonctionnels on pleine autorité pour prendre les mesures conservatoires nécessaire en cas de manquement à la présente charte et interdire aux utilisateurs fautifs l'accès au moyens informatiques et au réseau.
- Pénale : L'évolution des techniques électroniques et informatiques a conduit le législateur à définir des sanctions pénales d'une grande sévérité à la mesure du risque que peut faire courir aux libertés individuelles l'usage incontrôlé des fichiers ou des traitement informatiques.

6. Usage personnel :

L'utilisation des ressources informatiques de GSB pour motif personnel ne doit pas être susceptible d'amoindrir les conditions d'accès professionnel à ces ressources. Elle est autorisée dans la mesure où elle ne porte pas atteinte au bon fonctionnement du service, et ne met pas en cause la productivité de l'entreprise. L'ensemble des règles de cette charte s'applique également pour ce type d'utilisation. Le devoir de réserve incombant à tout fonctionnaire doit être respecté.

La messagerie électronique peut également être utilisée pour un usage personnel, dans les limites imposées par le bon fonctionnement du service.

Conformément aux principes de droit, il est considéré qu'un message envoyé ou reçu depuis un poste de travail mis à la disposition de l'utilisateur par GSB revêt un caractère professionne

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

Conclusion

Au terme de notre étude, notre choix de masterisation se portera vers Norton Ghost de Symantec. Le déploiement sera réparti entre les différents pôles informatique de GSB via le réseau. Les postes auront pour n et s'incrémenteront en fonction du nombres d'utilisateurs. En cas de panne de l'équipement informatique, il sera nécessaire de suivre la procédure adéquate.

Pour finir, une charte informatique concernant l'utilisation du matériel a été rédigée au sein de GSB afin de veiller au bon fonctionnement de l'équipement, ainsi que déterminer la responsabilité de chaque utilisateur.

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

Signature :

Compte-rendu des réunions

Objet : Planification, répartition des tâches et avancement

Lieu : Groupe Ecole Pratique et travail personnel chez soi

Support : Google Drive

Sujet : Déploiement et maintenance du parc informatique

Démarche :

- Communication
- Répartition des tâches
- Travail et aide entre les différentes tâches
- Regroupement des travaux terminés
- Vérification et dernières modifications avant la création du dossier final

A chaque séance, nous nous sommes regroupés afin de faire le point sur l'avancement des différentes tâches qui nous ont été confiés, sur l'avancement global du projet et ainsi terminer par l'assemblage des différents travaux et créer le dossier final.

La répartition des tâches a été faite de la manière suivante :

Vincent Vandaele

- Etude de la maîtrise

Grégory Orsoni

- Rédaction de la charte informatique du bon usage des ressources informatiques

Nicolas Hernandez

Groupe école pratique	PPE 1 : Contexte laboratoire GSB Activité 1-3	Membres : Nicolas Hernandez, Ingrid Nguyen, Vincent Vandaele, Grégory Orsoni
Année : 2014 -2015		

- Réalisation d'une charte de procédure pour les réparations
- Réalisation d'une procédure en cas de panne

Ingrid Nguyen

- Réalisation du compte-rendu des réunions
- Remise en situation
- Réalisation de la nomenclature des équipements
- Fiche de remise en cas de panne et schéma d'une solution en cas de panne