LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale,
de l'Enfance et de la Jeunesse

Maisons de jeunes du Grand-Duché de Luxembourg

Sécurité de l'information

Charte de bonnes pratiques du responsable opérationnel

Informations générales :

Version :	1.1
État document :	Final
Classification :	Public
Contexte :	Maisons de jeunes du Grand-Duché de Luxembourg
Domaine :	Sécurité de l'information
Type de document :	Charte de bonnes pratiques du responsable opérationnel
Date :	13/02/2014
Mandataire :	Ministère de l'Education nationale, de l'Enfance et de la Jeunesse
Rédaction et Conseils :	CASES Luxembourg

1 Charte de bonnes pratiques à destination du responsable opérationnel de la maison de jeunes

1.1 Attribution des responsabilités

Le responsable opérationnel doit :

- distribuer avec accusé de réception la charte « Éducateur » au personnel encadrant en place et à tous les nouveaux collaborateurs ;
- intervenir, s'il constate qu'une personne ne respecte pas la charte ;
- vérifier que les changements d'ordre technique ou organisationnel qui ont lieu au sein de la maison de jeunes respectent les différentes chartes en place ;
- avertir le gestionnaire de la maison de jeunes si une situation de non-conformité aux chartes persiste ou est non solvable localement. Ce dernier en informera le ministère de l'éducation nationale, de l'enfance et de la jeunesse, le cas échéant.

1.2 Maîtrise de l'information

L'information sensible traitée dans une maison de jeunes peut être de deux natures :

1) les données opérationnelles : Concerne tous les documents concernant l'exploitation de la maison de jeunes qui ne doivent être ni détruits, ni perdus ni modifiés et qui peuvent être à caractère confidentiel (comptabilité, salaires, factures, courriers importants, contrats, etc.) ;
2) les données à caractère personnel : Concerne tous les documents contenant des informations nominatives sur des personnes internes ou externes (notes personnelles, fichier de présence, fichier de consultation internet, etc.), dans ce cas, ces informations ont un caractère confidentiel.

Le responsable opérationnel est en charge de répertorier ces informations et de définir où elles doivent être stockées, sachant que ces informations peuvent exister sous plusieurs formes (électronique, papier, etc.).

1.2.1 Contrôle de l'accès aux données

Le responsable opérationnel est en charge de définir si l'information peut être partagée ou non, et comment elle doit être manipulée.

Si cela est possible, deux principes de bases doivent toujours être mis en œuvre :

1) le besoin de savoir : Ne pas donner un accès systématique à toutes les personnes, si elles n'en ont pas besoin dans leur travail quotidien. Exemple : accès à la comptabilité de la maison par un éducateur ;
2) le moindre privilège : Ne pas donner tous les droits à une personne, si elle n'en a pas besoin. Exemple : Si un utilisateur ne doit utiliser qu'un seul logiciel. Alors il n'y a pas besoin de lui laisser le droit d'en installer d'autres.

Note : Ces deux principes ne remettent pas en cause la bonne foi d'un utilisateur, ni même son intégrité. Simplement en cas d'erreur de celui-ci, les conséquences seront plus limitées Exemple : si une personne se fait voler son mot de passe (hacker ou virus), l'usurpateur n'aura que les droits minimums de cette personne.

1.2.1.1 Information électronique (fichiers bureautiques, base de données, etc.)

Dans le cas de l'information sous forme électronique, des mots de passe (ou autres moyens) permettant de s'assurer de l'identité des personnes doivent être utilisés. Les réseaux de toutes les maisons de jeunes sont construits de la même façon. Ils permettent un cloisonnement qui crée des zones de « confiance » qui ne communiquent pas entre elles. Ces zones doivent être utilisées correctement:

- la zone « jeunes » (e.g. Jugend) est utilisée par les jeunes et ne doit stocker aucune information sensible ;
- la zone « personnel encadrant » (e.g. Betreuungspersonal) ne doit être utilisée que par le personnel encadrant permanent, parce qu'elle contient les informations sensibles ;
- la zone « intermédiaire » (e.g. Mittelzone), anciennement « Multimédia » est réservée au personnel non permanent.
    - Si cette zone n'est pas utilisée, elle peut héberger le Wifi.
    - Si elle est utilisée, alors une interface peut être ajoutée pour créer une quatrième zone et ainsi obtenir une zone pour le personnel non permanent et une zone Wifi séparées.

1.2.1.2 Information sur support papier ou amovible (classeurs, clé USB, etc.)

Dans le cas de l'information sur support papier ou amovible, c'est l'accès physique aux supports qui doit être restreint en les stockant dans des coffres, armoires, ou des locaux verrouillés et inaccessibles. L'organisation et la gestion des clés requièrent alors une importance primordiale dans le niveau de sécurité, des contraintes d'organisation doivent être définies et communiquées à l'équipe d'encadrement.

1.2.2 Sauvegarde des données

Toutes les informations sensibles doivent être sauvegardées selon une périodicité compatible avec leur importance pour les activités de la maison de jeunes. Les supports servant de backup doivent être protégés de la même façon que les données originales et si possible externalisées, pour se prémunir d'une perte totale en cas de sinistre majeur comme le feu ou le vandalisme.

1.3 Sécurité physique du matériel

Le matériel de routage fournit par le prestataire de service du ministère de l'éducation nationale, de l'enfance et de la jeunesse doit rester enfermé dans le rack fourni à cet effet. La clé de celui-ci doit être inaccessible aux personnes n'en ayant aucune utilité.

L'agencement des postes utilisateurs ne peut être modifié que dans la mesure ou le câblage ne présente aucun danger pour les enfants ou le personnel encadrant.

1.4 Protection contre les logiciels malveillants

Tous les ordinateurs doivent disposer d'un logiciel antivirus mis à jour.

La mise à jour du système et des programmes est soit automatique, soit exécutée régulièrement par une personne ayant les compétences requises.

1.5 Sécurité des connexions sans fil – WiFi

Si un réseau Wifi est mis à disposition, il doit être branché sur une zone dédiée pour que le trafic soit également filtré, voir chapitre 1.2.1.1.

1.6 Conformité à la législation

1.6.1 Droits d'auteurs

Tous les systèmes d'exploitation et logiciels soumis à des droits de licences doivent avoir été acquis et utilisés en toute légalité.

1.6.2 Information aux utilisateurs

Le document « Cyber Rules à la maison des jeunes » (e.g. Cyber Rules im Jugendhaus) doit être distribué ou affiché de façon à être très visible depuis les postes des utilisateurs, parce qu'il contient d'une part des règles de bonne conduite qui doivent être respectées, mais surtout l'avertissement qui informe l'utilisateur que toute action sur internet est enregistrée. Cet avertissement est obligatoire.