

GUIDE DE CYBERSÉCURITÉ

INFRASTRUCTURES NUMÉRIQUES SÉCURISÉES

DANS LES ÉCOLES ET LES STRUCTURES NON FORMELLES



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



Cofinancé par
l'Union européenne



CLAUDE DE NON-RESPONSABILITÉ

Ce guide constitue une aide générale et présente des recommandations de base en matière de sécurité dans les écoles fondamentales et les structures non formelles. Il n'est pas exhaustif et ne saurait se substituer aux dispositions légales, à une analyse individuelle des risques ou aux conseils des services spécialisés compétents.

Chaque structure est responsable de l'évaluation de ses risques spécifiques, de la mise en œuvre de mesures de sécurité appropriées ainsi que, si nécessaire, de l'implication des autorités ou services spécialisés compétents.

La mise en œuvre des mesures décrites dans ce guide ne garantit pas que les incidents de sécurité puissent être évités. L'organisme responsable décline également toute responsabilité quant aux dommages ou aux conséquences résultant de l'application ou de la non-application des recommandations contenues dans ce guide.

INFORMATIONS DESTINÉES AU PERSONNEL ÉDUCATIF

Ce guide se concentre sur les mesures de sécurité techniques et organisationnelles. Pour le personnel enseignant et éducatif, BEE SECURE propose également le guide « Un modèle à l'ère du numérique ». Cette publication contient des recommandations pratiques pour une utilisation responsable et sûre des outils numériques dans la vie professionnelle et privée.



Éditeur: Service national de la jeunesse (SNJ)
Service national de la jeunesse - B.P. 707 L-2017 Luxembourg
www.snj.lu | www.bee-secure.lu

© 2026 Service national de la jeunesse (SNJ) – Initiative BEE SECURE



Consulter la licence Creative Commons de cette publication :
www.creativecommons.org/licenses/by-nc-sa/4.0/deed.fr

Guide de cybersécurité
Infrastructures numériques sécurisées
Dans les écoles et les structures non formelles
09.2026

ISBN 978-2-919846-69-6
Ressource électronique

Initié par:



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Opéré par:



Service national
de la jeunesse



Cofinancé par:



Cofinancé par
l'Union européenne

En partenariat avec:



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

Précisions:

- Des outils d'intelligence artificielle ont été utilisés pour la mise en forme et la révision linguistique du texte. Ce texte a ensuite été relu et validé par l'équipe de BEE SECURE.
- Afin d'alléger la lecture de la présente publication, la forme masculine a été employée comme genre neutre pour désigner toute la population.

SOMMAIRE

INTRODUCTION	3
1. PRINCIPES DE BASE POUR UN ENVIRONNEMENT NUMÉRIQUE SÛR	4
2. GÉRER LES APPAREILS ET LES LOGICIELS EN TOUTE SÉCURITÉ	6
3. PROTÉGER LES RÉSEAUX ET L'INFRASTRUCTURE	10
4. RENFORCER LA PROTECTION DES DONNÉES ET LA CONFIDENTIALITÉ	13
5. SAUVEGARDER ET RESTAURER LES DONNÉES	16
6. PROTÉGER LES ENFANTS ET LES JEUNES	19
7. SE PRÉPARER AUX INCIDENTS DE SÉCURITÉ	22
8. EXEMPLES PRATIQUES	24
LIENS UTILES	27
BIBLIOGRAPHIE	27

INTRODUCTION

Les médias numériques accompagnent aujourd'hui les enfants et les jeunes dans presque tous les domaines de leur vie. Que ce soit à l'école, dans une maison relais, dans une maison de jeunes ou dans un foyer, partout sont utilisés des appareils, des plateformes et des services en ligne. Cette évolution s'accompagne également d'une responsabilité accrue : celle de rendre ces environnements numériques sûrs et de protéger les jeunes contre les risques sur Internet.

Ce guide s'adresse aux structures qui souhaitent sécuriser leur infrastructure numérique et la gérer de manière responsable. Il contient des recommandations pratiques concernant les comptes utilisateurs, les appareils, les réseaux, la protection des données, les systèmes de sauvegarde ainsi que la protection des enfants et des jeunes dans l'espace numérique.

Les recommandations s'adressent en premier lieu aux personnes responsables de l'infrastructure technique. Il peut s'agir, par exemple, de spécialistes informatiques internes ou externes à une structure, de techniciens, de membres du personnel des administrations communales, du personnel d'organismes gestionnaires ainsi que du personnel administratif de direction. Certaines recommandations s'adressent également au personnel enseignant et éducatif et sont marquées comme telles.

Les mesures présentées dans ce guide contribuent à réduire les risques numériques, à protéger les ressources techniques et à offrir aux enfants et aux jeunes un environnement numérique sûr.

1. PRINCIPES DE BASE POUR UN ENVIRONNEMENT NUMÉRIQUE SÛR

Quelques mesures organisationnelles et techniques de base permettent déjà d'éviter de nombreux problèmes de sécurité. Il s'agit notamment de gérer soigneusement les comptes utilisateurs, de définir clairement les droits d'accès et de vérifier régulièrement les principaux paramètres des systèmes.

1.1 Sécuriser les comptes utilisateurs

Les comptes utilisateurs constituent la base de l'accès aux appareils, aux réseaux et aux services numériques d'une structure. Ils permettent au personnel d'accéder aux appareils de travail, aux comptes de messagerie électronique, aux plateformes d'apprentissage, aux serveurs ou aux programmes de gestion. Ils permettent également d'attribuer clairement les accès à chaque personne.

De nombreux incidents de sécurité commencent par des données d'accès compromises. Une personne qui accède à un compte utilisateur peut, selon les droits accordés à ce compte, accéder à des appareils, à des réseaux ou à des informations sensibles. Il est donc particulièrement important de gérer les comptes utilisateurs avec soin.

Il est donc recommandé de mettre en place des règles claires pour la création et la gestion des données d'accès. Celles-ci comprennent notamment l'utilisation de phrases de passe longues et individuelles ou de mots de passe complexes, ainsi que la sensibilisation des utilisateurs aux bonnes pratiques en matière de sécurité.

Par rapport aux mots de passe classiques, les phrases de passe présentent l'avantage d'être à la fois sûres et plus faciles à mémoriser. Elles se composent de plusieurs mots choisis au hasard et doivent être complétées par des caractères spéciaux ou des chiffres.

Exemple :

Choisissez une phrase facile à mémoriser et qui ne contient aucune information personnelle. Par exemple :

« 225 enfants viennent à la MR. »

Une phrase de passe pourrait alors être créée de la manière suivante :

225.enfants.viennent.à.la.MR

Ou, de manière encore plus compacte, il est possible de créer un mot de passe à partir des premières lettres des mots d'une phrase :

« Dans notre grande MR, 225 enfants heureux viennent chaque jour !! »

DngMR225ehvcj!!

Vous pouvez ensuite utiliser le test de mot de passe de BEE SECURE pour vérifier le niveau de sécurité de votre mot de passe ou de votre phrase de passe.

Des gestionnaires de mots de passe peuvent constituer une aide utile pour conserver les données d'accès en toute sécurité. L'activation de l'authentification multifacteur (MFA) est particulièrement efficace. En plus du mot de passe ou de la phrase de passe, une confirmation supplémentaire est alors demandée, par exemple via une application ou un code de sécurité. Cette mesure rend considérablement plus difficile l'utilisation abusive de données d'accès compromises.



RECOMMANDATIONS

- Utilisez un mot de passe ou une phrase de passe individuelle pour chaque compte utilisateur.
- Évitez les mots de passe simples comme « 123456 », « password2025 », « ABC », « AZERTY » ou les combinaisons de touches faciles à deviner.
- Un mot de passe robuste comporte au moins 12 caractères choisis au hasard parmi des lettres minuscules et majuscules, des chiffres et des caractères spéciaux.
- Les phrases de passe longues et individuelles renforcent la sécurité et sont souvent plus faciles à mémoriser.
- Activez l'authentification multifacteur (MFA) lorsqu'elle est disponible.
- Utilisez un gestionnaire de mots de passe pour gérer vos données d'accès en toute sécurité.

1.2 Comptes utilisateurs individuels et droits d'administrateur

Dans la mesure du possible, chaque personne devrait disposer de son propre compte utilisateur. Les comptes individuels permettent de mieux retracer les activités et réduisent les risques liés au partage des données d'accès. Les comptes partagés rendent plus difficile l'identification de l'auteur de modifications ou d'incidents et augmentent le risque d'un accès involontaire ou abusif aux données et aux systèmes.

Il est également recommandé de séparer systématiquement les comptes utilisateurs ordinaires des comptes administrateur. Pour les tâches quotidiennes, un

compte standard suffit ; les droits d'administrateur ne doivent être utilisés que lorsque des modifications des systèmes, des logiciels ou des paramètres de sécurité sont nécessaires.

Les comptes administrateur font partie des accès qui nécessitent une protection particulière au sein d'une structure. Leur sécurisation à l'aide de l'authentification multifacteur (MFA) offre une protection supplémentaire contre les accès non autorisés.

RECOMMANDATIONS

- Créez un compte utilisateur individuel pour chaque personne.
- Utilisez les comptes administrateur exclusivement pour les tâches de gestion informatique.
- Au quotidien, travaillez avec un compte standard.
- Activez l'authentification multifacteur (MFA) pour les comptes administrateur.

2. GÉRER LES APPAREILS ET LES LOGICIELS EN TOUTE SÉCURITÉ

Dans la plupart des structures, de nombreux appareils numériques sont aujourd'hui utilisés, des ordinateurs et tablettes aux smartphones et écrans interactifs. Afin de pouvoir utiliser ces outils de manière fiable, il convient d'accorder une attention particulière à leur gestion et à leur sécurisation.

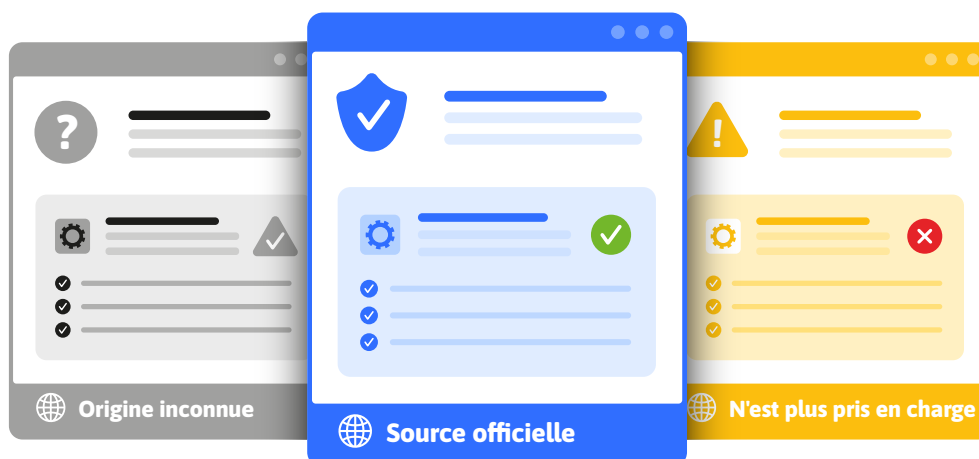
2.1 Choisir les logiciels avec soin

Tous les logiciels ne présentent pas le même niveau de fiabilité. Le choix des programmes utilisés a une influence directe sur la sécurité des différents appareils et de l'ensemble de l'infrastructure informatique. Les programmes provenant de sources inconnues ou les applications qui ne sont plus prises en charge peuvent présenter des failles de sécurité ou diffuser des logiciels malveillants.

Il est donc recommandé d'utiliser des logiciels provenant de sources officielles, comme les sites web des fabricants ou des magasins d'applications fiables. Avant d'introduire de nouveaux programmes, il est également utile de vérifier qu'ils sont toujours pris en charge par leur fabricant et qu'ils bénéficient régulièrement de mises à jour de sécurité.

RECOMMANDATIONS

- Téléchargez les logiciels uniquement à partir de sources officielles ou de magasins d'applications fiables.
- Avant l'installation, vérifiez que l'application est toujours prise en charge par son fabricant.
- N'utilisez pas de programmes modifiés ni de copies piratées.



2.2 Contrôler l'installation des logiciels

Chaque application supplémentaire augmente la surface d'attaque numérique d'un appareil. Il est donc recommandé de gérer les installations de logiciels de manière réfléchie.

L'installation de nouveaux programmes devrait être réservée aux personnes responsables de la gestion des appareils. Cela permet de réduire le risque que des applications non vérifiées ou inadaptées soient utilisées sur des appareils professionnels.

Il est également utile de vérifier régulièrement les programmes déjà installés. Les applications qui ne sont plus nécessaires devraient être supprimées afin d'améliorer la visibilité d'ensemble et la sécurité des appareils.

Sur les appareils utilisés par des enfants et des jeunes, des paramètres de protection des mineurs ou de restriction selon l'âge peuvent également être activés. Le chapitre 6 contient plus d'informations à ce sujet.

RECOMMANDATIONS

- Limitez l'installation de logiciels aux personnes autorisées.
- Supprimez les applications dont vous n'avez plus besoin.
- Activez des fonctions de protection des mineurs adaptées sur les appareils utilisés par des enfants et des jeunes.



2.3 Automatiser les mises à jour

Des vulnérabilités de sécurité sont régulièrement découvertes et corrigées grâce à des mises à jour. Les appareils et les applications qui ne sont pas mis à jour peuvent plus facilement devenir la cible de cyberattaques.

Les mises à jour automatiques permettent de maintenir les systèmes d'exploitation, les applications et les pilotes à jour sans effort supplémentaire. Cela concerne non seulement les ordinateurs, mais aussi les tablettes, les smartphones, les imprimantes, les serveurs, les routeurs et d'autres appareils connectés.

RECOMMANDATION

- Activez les mises à jour automatiques des systèmes d'exploitation, des programmes et des micrologiciels sur tous les appareils des utilisateurs, les serveurs et les équipements réseau.



2.4 Utiliser une protection antivirus

Les programmes antivirus détectent et bloquent de nombreuses menaces connues avant qu'elles ne puissent causer des dommages. Ils constituent donc un élément important d'un dispositif de sécurité à plusieurs niveaux. Sur les appareils de travail, il est recommandé d'utiliser une protection antivirus à jour, régulièrement mise à jour et capable de détecter en permanence de nouvelles menaces.

De nombreux systèmes d'exploitation disposent déjà de mécanismes de protection intégrés. Il reste néanmoins important de vérifier régulièrement qu'ils sont à jour et de s'assurer que les fonctions de protection sont activées. Les serveurs et autres systèmes centraux peuvent également bénéficier d'une protection supplémentaire.

RECOMMANDATIONS

- ◆ Activez la protection antivirus sur tous les appareils de travail.
- ◆ Maintenez les signatures antivirus à jour grâce à des mises à jour régulières.

2.5 Activer la journalisation du système

Les journaux système – également appelés « logs » – enregistrent les événements importants sur les appareils et les réseaux. Il peut s'agir, par exemple, de tentatives de connexion, de modifications du système ou d'incidents liés à la sécurité.

L'activation de la journalisation facilite l'analyse des problèmes techniques et permet de mieux retracer les incidents de sécurité. En cas de cyberattaque, les

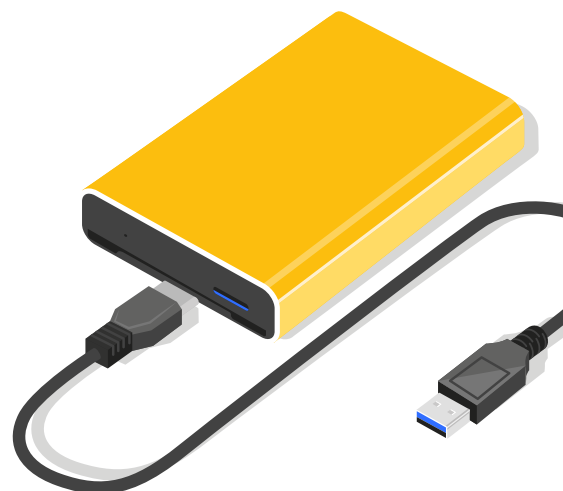
journaux peuvent fournir des indications importantes afin d'identifier les causes et les failles de sécurité et de mettre en place des mesures appropriées.

Selon le système d'exploitation utilisé et l'infrastructure existante, différents outils de journalisation sont disponibles. Pour les systèmes Windows, par exemple, la journalisation avancée à l'aide du service Sysmon¹ permet d'enregistrer des informations supplémentaires.

RECOMMANDATIONS

- ◆ Activez la journalisation du système sur les appareils utilisateurs administrés et les serveurs.
- ◆ Documentez les événements liés à la sécurité de manière traçable.

¹ <https://learn.microsoft.com/de-de/sysinternals/downloads/sysmon>



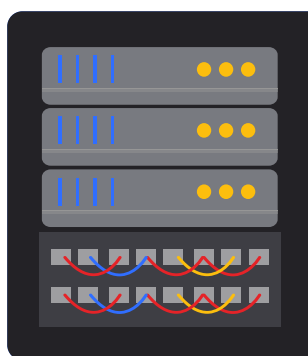
2.6 Éviter les supports de stockage externes

Les clés USB, les disques durs externes ou d'autres supports de stockage peuvent constituer une solution pratique pour transférer des données. Cependant, ils augmentent également le risque de perte de données, voire de fuite involontaire de données, car ces supports peuvent facilement être perdus ou volés. Il est donc généralement déconseillé d'utiliser des supports de stockage externes.

En outre, les supports de stockage provenant de sources externes ou inconnues, en particulier les clés USB, peuvent constituer une porte d'entrée pour les logiciels malveillants. Avant de les utiliser, il est toujours recommandé de les analyser à l'aide d'un programme antivirus à jour. Il est également

conseillé de désactiver les fonctions «AutoRun» et «AutoPlay». Cela permet d'éviter que des programmes ne s'exécutent automatiquement lors de la connexion d'un support de stockage.

Lorsque des solutions sécurisées et conformes aux exigences en matière de protection des données sont disponibles sur des serveurs ou dans le cloud (par exemple, des serveurs de fichiers internes), elles peuvent constituer une alternative sûre à l'échange de fichiers au moyen de supports physiques. Lors de l'utilisation de services de cloud, des mesures de sécurité appropriées, telles que des droits d'accès clairement définis et l'authentification multifacteur (MFA), contribuent également à protéger les données.



CONSEIL

Sensibilisez le personnel enseignant et éducatif ainsi que l'ensemble des autres membres du personnel à l'utilisation sûre des supports de stockage externes. Les clés USB provenant de sources externes ou inconnues ne devraient, en principe, pas être connectées aux appareils professionnels. Recommandez plutôt d'échanger les fichiers au moyen des solutions de serveur ou de cloud prévues par la structure.

RECOMMANDATIONS

- Utilisez uniquement des supports de stockage provenant de sources fiables.
- Désactivez «AutoRun» et «AutoPlay».
- Utilisez des serveurs sécurisés ou des solutions de cloud pour l'échange de fichiers.



3. PROTÉGER LES RÉSEAUX ET L'INFRASTRUCTURE

Une infrastructure réseau stable et sécurisée constitue la base d'un fonctionnement fiable des services numériques. Les réseaux relient entre eux les appareils, les utilisateurs et les applications. Ils jouent ainsi un rôle central dans la protection des données et des systèmes.

3.1 Pare-feu

Un pare-feu (*firewall*) surveille le trafic de données entre les réseaux et détermine quelles connexions sont autorisées ou bloquées. Il constitue une couche de protection importante entre Internet et les systèmes internes d'une structure.

De nombreux routeurs disposent déjà de fonctions de pare-feu intégrées. Dans les environnements plus complexes ou lorsque des infrastructures sont

partagées, un pare-feu dédié peut offrir une protection supplémentaire. Lorsque plusieurs organisations ou services utilisent la même connexion Internet, il est particulièrement recommandé de séparer clairement les différents réseaux et de les sécuriser.

RECOMMANDATIONS

- ◆ Assurez-vous que le pare-feu est activé sur les routeurs, les serveurs et les appareils de travail.
- ◆ Vérifiez s'il est nécessaire de mettre en place une séparation supplémentaire de votre réseau interne.



3.2 Séparer les réseaux

Tous les appareils et tous les utilisateurs n'ont pas besoin d'accéder aux mêmes données, fichiers et dossiers. Une séparation claire des différents réseaux renforce la sécurité et facilite leur gestion.

Il est par exemple possible de distinguer un réseau destiné au personnel, un réseau pour les enfants et les jeunes ainsi qu'un réseau pour les invités. Chacun de

ces réseaux peut disposer de ses propres droits d'accès et mécanismes de protection. Une telle segmentation permet d'éviter qu'un incident de sécurité survenant dans une partie du réseau n'ait automatiquement des conséquences sur les autres.

Exemple :

Une structure peut prévoir les réseaux suivants :

- Réseau du personnel avec accès aux fichiers internes, aux services et aux imprimantes
- Réseau pour les enfants et les jeunes avec des mesures de protection supplémentaires
- Réseau pour les invités avec un accès à Internet uniquement



RECOMMANDATIONS

- Limitez l'accès aux services internes aux personnes autorisées.
- Séparez les réseaux partagés les uns des autres.

3.3 Sécurité du réseau Wi-Fi

Les réseaux sans fil permettent un accès flexible à Internet et aux services internes. Ils peuvent toutefois constituer un point d'entrée potentiel pour des attaques s'ils ne sont pas suffisamment protégés. Les méthodes de chiffrement modernes comme WPA3 offrent un niveau de protection plus élevé que les anciennes normes. Lorsque cela est techniquement possible, il est recommandé d'utiliser WPA3.

Les données d'accès au réseau Wi-Fi doivent bénéficier du même niveau de protection que les autres données d'accès. Elles devraient être accessibles uniquement aux

personnes autorisées et être vérifiées régulièrement. Les données d'accès aux réseaux du personnel ou des invités ne devraient pas être affichées publiquement ni être visibles dans des endroits où des enfants, des jeunes ou des personnes non autorisées pourraient les consulter. En particulier pour les réseaux destinés aux invités, il convient de veiller à ce qu'aucune connexion avec les systèmes internes ne soit possible et, si nécessaire, de mettre en place des mesures de protection supplémentaires.



CONSEIL

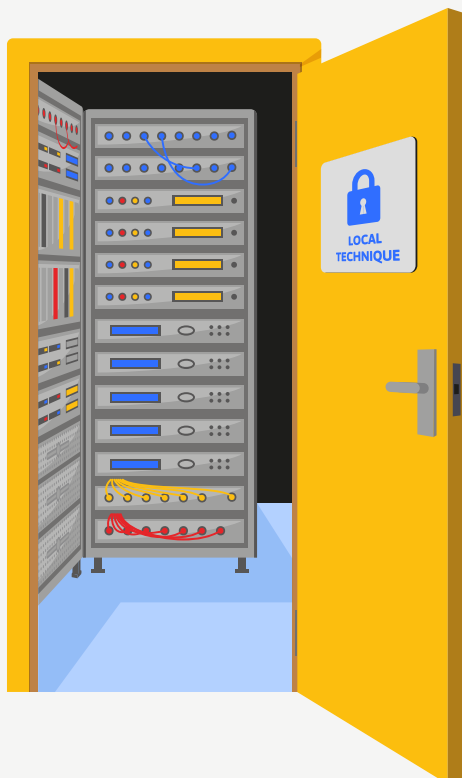
Les mots de passe Wi-Fi prévisibles, comme une année, le nom de la structure ou une simple suite de chiffres, n'offrent qu'une protection limitée. Les phrases de passe longues et individuelles renforcent considérablement la sécurité.

Le test de mot de passe de BEE SECURE vous permet de vérifier le niveau de sécurité d'un mot de passe ou d'une phrase de passe : pwdtest.bee-secure.lu



RECOMMANDATIONS

- Activez WPA3 ou au minimum WPA2.
- Séparez les réseaux destinés aux invités du réseau interne.
- Protégez les réseaux, y compris le réseau destiné aux invités, par un mot de passe.



3.4 Contrôle des accès et sécurité physique

La sécurité numérique ne se limite pas à ce qui se passe devant un écran. L'accès physique aux appareils, aux documents et aux installations techniques joue également un rôle important.

Les serveurs, les équipements réseau et les autres composants centraux contiennent souvent des informations sensibles ou permettent d'accéder à des systèmes critiques. Il est donc recommandé de mettre en place un contrôle d'accès approprié aux locaux techniques et aux infrastructures.

Les documents confidentiels, les supports de stockage et les appareils mobiles doivent également être conservés de manière à être protégés contre tout accès non autorisé. L'attribution des clés, des cartes d'accès ou des badges devrait être documentée de manière traçable. Cela permet de savoir à tout moment qui dispose de quels droits d'accès.

RECOMMANDATIONS

- Limitez aux personnes autorisées l'accès aux salles des serveurs.
- Lorsque vous ne vous en servez pas, conservez les appareils mobiles et les supports de stockage dans des armoires ou des tiroirs verrouillables
- Tenez une liste des clés, des *badges* et des cartes d'accès attribués.
- Verrouillez votre écran lorsque vous laissez votre poste de travail sans surveillance.
- Verrouillez votre bureau lorsque vous le quittez.



4. RENFORCER LA PROTECTION DES DONNÉES ET LA CONFIDENTIALITÉ

Dans le quotidien les écoles et des services d'éducation et d'accueil traitent de nombreuses données à caractère personnel, telles que des photos, de photos, des informations relatives à la santé, ou de coordonnées. Une gestion rigoureuse de ces informations contribue de manière essentielle à la protection de la vie privée de toutes les personnes concernées.

4.1 Choisir des services conformes au RGPD

De nombreux outils numériques facilitent le travail quotidien des écoles, des services d'éducation et d'accueil et des maisons de jeunes. Toutefois, ces services traitent souvent des données à caractère personnel.

Avant d'introduire de nouvelles applications, il est donc recommandé de vérifier leur conformité au règlement

général sur la protection des données (RGPD) de l'Union européenne. Il convient notamment de prendre en compte la nature des données traitées, les lieux de stockage ainsi que les dispositions du fournisseur en matière de protection des données.



CONSEIL

Toutes les applications pratiques ne répondent pas automatiquement aux exigences en matière de protection des données et de sécurité de l'information. Avant leur mise en place, vérifiez donc que les nouveaux services sont conformes au RGPD ainsi qu'aux directives internes de votre structure.

Une vue d'ensemble des services autorisés ou recommandés facilite le choix d'outils adaptés par le personnel et contribue à une utilisation cohérente au sein de la structure.

RECOMMANDATIONS

- Vérifiez, avant leur mise en place, que les nouvelles applications sont conformes au RGPD.
- Créez et tenez à jour une liste des services numériques autorisés par votre structure. Dans la mesure du possible, appuyez-vous sur les recommandations des organismes compétents, par exemple le MENJE ou le CGIE.
- Informez le personnel des applications dont l'utilisation est autorisée.



4.2 Garantir la confidentialité

Dans le cadre de leur activité, de nombreux membres du personnel ont accès à des informations sensibles concernant des enfants, des jeunes, des familles ou des collègues. Une gestion responsable de ces données contribue de manière essentielle à la protection de la vie privée.

Les personnes disposant de droits d'accès étendus, par exemple les spécialistes informatiques, les administrateurs ou les prestataires externes, ont souvent accès à des systèmes, des fichiers ou des journaux. L'accès à ces informations devrait être

limité aux contenus nécessaires à l'accomplissement de la tâche concernée.

Il est également recommandé de n'accorder aux membres du personnel que l'accès aux dossiers, fichiers ou systèmes dont ils ont réellement besoin pour leur travail quotidien. Cela permet de réduire le risque d'un accès involontaire à des informations sensibles.

Les accords de confidentialité peuvent contribuer à définir clairement les attentes et les responsabilités et à renforcer la sensibilisation à la protection des données sensibles.



QU'EST-CE QU'UN ACCORD DE CONFIDENTIALITÉ ?

Un accord de confidentialité – souvent également appelé « *Non-Disclosure Agreement* » (NDA) – précise que les informations confidentielles doivent être utilisées uniquement dans le cadre convenu et ne peuvent pas être transmises à des personnes non autorisées.

RECOMMANDATIONS

- Limitez les droits d'accès aux personnes qui en ont réellement besoin.
- Si nécessaire, concluez des accords de confidentialité avec les prestataires externes.
- Vérifiez régulièrement les droits d'accès accordés.
- Sensibilisez le personnel à la gestion des informations confidentielles.



4.3 Promouvoir une culture de la protection des données

La protection des données ne repose pas uniquement sur des mesures techniques. Une gestion consciente et responsable des données à caractère personnel dans le travail quotidien est tout aussi importante. Le personnel bénéficie d'informations claires sur ses droits et ses obligations dans le cadre du RGPD. Des actions régulières de sensibilisation et de formation peuvent contribuer à identifier rapidement les risques liés à la protection des données et à agir de manière appropriée.

Une culture de la protection des données implique également de vérifier régulièrement les données à

caractère personnel et de les supprimer dès qu'elles ne sont plus nécessaires ou que les délais légaux de conservation ont expiré. Cela concerne aussi bien les données numériques – par exemple sur des serveurs, des sites web ou dans des applications – que les documents papier contenant des informations à caractère personnel.

En outre, la désignation d'une personne de contact pour les questions relatives à la protection des données facilite la gestion des incertitudes ou des incidents. De nombreuses structures désignent à cette fin un « *Data Protection Officer* » (DPO).



RECOMMANDATIONS

- Désignez une personne de contact pour les questions relatives à la protection des données et encouragez un dialogue ouvert en cas de questions ou d'incertitudes.
- Prévoyez régulièrement des actions de sensibilisation.

4.4 Utiliser l'intelligence artificielle de manière responsable

Les outils basés sur l'intelligence artificielle (IA) et les agents conversationnels (chatbots) font désormais partie du quotidien professionnel dans de nombreuses structures. Ils peuvent considérablement faciliter les recherches, les traductions, la rédaction de textes ou d'autres tâches.

Toutefois, l'utilisation de ces services nécessite une attention particulière en ce qui concerne les données à caractère personnel. Selon la plateforme, les informations saisies peuvent être traitées, stockées ou utilisées pour améliorer les systèmes.

Lors de l'utilisation d'applications d'IA accessibles au public, il est donc recommandé de faire preuve de prudence avec les données à caractère personnel. Les noms, adresses, numéros de téléphone, données relatives à la santé ou autres informations sensibles concernant des enfants, des jeunes, des parents ou des membres du personnel ne doivent, en principe, pas être saisis dans des systèmes d'IA accessibles au public.



CONSEIL

Avant d'utiliser des applications d'IA, les données à caractère personnel peuvent être remplacées par des éléments fictifs ou être anonymisées au préalable. Par exemple, les noms peuvent être remplacés par des formulations comme « élève A », « membre du personnel B » ou « personne X ».



RECOMMANDATIONS

- Ne saisissez aucune donnée à caractère personnel dans des applications d'IA accessibles au public.
- Utilisez, dans la mesure du possible, des exemples anonymisés ou fictifs.
- Informez le personnel des possibilités et des risques liés aux applications d'IA.

INFORMATION POUR LE PERSONNEL ÉDUCATIF

Les enseignants, éducateurs et encadrants trouvent sur le site [KI-Kompass.lu](https://ki-kompass.lu) des informations, du matériel et des offres de formation continue pour une utilisation sûre et responsable de l'IA dans leur pratique pédagogique quotidienne.

5. SAUVEGARDER ET RESTAURER

LES DONNÉES

La perte de données a souvent des causes très courantes et n'est pas uniquement liée à des cyberattaques. Il s'agit fréquemment de situations du quotidien – un appareil défectueux, un document supprimé par erreur ou un smartphone perdu – qui peuvent rendre des informations importantes inaccessibles. Une stratégie réfléchie de stockage et de sauvegarde des données contribue à réduire les temps d'interruption et permet de restaurer les informations importantes en cas de besoin.

5.1 Choisir soigneusement les lieux de stockage

L'endroit où les données sont stockées a une influence directe sur leur sécurité et leur disponibilité. Lorsque les fichiers sont enregistrés uniquement sur des appareils individuels, ils risquent de ne plus être accessibles en cas de panne, de perte ou de vol de l'appareil. Les espaces de stockage partagés facilitent en revanche la collaboration et réduisent la dépendance à l'égard d'appareils individuels.

Lorsque des solutions adaptées sont disponibles, des serveurs de fichiers centralisés, des services de cloud fiables ou d'autres espaces de stockage gérés collectivement peuvent constituer des alternatives appropriées. Les supports de stockage physiques, comme les clés USB ou les disques durs externes, peuvent rester utiles pour certains usages, mais ils présentent des risques supplémentaires. Ils peuvent être perdus, endommagés ou tomber entre de mauvaises mains.

RECOMMANDATIONS

- Dans la mesure du possible, stockez les fichiers importants dans un système de stockage géré de manière centralisée.
- Évitez de stocker vos fichiers exclusivement sur un seul appareil.



5.2 Utiliser les fonctions de localisation des appareils

Les appareils mobiles comme les smartphones ou les tablettes contiennent souvent des données professionnelles et permettent d'accéder à différents services et comptes utilisateurs. En cas de perte ou de vol d'un appareil, les fonctions de localisation et de contrôle peuvent aider à le retrouver ou à le verrouiller à distance. De nombreux systèmes d'exploitation disposent déjà de fonctions correspondantes, comme «Localiser» ou «Localiser mon appareil».

La tenue d'un inventaire des appareils mobiles utilisés peut également faciliter leur gestion. Celui-ci peut notamment contenir le type d'appareil, le numéro de série ou l'«identité internationale d'équipement mobile» (*International Mobile Equipment Identity, IMEI*) des téléphones mobiles. Ces informations peuvent être utiles en cas de perte et faciliter les démarches auprès de la police ou des opérateurs de téléphonie mobile.



QU'EST-CE QUE L'IMEI ?

L'«identité internationale d'équipement mobile» (*International Mobile Equipment Identity, IMEI*) est un numéro d'identification unique attribué aux téléphones mobiles. Il peut notamment être utile en cas de perte ou de vol d'un appareil. L'IMEI figure généralement sur l'emballage de l'appareil. Sur de nombreux téléphones mobiles, il peut également être affiché directement en saisissant le code *#06# dans l'application Téléphone.

RECOMMANDATIONS

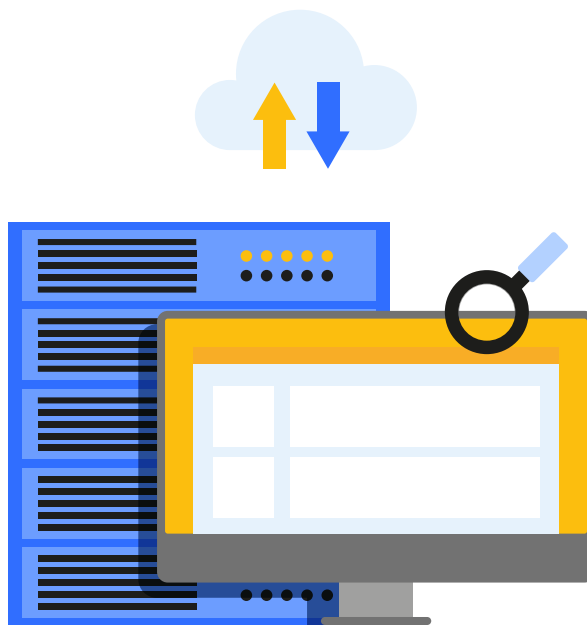
- Activez les fonctions de localisation sur les appareils mobiles professionnels.
- Documentez les types d'appareils, les numéros de série et les numéros IMEI.
- Définissez une procédure à suivre en cas de perte ou de vol d'un appareil mobile.
- Verrouillez ou effacez à distance les appareils perdus dans les meilleurs délais.



5.3 Planifier et tester les sauvegardes

Les sauvegardes (*back-ups*) font partie des mesures les plus importantes pour se protéger contre la perte de données. Elles permettent de restaurer des informations importantes après des problèmes techniques, des cyberattaques ou des erreurs humaines.

Dans un premier temps, il est recommandé de dresser une vue d'ensemble de tous les emplacements de stockage au sein de la structure. Il peut s'agir des ordinateurs de travail, des appareils mobiles, des serveurs de fichiers, des services de cloud ou d'autres systèmes de stockage. Pour chaque emplacement, il est ensuite possible de déterminer à quelle fréquence une sauvegarde doit être effectuée et quelle quantité de données pourrait être perdue de manière acceptable en cas d'incident.



La règle dite « 3-2-1-0 » constitue une bonne référence :

3 copies des données

En plus des données originales, il existe au moins deux copies de sauvegarde supplémentaires.

2 supports de stockage différents

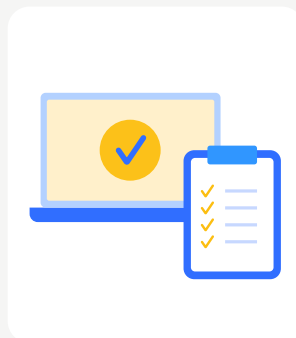
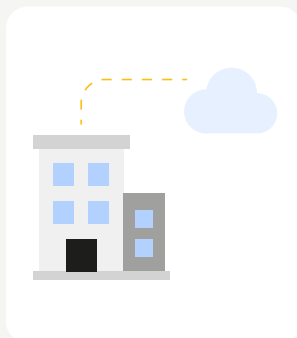
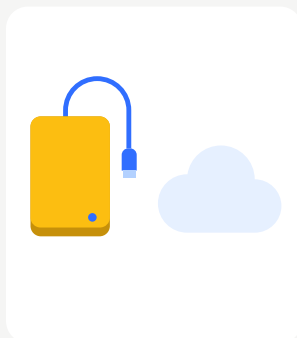
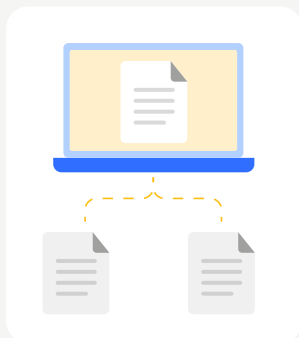
Les sauvegardes sont enregistrées sur au moins deux supports ou solutions de stockage différents, par exemple sur un disque dur externe et dans une solution de cloud.

1 copie externe

Au moins une sauvegarde est conservée en dehors de la structure afin de rester disponible même en cas d'incendie, de dégât des eaux ou d'autres incidents graves.

0 erreur lors de la restauration

Les sauvegardes sont testées régulièrement afin de détecter et de corriger rapidement les sauvegardes endommagées ou incomplètes.



INFORMATIONS POUR LE PERSONNEL ÉDUCATIF

Le personnel enseignant et éducatif devrait également être conscient de l'importance de sauvegarder régulièrement ses données de travail. Les supports pédagogiques, les documents ou les autres fichiers utilisés dans le cadre professionnel devraient être sauvegardés régulièrement dans les solutions de stockage prévues par la structure et ne pas être conservés exclusivement sur des appareils locaux ou privés.

RECOMMANDATIONS

- Effectuez régulièrement des sauvegardes de toutes les données importantes.
- Utilisez la règle 3-2-1-0 comme référence.



6. PROTÉGER LES ENFANTS ET LES JEUNES

Les enfants et les jeunes évoluent aujourd'hui beaucoup dans des espaces numériques. Ils apprennent, jouent, communiquent et s'informent en ligne. Cependant, ils peuvent aussi être confrontés à des contenus ou à des offres qui ne sont pas adaptés à leur âge ou à leur développement. Des mesures de protection techniques peuvent contribuer à limiter les risques et à créer un cadre sûr pour l'utilisation des services numériques.

6.1 Utiliser des filtres de contenu

Les filtres de contenu peuvent limiter l'accès aux sites web et aux services en ligne qui sont inadaptés ou potentiellement dangereux pour les enfants et les jeunes. Ils permettent par exemple de restreindre l'accès aux contenus destinés aux adultes, aux jeux d'argent, aux représentations de violence, aux logiciels malveillants ainsi qu'à certaines formes de fraude en ligne.

Selon l'infrastructure technique, ces filtres peuvent être configurés au niveau du réseau, sur certains appareils ou directement dans les applications. En complément, des paramètres de contrôle parental peuvent être utilisés sur les appareils mobiles et dans les applications afin de limiter davantage l'accès aux contenus inadaptés à l'âge.

CONSEIL UTILE

Pour les écoles et les services d'éducation et d'accueil, différents filtres de contenu sont disponibles via RESTENA. Ils permettent de limiter l'accès à des contenus en ligne inadaptés ou potentiellement dangereux. Les communes et les autres structures intéressées peuvent contacter directement RESTENA afin d'obtenir des informations sur les solutions de filtrage disponibles et leur mise en place. Comme les contenus et les plateformes en ligne évoluent en permanence, il est recommandé de vérifier régulièrement les paramètres de filtrage.

Contact: restena.lu/fr/contact



IMPORTANT

Aucun système de filtrage ne peut détecter ou bloquer de manière fiable l'ensemble des contenus problématiques. Les filtres de contenu complètent donc l'accompagnement pédagogique ou la supervision des enfants, mais ne les remplacent pas.

RECOMMANDATIONS

- Configurez des filtres de contenu au niveau du réseau, des appareils ou des applications.
- Activez les paramètres de contrôle parental sur les appareils mobiles et dans les applications.



6.2 Comptes utilisateurs adaptés aux enfants

Pour les appareils mis à la disposition des enfants ou des jeunes, il est recommandé d'adapter la configuration à leur âge. Des comptes utilisateurs individuels permettent de mieux adapter les droits d'accès, les applications et les paramètres de sécurité. Ils facilitent également la séparation entre les accès du personnel et ceux des enfants ou des jeunes.

Lorsque des ordinateurs ou des tablettes sont mis à disposition, il est recommandé de créer un compte utilisateur personnel pour chaque enfant. Dans les écoles, cela peut par exemple se faire au moyen des comptes IAM (*Identity and Access Management*). Les comptes individuels facilitent la gestion des droits d'accès et favorisent une utilisation responsable des outils numériques.

S'il n'est pas possible de créer un compte utilisateur personnel pour chaque enfant, il est recommandé de séparer au minimum les comptes du personnel de ceux

des enfants ou des jeunes. En plus du compte principal destiné aux adultes, un compte utilisateur distinct peut être créé pour les enfants ou les jeunes. Ce compte devrait disposer de droits limités et, en particulier, ne pas avoir de droits d'administrateur. Des fonctions supplémentaires de protection des mineurs ou de contrôle parental peuvent également aider les adultes dans la gestion et l'accompagnement.

Les comptes adaptés aux enfants peuvent par exemple empêcher l'installation de logiciels, la modification des paramètres de sécurité ou l'accès à des contenus inadaptés. Des applications et des offres pédagogiques déjà préinstallées facilitent en outre une utilisation sûre des appareils et réduisent la nécessité d'installer des logiciels supplémentaires.

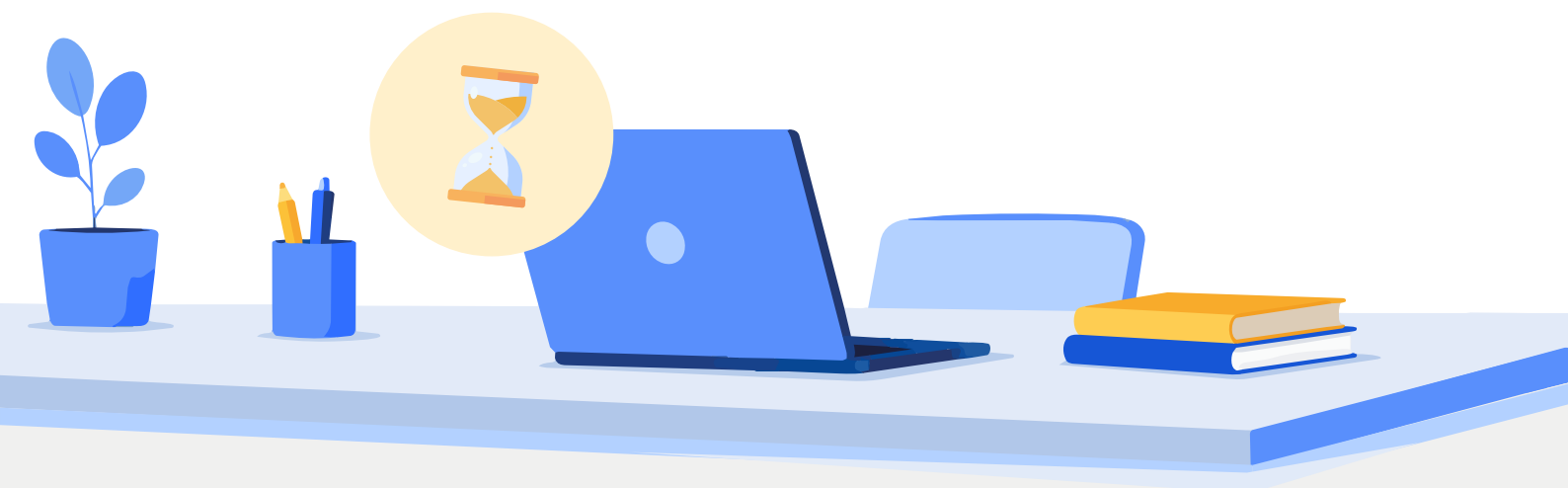
INFORMATIONS POUR LE PERSONNEL ÉDUCATIF

Les jouets connectés, les plateformes d'apprentissage numériques et les applications basées sur l'intelligence artificielle (IA) nécessitent également une attention particulière. Avant de les utiliser, il est recommandé de vérifier les paramètres de protection des données et de sécurité ainsi que les recommandations relatives à l'âge.

RECOMMANDATIONS

- Dans la mesure du possible, créez un compte utilisateur individuel pour chaque enfant.
- Pour les enfants, utilisez uniquement des comptes standard sans droits d'administrateur.
- Utilisez des fonctions de protection des mineurs ou de contrôle parental.





6.3 Définir les temps d'utilisation

Selon le type de structure, il peut être utile de limiter l'accès à Internet à certaines plages horaires. Cela concerne en particulier les structures d'hébergement, les internats ou d'autres structures dans lesquelles les enfants et les jeunes ont également accès à des appareils numériques en dehors des heures d'enseignement ou d'encadrement.

Des réseaux Wi-Fi activés selon des horaires définis ou une limitation technique du temps d'écran peuvent aider à adapter les temps d'utilisation aux besoins de chaque structure. De telles mesures contribuent à réduire les périodes d'utilisation sans surveillance ou excessive et favorisent un usage équilibré des médias numériques.

INFORMATIONS POUR LE PERSONNEL ÉDUCATIF

Les limitations de temps peuvent fournir un cadre. Elles sont toutefois particulièrement efficaces lorsqu'elles s'accompagnent d'échanges sur l'utilisation des médias, les habitudes de sommeil et l'équilibre numérique.

RECOMMANDATIONS

- Fixez des temps d'utilisation pour les appareils partagés.
- Servez-vous des fonctionnalités techniques pour contrôler l'accès à Internet.



7. SE PRÉPARER AUX INCIDENTS DE SÉCURITÉ

Même les structures bien protégées ne sont pas à l'abri de problèmes techniques ou d'incidents de sécurité. Il est donc essentiel non seulement de prévenir les risques, mais aussi de se préparer aux situations dans lesquelles un problème survient.

7.1 Formation continue

Les technologies numériques évoluent en permanence. Parallèlement, de nouveaux risques de sécurité, de nouvelles formes de fraude et de nouvelles méthodes d'attaque apparaissent.

Des formations régulières permettent de suivre les évolutions actuelles et de mettre à jour les connaissances existantes. Cela concerne non seulement les personnes

responsables des aspects techniques, mais aussi celles qui utilisent des outils numériques dans leur travail quotidien. Selon le domaine d'activité, des thèmes comme la cybersécurité, la protection des données, la cyberhygiène, l'éducation aux médias ou l'utilisation de l'intelligence artificielle (IA) peuvent être pertinents.

INFORMATIONS POUR LE PERSONNEL ÉDUCATIF

Le personnel enseignant et éducatif bénéficie également de formations régulières dans des domaines comme les médias numériques et les tendances actuelles en ligne (*online trends*). Cela facilite l'accompagnement des enfants et des jeunes dans leur quotidien numérique. Profitez des nombreuses offres de formation continue proposées, par exemple, par l'Institut national d'administration publique, l'Institut de Formation de l'Éducation Nationale, la Plattform, le Digital Learning Hub ou le Lifelong Learning Centre.

RECOMMANDATIONS

- Prévoyez régulièrement des formations pour les responsables informatiques et les autres membres du personnel.
- Informez le personnel des formes de fraude actuelles et des nouveaux risques de sécurité.

7.2 Tenir des listes de contacts à disposition

En cas d'incident de sécurité, chaque minute peut compter. Une liste de contacts à jour facilite une communication rapide et contribue à coordonner les mesures nécessaires.

Selon la structure, cette liste peut regrouper des personnes de contact internes et externes. Il peut s'agir, par exemple, des responsables techniques, des délégués

à la protection des données, des prestataires externes ou des organismes compétents pour le signalement des incidents. Les coordonnées du *Computer Emergency Response Team* compétent peuvent également figurer dans cette liste. Celle-ci devrait être vérifiée régulièrement et mise à jour en cas de changements de personnel ou d'organisation.



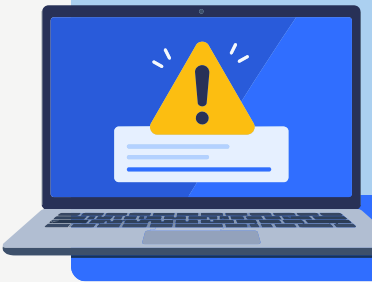
QU'EST-CE QU'UN CERT ?

Un *Computer Emergency Response Team* (CERT) aide les organisations à faire face aux cyberincidents et aux problèmes techniques liés à la sécurité. Vous trouverez sur cert.lu une liste de tous les CERT établis au Luxembourg.

7.3 Préparer des plans de réponse

Lorsqu'un incident de sécurité survient, les responsables doivent souvent agir sous pression. Un plan de réponse préparé à l'avance peut aider à suivre les étapes importantes de manière systématique. Le plan peut préciser qui doit être informé, quelles mesures immédiates sont prévues et comment les décisions doivent être documentées. Cela permet d'éviter que des tâches importantes ne soient oubliées.

Selon la nature de l'incident, les premières mesures peuvent par exemple consister à déconnecter du réseau les appareils concernés, à modifier les données d'accès ou à informer les spécialistes compétents. Des exercices ou des réunions régulières peuvent contribuer à faire connaître les procédures et à renforcer la capacité d'action en cas d'incident.



GARDER SON CALME

Un incident de sécurité exige d'agir rapidement, mais de manière réfléchie. Évitez les décisions précipitées et suivez le plan de réponse préparé étape par étape. Des procédures claires et des responsabilités définies permettent d'évaluer la situation de manière systématique, de mettre en place les mesures appropriées et de limiter autant que possible les dommages supplémentaires.

RECOMMANDATIONS



- Établissez une liste de contacts à jour pour les incidents de sécurité et renseignez les personnes de contact internes et externes.
- Élaborez un plan de réponse en cas d'incident de sécurité.
- Définissez clairement les responsabilités et les voies de communication.
- Documentez les mesures immédiates à prendre pour différents scénarios.
- Entraînez-vous régulièrement à suivre la procédure avec les personnes concernées.

8. EXEMPLES PRATIQUES

Chaque structure dispose de conditions techniques et d'un cadre organisationnel qui lui sont propres. Les exemples suivants montrent comment différentes mesures de sécurité peuvent être mises en œuvre dans des situations typiques du quotidien. Les mesures décrites servent de repères et peuvent être adaptées aux besoins spécifiques de chaque structure.

Cas pratique 1 Sauvegarde des données dans une école fondamentale

SITUATION DE DÉPART

Une école fondamentale souhaite s'assurer que les données importantes restent disponibles même après une panne technique ou un incident de sécurité.

DÉFIS

- Identifier les différents emplacements de stockage
- Éviter la perte de données
- Permettre la restauration des données

MESURES POSSIBLES

● Inventaire des emplacements de stockage

Il est possible de prendre en compte, entre autres, les ordinateurs de travail, les serveurs, les services de cloud et les appareils mobiles.

● Définir une stratégie de sauvegarde

La règle 3-2-1-0 constitue une référence éprouvée pour la création de copies de sauvegarde. Pour en savoir plus, consultez le chapitre 5.3.

● Tester la restauration

Des tests réguliers permettent de vérifier le bon fonctionnement des sauvegardes.

INFORMATIONS POUR LE PERSONNEL ÉDUCATIF

Les supports pédagogiques, les documents, les photos ou les autres fichiers utilisés dans le cadre professionnel doivent également faire l'objet d'une sauvegarde appropriée, quel que soit l'appareil sur lequel ils sont stockés.

Si des appareils privés sont utilisés à des fins professionnelles, une prudence particulière est recommandée. Ces appareils ne bénéficient pas nécessairement des mêmes mesures de sécurité que ceux de la structure. Dans la mesure du possible, enregistrez donc les données professionnelles dans les solutions de stockage prévues par la structure et évitez de les conserver exclusivement sur des appareils privés.

Cas pratique 2 Accès à Internet dans une structure d'hébergement ou un internat

SITUATION DE DÉPART

Dans une structure d'hébergement, les enfants et les jeunes utilisent Internet quotidiennement – pour faire leurs devoirs, se divertir ou rester en contact avec leur famille et leurs amis. La structure souhaite permettre cette utilisation tout en garantissant un niveau de protection approprié.

DÉFIS

- Éviter l'accès à des contenus inadaptés
- Tenir compte des différents groupes d'utilisateurs
- Réduire l'utilisation sans surveillance pendant la nuit
- Garantir la sécurité du réseau

MESURES POSSIBLES

● Filtres de contenu

L'utilisation de filtres de contenu peut contribuer à limiter l'accès à des contenus inadaptés ou potentiellement dangereux. RESTENA propose différentes solutions de filtrage à cet effet.

● Réseaux séparés

Des réseaux distincts pour le personnel, les résidents et les invités facilitent la gestion et renforcent la sécurité.

● Gestion des horaires d'accès à Internet

Selon le fonctionnement de la structure, il peut être utile de désactiver l'accès à Internet en dehors des plages horaires prévues, par exemple à l'heure du coucher.

Cas pratique 3 Postes informatiques dans une maison relais

SITUATION DE DÉPART

Une maison relais met des ordinateurs à la disposition des enfants pour faire leurs devoirs, utiliser des offres d'apprentissage ou réaliser des activités créatives.

DÉFIS

- Permettre une utilisation adaptée à l'âge
- Empêcher les modifications non souhaitées sur les appareils
- Favoriser une utilisation sûre d'Internet

MESURES POSSIBLES

● Créer des comptes utilisateurs

Des comptes distincts pour les enfants et les adultes facilitent la gestion des droits d'accès et des paramètres de sécurité. Les comptes utilisateurs adaptés aux enfants bénéficient de droits limités. Ainsi, par exemple, les enfants et les jeunes ne peuvent pas installer eux-mêmes des programmes ou des jeux ni modifier des paramètres système liés à la sécurité.

● Mettre à disposition des applications adaptées

Des programmes d'apprentissage préinstallés et des applications sélectionnées peuvent contribuer à une utilisation sûre.

● Sécuriser le réseau

Des réseaux distincts pour les enfants et le personnel renforcent la sécurité et simplifient la gestion. Des noms de réseau clairement définis facilitent l'identification et réduisent le risque de confusion. Il est par exemple possible d'utiliser des noms comme « MR_WLAN_Kids » et « MR_WLAN_Staff ».

● Utiliser des filtres de contenu

Les filtres peuvent limiter l'accès aux contenus inadaptés et favoriser une utilisation sûre.

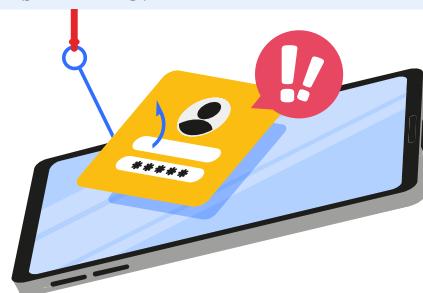
RÉSULTAT

Les appareils peuvent être utilisés pour les activités prévues tout en tenant compte des principales mesures de sécurité.

Cas pratique 4 Réagir à un incident d'hameçonnage (phishing)

SITUATION DE DÉPART

Un membre du personnel reçoit un e-mail contenant un lien vers une prétendue page de *Microsoft Teams*. Après s'être connecté, il soupçonne qu'il s'agissait d'une tentative d'hameçonnage (*phishing*).



DÉFIS

- Empêcher une éventuelle utilisation abusive du compte utilisateur
- Informer les services compétents

● Tenir compte des autres comptes

Si le même mot de passe a été utilisé ailleurs, il est également recommandé de modifier les données d'accès de ces comptes.

MESURES POSSIBLES

● Contacter les services compétents

Informez au plus vite les responsables informatiques internes ainsi que, le cas échéant, le *Centre de gestion informatique de l'éducation (CGIE)* ou d'autres services spécialisés.

● Modifier les données d'accès et vérifier la sécurité

Modifiez immédiatement le mot de passe concerné, si nécessaire avec l'aide de services spécialisés. Vérifiez si des sessions de connexion sont encore actives et fermez-les. Activez l'authentification multifacteur (MFA).

● Documenter et signaler l'incident

Consignez la date et l'heure de l'incident, la plateforme concernée ainsi que les informations qui auraient éventuellement été divulguées. S'il s'agit d'un incident majeur soumis à une obligation légale de notification, signalez-le aux autorités compétentes en matière de protection des données ou de cybersécurité.

LIENS UTILES

BEE SECURE Un modèle à l'ère du numérique

bee-secure.lu/de/publikation/erzieher-und-lehrer-im-umgang-mit-medien-und-technologien/

CGIE

cgie.lu

CIRCL

circl.lu

CNPD

cnpd.public.lu

Fondation RESTENA – DNS Server

restena.lu/fr/service/serveurs-dns

Guide pratique – Mettre en place la sécurité de l'information : les étapes clés pour bien débuter

anssi.extranet.etat.lu/fr/actualites/2026/approche-securite-information

Microsoft – What is incident response

microsoft.com/de-de/security/business/security-101/what-is-incident-response

BIBLIOGRAPHIE

Cyber fundamentals SMALL

atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

Quelle est la règle de sauvegarde 3-2-1-1-0 ?

zmanda.com/fr/blog/understanding-the-3-2-1-1-0-backup-rule/

Microsoft Phishing

support.microsoft.com/de-de/windows/sch%C3%BCtzen-sie-sich-vor-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

Pour plus d'informations, consultez

BEE-SECURE.LU