Prevention first:

Cycle de vie de vos collaborateurs :

Comment encadrer le parcours des employés en matière de sécurité cyber ?

(Guide à destination des équipes informatiques)

Digital Security
Progress. Protected.

De l'intégration au travail quotidien en passant par l'éventuel départ de l'entreprise, le parcours de chaque employé comprend des phases spécifiques qui nécessitent votre attention et un accompagnement informatique rigoureux et adapté (chaque organisation ayant son propre fonctionnement et ses exigences en matière d'équipements et de politique de sécurité).

Qu'il s'agisse d'accueillir de nouvelles recrues, de consolider le groupe de collaborateurs ou de gérer des départs, l'équipe informatique joue un rôle essentiel pour assurer la continuité et la sécurité de l'organisation.

Disposer d'un processus ou d'une feuille de route bien définis pour le cycle de vie des employés n'est pas seulement une question d'efficacité : c'est une mesure préventive robuste. En alignant les procédures informatiques sur des pratiques éprouvées, les entreprises peuvent atténuer les risques liés à la sécurité des données, au contrôle d'accès et à la conformité. Cette checklist guidera les administrateurs et équipes informatiques à travers les différentes étapes de la vie professionnelle des employés, en leur offrant des ressources pour responsabiliser les collaborateurs et protéger l'environnement numérique de l'entreprise.

Comment utiliser ce document ?

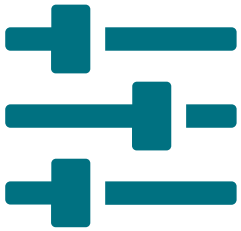
Cette checklist encadre l'arrivée et le départ des collaborateurs et pourra vous servir de référence pour maintenir la sécurité et la performance de votre infrastructure numérique.

Elle vous permettra de prendre en compte toutes les étapes nécessaires à chaque moment du cycle de vie de l'employé.

INTÉGRATION DU NOUVEAU COLLABORATEUR

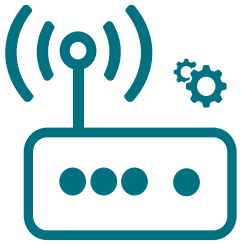
Digital Security
Progress. Protected.

1. Préparer les appareils pour les nouveaux employés :



- Attribuez le matériel hardware et étiquetez chaque appareil en conséquence.
- Trouvez tous les accessoires nécessaires, y compris les moniteurs, les stations d'accueil, les claviers et les souris.
- Préparez ces équipements pour les nouveaux employés. Plusieurs étapes peuvent être nécessaires :
  - ☐ Installer et fournir tout le matériel et les logiciels nécessaires
  - ☐ Configurer les comptes de messagerie et les autorisations d'accès
  - ☐ Mettre en place des mesures de sécurité et des profils d'utilisateurs
  - ☐ Personnaliser l'appareil en fonction du rôle et des besoins de l'utilisateur

2. Transmission des informations des premiers jours :



- Proposez une assistance aux nouveaux employés pour qu'ils puissent se connecter pour la première fois sur le site.
- Aidez les employés à définir leurs mots de passe
- Effectuez une vérification de l'appareil avec l'utilisateur pour vous assurer que tout fonctionne correctement
- Fournissez une fiche d'instructions de base sur la sécurité, la configuration du Wi-Fi et d'autres points essentiels (à définir selon vos exigences et besoins)
- Veillez à ce que le nouvel employé signe la charte de sécurité de l'entreprise

3. Règlements et directives :

- Etablissez une liste et des directives concernant les applications et les logiciels que les employés doivent/peuvent utiliser
- Familiarisez vos employés avec les différentes politiques de l'entreprise, dont, par exemple :
  - ☐ Politique en matière d'informatique/de cybersécurité
  - ☐ Politique de protection des données (RGPD)
  - ☐ Politique de travail à distance
  - ☐ Politique en matière de réseaux sociaux
  - ☐ Politique en matière de BYOD (Bring Your Own Device)

POLITIQUE BYOD (Bring Your Own Device)

Le **système BYOD** est assez populaire de nos jours : il consiste à permettre à vos employés d'utiliser leurs appareils à des fins personnelles et professionnelles. Votre politique de sécurité doit pouvoir indiquer la marche à suivre pour l'autoriser sans mettre en danger la sécurité de votre entreprise.
Voici quelques questions que la politique BYOD devrait prendre en compte :

- ☐ **Qui peut participer au programme BYOD ?**
- ☐ **Liste des appareils, systèmes d'exploitation et plateformes autorisés et pris en charge dans le cadre de la politique**
- ☐ **Exigences en matière de mot de passe**
- ☐ **Exigences en matière de chiffrement des données**
- ☐ **Explication du processus d'effacement à distance**
- ☐ **Limitations de l'accès aux données et de l'utilisation des données**
- ☐ **Clarification du niveau d'assistance informatique fourni pour les appareils personnels**
- ☐ **Particularités de la surveillance et de l'audit**
- ☐ **Responsabilités des employés en matière de sécurité et de conformité**
- ☐ **Que faire en cas de perte ou de vol d'un appareil ?**
- ☐ **Que faire lorsque la collaboration se termine ?**

AU COURS DE LA COLLABORATION

Digital Security
Progress. Protected.

1. Formation à la cybersécurité :

- Sensibiliser en permanence les employés aux menaces et aux pratiques indispensables de cyberhygiène.

Comment créer une culture cyber robuste et éviter la lassitude à l'égard de la sécurité ?

- ☐ Collaborez avec le département des RH pour rendre la formation interactive et utile
- ☐ Mettez en place des sessions de formation plus courtes et plus fréquentes, qui sont souvent plus efficaces qu'une seule formation annuelle
- ☐ Partagez des histoires vraies et des exemples tirés de votre expérience pour rendre le contenu plus concret
- ☐ Utilisez des formats ludiques - comme des jeux, des quiz et des simulations de façon à mieux impliquer les employés
- ☐ Ce n'est pas en effrayant les employés que vous les sensibiliserez à la cybersécurité. Si vous adoptez cette approche, ils risquent de craindre de signaler une erreur ou toute potentielle cybermenace
- ☐ Soyez ouvert aux questions et rassurez vos employés sur le fait que vous êtes disponible pour les aider s'ils en ont besoin

2. Principe du moindre privilège :

- Veillez à ce que le principe du moindre privilège soit respecté (les utilisateurs ne disposent que de l'accès réellement nécessaire à leurs missions)
- Examinez régulièrement les autorisations d'accès et adaptez-les en conséquence
- Désactivez le partage de fichiers et le transfert de courriels vers des adresses externes pour éviter les fuites de données

3. Maintenance des appareils :

- Vérifiez régulièrement que les appareils des employés soient dotés des derniers correctifs de sécurité et des dernières mises à jour logicielles. Cela concerne à la fois les appareils fournis par l'entreprise et les appareils personnels utilisés pour le travail

4. Règles pour le travail à distance :

- Déconseillez l'utilisation d'appareils personnels pour des tâches professionnelles - à moins que votre entreprise n'applique le système BYOD
- Encouragez l'utilisation d'un réseau privé virtuel (VPN) pour des connexions sécurisées
- Promouvez l'utilisation du chiffrement pour les données sensibles
- Soulignez l'importance de mots de passe Wi-Fi forts pour empêcher tout accès non autorisé
- Veillez à ce que la protection des endpoints soit active et à jour sur tous les appareils distants

DÉPART DU COLLABORATEUR

Digital Security
Progress. Protected.

1. Gestion des comptes et des accès :

- Révoquez les autorisations pour toutes les applications et tous les services auxquels l'employé quittant l'entreprise avait accès
- Réinitialisez les mots de passe de tous les appareils de l'entreprise utilisés par l'employé

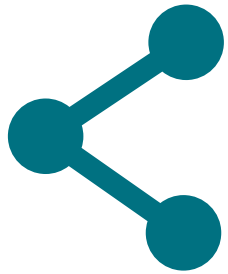
2. Accès physique et matériel :

- Révoquez l'accès aux bâtiments, y compris les cartes d'accès et les clés
- Collectez et récupérez tous les appareils de l'entreprise remis à l'employé qui quitte l'entreprise, y compris les ordinateurs portables, les smartphones et tout autre matériel.

3. Contrôle et protection des données :

- Maintenez une communication régulière avec l'employé qui quitte l'entreprise afin de surveiller son comportement au cours du processus de sortie
- Procédez à un examen final des outils de surveillance et de journalisation afin de détecter toute activité inhabituelle ou non autorisée liée aux comptes et systèmes de l'employé concerné
- Envisagez le déploiement d'une solution de prévention de la perte des données (DLP) pour détecter tout accès non autorisé à des appareils ou à des données pendant ou après le départ du collaborateur

4. Procédures du dernier jour :



- Veillez à ce que la remise du matériel soit finalisée
- Bloquez les comptes de l'employé pour empêcher tout accès ultérieur
- Effectuez un effacement sécurisé des appareils de l'employé pour supprimer les données de l'entreprise

Nous sommes ESET.

Une défense proactive. Notre activité consiste à minimiser la surface d'attaque.

Gardez une longueur d'avance sur les cybermenaces connues et émergentes grâce à **notre approche axée sur la prévention, alimentée par l'IA et l'expertise humaine.**

Profitez d'une protection de premier ordre grâce à nos renseignements sur les cybermenaces, accumulés et analysés depuis plus de 30 ans.

Notre réseau étendu de recherche et développement, dirigé par des experts reconnus, assure la sécurité de votre entreprise pour qu'elle puisse exploiter pleinement le potentiel de la technologie.

EN SAVOIR PLUS

ESET®
Digital Security
Progress. Protected.