1. LES BONNES PRATIQUES EN SÉCURITÉ NUMÉRIQUE

Chez **ÉtudeSecours**, la sécurité informatique est une priorité absolue. Nous nous engageons à protéger les données de nos utilisateurs, employés et partenaires de manière proactive.

ÉtudeSecours déclare qu'elle met en place des mesures selon les meilleures pratiques en sécurité informatique fait partie intégrante de notre **Politique de confidentialité** et détaille nos engagements en matière de sécurité des données.

1.1 Gestion de l'accès aux données

Nous mettons en place des contrôles d'accès stricts pour garantir que seules les personnes autorisées ont accès aux données sensibles. L'accès aux données est attribué en fonction des besoins de chaque individu, et les autorisations sont revues régulièrement pour s'assurer de leur pertinence.

1.2 Sensibilisation à la sécurité

Nous formons régulièrement nos employés aux bonnes pratiques en matière de sécurité informatique, y compris la gestion des mots de passe, la détection des menaces et la protection des données confidentielles.

1.3 Gestion des mots de passe

Nous exigeons des mots de passe forts et leur rotation régulière. Les informations d'authentification sont stockées de manière sécurisée et ne sont pas partagées avec des tiers non autorisés.

1.4 Surveillance des menaces

Nous utilisons des outils de surveillance des menaces pour détecter et contrer les activités suspectes ou malveillantes. Les incidents de sécurité sont signalés, analysés et résolus en temps opportun.

1.5 Mises à jour et correctifs

Nous maintenons tous nos systèmes, logiciels et applications à jour en appliquant les derniers correctifs de sécurité pour prévenir les vulnérabilités connues.

1.6 Gestion des appareils

Les appareils utilisés pour accéder aux données de l'entreprise sont soumis à des politiques de sécurité strictes, y compris des configurations de sécurité, des mises à jour régulières et des contrôles d'accès appropriés.

1.7 Gestion des incidents

En cas d'incident de sécurité, nous avons un plan d'intervention en place pour atténuer les risques, rétablir la sécurité et informer toutes les parties prenantes concernées.

1.8 Respect de la législation et des normes

Nous nous conformons à toutes les lois et réglementations applicables en matière de protection des données, ainsi qu'aux normes de l'industrie en matière de sécurité informatique.

1.9 Audit et amélioration continue

Nous menons régulièrement des audits de sécurité pour évaluer l'efficacité de nos pratiques et nous engageons à améliorer en permanence nos mesures de sécurité informatique.

2. COLLECTE DES DONNÉES NÉCESSAIRES À L'UTILISATION DE NOS PLATEFORMES

Chez **ÉtudeSecours**, nous nous engageons à respecter la vie privée de nos utilisateurs et à collecter uniquement les données strictement nécessaires à l'utilisation de notre plateforme. Cette déclaration vise à vous informer sur notre Politique de collecte de données limitée, soulignant notre engagement envers la protection de vos informations personnelles.

2.1 Collecte ciblée des informations

Nous collectons uniquement les données qui sont essentielles pour vous fournir les services de notre plateforme de manière efficace. Ces informations peuvent inclure, par exemple, votre nom, votre adresse e-mail et d'autres données spécifiques requises pour l'utilisation de nos services.

2.2 Finalités claires

Les données collectées sont utilisées uniquement dans le but explicite pour lequel elles ont été fournies. Nous ne traitons pas vos informations à des fins autres que celles pour lesquelles vous nous les avez communiquées.

2.3 Consentement éclairé

Avant de collecter vos données, nous sollicitons votre consentement explicite, en vous informant de manière claire et compréhensible des informations que nous allons recueillir, des finalités de cette collecte et de la manière dont ces données seront traitées. Votre consentement est exprimé lorsque vous acceptez les conditions d'utilisation de nos plateformes et de notre site Web.

2.4 Transparence

Nous vous informons de manière transparente sur notre Politique de confidentialité, y compris sur les données que nous collectons, la manière dont nous les utilisons et les mesures que nous prenons pour les protéger.

2.5 Protection des données

Nous mettons en place des mesures de sécurité appropriées pour protéger vos données contre tout accès non autorisé, leur divulgation, leur altération ou leur destruction.

2.6 Conservation limitée

Nous conservons vos données personnelles pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Une fois que ces finalités sont atteintes, nous supprimons vos données de manière sécurisée.

2.7 Accès restreint

Seules les personnes autorisées au sein de notre organisation ont accès à vos données personnelles, et ce, dans la mesure où cela est nécessaire pour fournir nos services. Nous exigeons de ces employés le respect strict de la confidentialité.

Nous nous engageons à maintenir une collecte de données aussi limitée que possible pour garantir la protection de votre vie privée.

3. POLITIQUE DE GESTION DES RUSTINES (CORRECTIFS ET PATCHS)

Chez **ÉtudeSecours**, nous sommes déterminés à maintenir un environnement informatique sécurisé et fiable pour nos utilisateurs. Nous considérons que les mises à jour et les rustines sont essentielles pour garantir la sécurité de nos systèmes, la fiabilité de nos services et la protection des données. Par conséquent, nous tenons à souligner notre engagement à effectuer des mises à jour et à appliquer des rustines de manière régulière.

3.1 Définition des rustines

Le terme *rustine* (ou *patch* en anglais) désigne des correctifs mineurs pour résoudre des problèmes, des vulnérabilités ou des bogues dans un programme informatique, un système d'exploitation, une application ou un logiciel. Ces correctifs sont mis en place par les développeurs du logiciel ou de la plateforme pour corriger des erreurs ou des failles de sécurité après que le logiciel a été publié (rendu public). Les rustines sont mises en place sur une base régulière,afin d'améliorer la stabilité, la performance et la sécurité des logiciels.

3.2 Mises à jour de logiciels et de systèmes

Nous surveillons constamment les nouvelles versions de logiciels, d'applications et de systèmes que nous utilisons au sein de notre organisme. Dès qu'une mise à jour est disponible et qu'elle est jugée nécessaire, nous nous engageons à la déployer rapidement.

3.3 Correctifs de sécurité

La sécurité de nos systèmes et de nos données est notre priorité. Ainsi, nous veillons à appliquer les correctifs de sécurité dès leur disponibilité pour remédier aux vulnérabilités connues et prévenir les menaces potentielles.

3.4 Plan de gestion des mises à jour

Nous avons un plan de gestion des mises à jour qui spécifie les responsabilités, les procédures et les délais pour garantir que les mises à jour et les rustines sont appliquées de manière cohérente et efficace.

3.5 Communication transparente

En cas de maintenance ou de mise à jour planifiée, nous communiquerons avec nos utilisateurs pour les informer de toute interruption de service potentielle. Nous

nous engageons à minimiser ces interruptions. Les utilisateurs seront informés des interventions qui pourraient changer leur expérience de façon significative.

3.6 Surveillance continue

Nous surveillons constamment nos systèmes pour détecter les éventuelles anomalies ou irrégularités et nous prenons des mesures immédiates en cas de problème.

Nous croyons que la mise à jour régulière de nos logiciels et la gestion proactive des rustines sont essentielles pour garantir la sécurité et la stabilité de nos services.

4. DÉCLARATION SUR LA CONSIGNATION DES ÉVÉNEMENTS (LOGS)

Chez ÉtudeSecours, la consignation des événements (logs) dans le cadre de l'utilisation de ses systèmes informatiques constitue une pratique essentielle visant à assurer la sécurité, la stabilité et la performance optimale de nos systèmes.

4.1 Objectifs de la consignation des événements

Sécurité : Les logs nous permettent de détecter et de répondre rapidement à toute activité suspecte ou non autorisée sur nos systèmes. En enregistrant les événements, nous renforçons la sécurité de nos données sensibles et des informations confidentielles.

Diagnostic des problèmes : En consignant les événements, nous facilitons l'identification et la résolution rapide des problèmes techniques. Les logs jouent un rôle crucial dans le processus de dépannage, permettant à notre équipe informatique d'intervenir efficacement en cas d'incident.

Optimisation des performances : L'analyse des logs nous offre des informations précieuses sur l'utilisation de nos systèmes. Cette compréhension approfondie nous permet d'optimiser les performances, d'anticiper les besoins en ressources et de garantir une expérience utilisateur fluide.

4.2 Protection de la confidentialité

Les informations consignées dans les logs sont traitées avec le plus grand soin et dans le respect absolu de la confidentialité. Les mesures appropriées sont mises en

place pour garantir que seules les personnes autorisées ont accès à ces données, conformément à notre Politique de confidentialité.

Enfin, nous sommes résolus à maintenir notre environnement informatique à jour et à agir de manière diligente pour protéger les données de nos utilisateurs. Si vous avez des questions ou des préoccupations concernant nos différentes politiques et déclarations, n'hésitez pas à nous contacter à cybersecurite@etudesecours.com.