DIRECTIVE INFORMATIQUE

Département: Legal & Compliance

Auteur: Christina Hooker Legal Counsel

Créé: Berne, 07.06.2021

Ce règlement décrit l'utilisation des ressources informatiques et des informations des entreprises de BMS. Une utilisation inappropriée des ressources informatiques expose BMS à divers risques tels que des virus informatiques, la compromission de la disponibilité de systèmes et des services, ainsi qu'à des répercussions juridiques. Pour garantir une sécurité efficace,
il importe que tous les membres du personnel jouent leur rôle.

Domaine de validité

Cette directive s'applique à tous les collaborateurs des entreprises de BMS. Ces entreprises sont les suivantes:

- BR Bauhandel AG
- Gétaz-Miauton SA
- Barrit Baubedarf AG
- Regusci Reco SA

La directive est jointe au règlement du personnel. BMS est fondée à compléter et à amender le présent règlement à tout moment. La version en vigueur de la directive informatique peut être consultée sur les canaux de communication de BMS, ou auprès du service RH ou du supérieur de chaque collaborateur.

Assumer ses responsabilités

Indépendamment de la fonction ou de la position hiérarchique chez BMS, le collaborateur peut contribuer à améliorer la sécurité en assumant ses responsabilités.

Connaître les règles et les consignes de sécurité

Le collaborateur doit se familiariser avec cette directive et avec d'autres consignes de sécurité de BMS. En cas de questions, il doit s'adresser au helpdesk informatique ou à son supérieur.
BMS se réserve le droit de réprimer tout manquement à cette directive conformément aux articles 3.1 et 3.8 du règlement du personnel.

Signaler les vulnérabilités

Si des incidents critiques surviennent ou si des vulnérabilités sont identifiées, BMS attend de ses collaborateurs qu'ils agissent immédiatement en informant le helpdesk informatique ou leur supérieur PAR TÉLÉPHONE. Attention: il est interdit de transmettre des tentatives d'hameçonnage, des ransomware ou toute autre menace au helpdesk ou à toute autre personne au sein du réseau BMS par e-mail. Il convient de supprimer immédiatement le message incriminé ou de le placer dans le dossier des e-mails indésirables. Si un virus a déjà été placé en quarantaine, il est inutile de prendre d'autres mesures. En cas de doute, il faut contacter le helpdesk informatique par téléphone.

Les collaborateurs sont priés de ne pas tester eux-mêmes les vulnérabilités qu'ils ont identifiées ou dont ils soupçonnent l'existence.

Aider ses collègues

Aidez vos collègues en attirant leur attention sur les risques de sécurité identifiés. Un conseil amical est souvent plus utile qu'une consigne.

Utilisation des logiciels et du matériel

Matériel et logiciels privés
Il est expressément interdit d'utiliser des appareils privés tels que des PC, des ordinateurs portables ou des appareils connectés au réseau au sein des entreprises de BMS. Il est également interdit de traiter ou de sauvegarder des informations confidentielles de BMS sur des appareils personnels au domicile du collaborateur.

Exceptions:

- Les utilisateurs ayant obtenu une autorisation écrite du service informatique leur permettant d'utiliser leurs propres appareils.
- Les collaborateurs internes et externes ou les invités qui utilisent le Wi-Fi des invités.
- La synchronisation professionnelle des e-mails et du calendrier avec des smartphones et des tablettes privés n'est permise **qu'avec le compte Exchange BMS** et non pas avec iCloud ou avec tout autre service privé (basé sur le cloud on non). Les utilisateurs acceptent explicitement que des directives de sécurité soient automatiquement configurées sur les appareils lors de la synchronisation.

Achat, installation et élimination d'appareils et de logiciels
Le service informatique achète et installe le nouveau matériel, les nouveaux logiciels et les nouveaux services. Un formulaire à cet effet est à la disposition de tout le personnel sur le portail libre-service Astra sur l'intranet BMS. Le supérieur hiérarchique et les RH transmettent ce formulaire directement au service informatique pour qu'il y soit approuvé (par l'intermédiaire du helpdesk) avant qu'un ticket de demande soit déclenché dans notre système de tickets (la helpline actuellement). Cette procédure s'applique également aux freeware (logiciels disponibles gratuitement), aux produits Open Source (codes sources disponibles gratuitement) ou aux services de cloud. Les logiciels utilisés doivent être associés à une licence, sans exception. Il faut par ailleurs s'assurer que les logiciels installés ne sont pas copiés de manière illégitime. Il est interdit d'installer des logiciels privés.

Tous les appareils doivent être nettoyés superficiellement et restitués au service informatique **avec tous leurs accessoires, tels que les chargeurs, les sacoches, etc**. L'assistance informatique reconfigure entièrement les ordinateurs portables et les ordinateurs de bureau, si bien que toutes les données sont supprimées. Les documents privés peuvent être stockés sur une clé USB avant la restitution, puis supprimés sur l'ordinateur portable/de bureau. **Les iPhones doivent être intégralement dissociés du compte iCloud et leurs réglages d'usine doivent être entièrement réappliqués** avant qu'ils ne soient restitués à l'assistance informatique. Si cette opération n'est pas réalisée avant la restitution, l'entreprise est susceptible de facturer au collaborateur les coûts correspondants.

Stockage sur le cloud
La sauvegarde de données sur des services de cloud privés tels que Dropbox, OneDrive, Box, G-Drive, etc., est interdite. Les besoins doivent être signalés au service informatique.

Pannes/vol de matériel et de logiciel
Toutes les pannes de logiciels et d'appareils doivent être immédiatement signalées au supérieur et au helpdesk informatique. Le vol de logiciels et d'appareils doit d'abord être immédiatement signalé à la police. La justification de la plainte (scan ou document original) doit être transmise au helpdesk informatique à l'aide d'un ticket (le document est nécessaire pour la déclaration du sinistre à l'assurance responsabilité civile). Conformément aux articles 3.1 et 3.8, la responsabilité des collaborateurs peut être engagée pour des dégâts intentionnels ou résultant d'une négligence grave subis par du matériel ou des logiciels, et ils peuvent être sanctionnés.

Utilisation, entretien et nettoyage des appareils
Les appareils informatiques de BMS doivent être utilisés conformément aux instructions du service informatique. Le matériel ne doit pas être modifié, durablement ou superficiellement (en y apposant des autocollants par exemple) sans l'accord du service informatique. Toute utilisation anormale d'un appareil doit être immédiatement signalée au service informatique.
Les collaborateurs sont responsables de l'entretien et du nettoyage externes des appareils de BMS. Le matériel bien entretenu dure plus longtemps et subit moins de pannes. Les boissons et les aliments doivent être tenus éloignés des claviers et des appareils.

Utilisation des outils de communication

Règles concernant l'utilisation d'Internet, des e-mails, de la téléphonie et des communications sur Beekeeper

- BMS permet à tous les collaborateurs d'accéder à Internet depuis les appareils informatiques à des fins professionnelles.

- Les collaborateurs sont responsables de leurs actes. Comme l'accès à Internet est restreint par un filtre, tous les services sur Internet ne sont pas disponibles. Les contenus interdits et ceux qui pourraient porter préjudice à BMS sont filtrés.

- Les restrictions assurées par le filtre sont contraignantes et ne doivent pas être contournées.

- Le téléchargement de documents illicites (en particulier de reproductions pornographiques, de documents politiques extrémistes, etc.), ainsi que la violation du copyright, sont interdits et peuvent s'accompagner de répercussions pénales pour les utilisateurs et de sanctions en vertu du règlement du personnel de BMS.

- L'utilisation occasionnelle d'Internet et du téléphone professionnel (pour passer des appels) à des fins privées est autorisée. La productivité des collaborateurs ne doit toutefois pas s'en trouver compromise pendant son temps de travail.

- Les règles suivantes s'appliquent si un smartphone privé sert également de téléphone professionnel:
    - Aucune synchronisation de cloud privée n'est autorisée.
    - Le dossier professionnel ne peut être synchronisé QUE sur le serveur Exchange BMS.
    - Il est interdit de sauvegarder des enregistrements numériques (vidéos, photos, audio, etc.) de données de BMS sur un espace de stockage privé (interne ou en plus).

- En utilisant Internet, les utilisateurs reconnaissent expressément le droit de BMS d'enregistrer le trafic de données dans le cadre des bases légales et de l'évaluer dans le cadre de la loi sur la protection des données.

- **L'utilisation du compte mail professionnel à des fins privées est interdit.** Le compte de messagerie du collaborateur qui quitte l'entreprise, ainsi que tous les autres comptes informatiques et la boîte de réception, sont sécurisés et condamnés au plus tard pendant son dernier jour de travail. Les comptes sont supprimés au bout d'un certain temps.
  Les comptes de messagerie de collaborateurs ayant quitté l'entreprise ou qui sont portés malades pour une période prolongée et qui n'ont pas eu l'occasion de transmettre leurs activités courantes à un suppléant peuvent être examinés pour identifier les e-mails concernant les activités courantes avec le consentement du département Legal & Compliance et sur la base d'un double contrôle. Si, contre toute attente, des e-mails privés apparaissent pendant la recherche, ils sont retirés sans être lus.

- La surveillance du trafic d'e-mails professionnels a lieu dans le cadre des dispositions légales correspondantes. BMS suit la procédure suivante:
  - S'il existe un soupçon sérieux de manquement grave dans l'entreprise qui ne permet toutefois pas de remonter à un individu précis, le service des RH doit demander par écrit au service informatique d'organiser une surveillance générale. Le service informatique peut alors engager une surveillance superficielle générale. Cette surveillance générale ne révèle aucune identité.
  - Si les soupçons se renforcent suite à la surveillance superficielle, le service informatique peut ordonner des analyses plus ciblées.
  - Si un collaborateur est soupçonné spécifiquement de manquement, le service informatique peut examiner son compte utilisateur pour savoir si le manquement est avéré, suite à une demande émanant du service des RH.
  - Le service informatique n'ouvre pas les e-mails et les documents portant la mention «Privé» ou les e-mails et les documents qui sont clairement de nature privée (s'il y a par exemple un diminutif dans l'objet).
  - Les collaborateurs concernés sont informés de l'investigation ciblée au plus tard après celle-ci.
  - Le département Legal & Compliance accompagne le service informatique pendant toutes ses investigations.

  Les conséquences en vertu du droit du travail peuvent s'étendre d'un avertissement à un licenciement sans préavis en fonction de la gravité de l'acte détecté.

- Les e-mails d'origine inconnue ou douteuse doivent être immédiatement supprimés. Il ne faut en aucun cas ouvrir des pièces jointes inconnues ou non désirées.

- En cas de doute, il faut contacter par TÉLÉPHONE le helpdesk informatique avant l'ouverture de la pièce jointe douteuse. Il est interdit de transmettre des pièces jointes douteuses au helpdesk informatique.

- Des numéros de cartes de crédit, des mots de passe, des codes secrets, etc. ne doivent jamais figurer dans des e-mails.

- Communications sur Beekeeper. Les règles d'utilisation suivantes s'appliquent:
  - Nous nous fions au sens des responsabilités des collaborateurs. En cas d'incertitudes, chaque collaborateur est tenu de s'adresser à son supérieur ou aux RH.
  - Les règles existantes concernant l'emploi de téléphones portables s'appliquent lors de l'utilisation de BMSmobile.
  - Tous les contenus publiés sur BMSmobile sont exclusivement destinés à un usage interne et ne doivent pas être transmis à des tiers.

- Il est expressément interdit de publier des articles racistes, sexistes ou outrageants pour certains collaborateurs ou groupes de collaborateurs. BMS se réserve le droit de supprimer les articles et les contenus qui contreviennent à cette règle.
- BMSmobile ne doit pas être utilisé par des clients.

Vous trouverez de plus amples renseignements sur Beekeeper à l'adresse https://bms.beekeeper.io/fairplay

Les actions suivantes sont explicitement interdites:

- toute violation des lois en vigueur ou des bonnes mœurs;
- tout contournement d'une mesure de sécurité du service d'information;
- toute violation de droits de propriété industrielle, de droits d'auteur, droits personnels, de droits de propriété ou d'autres droits de tiers;
- toute transmission de contenus associés à des logiciels malveillants (virus, chevaux de Troie, vers, logiciels espions, logiciels publicitaires) ou à toute autre programmation pouvant endommager les logiciels;
- toute utilisation d'une page ou toute exécution d'une application qui pourrait entraîner des dommages ou une défaillance fonctionnelle des sites Web de BMS, notamment par des modifications de la structure physique ou logique des serveurs ou du réseau;
- toute distribution ou tout affichage de courriels de masse non sollicités ou harcelants ou d'autres messages, promotions, enquêtes externes (basées sur Internet ou non), publicités ou autres sollicitations, etc.;
- tout accès à ou toute utilisation des applications, systèmes, services, outils, données, comptes, réseaux ou contenus sans autorisation écrite ou à des fins non prévues;
- toute désactivation, toute interruption, tout contournement, toute perturbation ou toute autre violation de la sécurité des sites Internet;
- toute attaque, tout abus, toute perturbation, toute interruption ou toute exploitation des utilisateurs, systèmes ou services, y compris, mais sans s'y limiter, le déni de service (DoS), la surveillance, le crawling, le spamming, l'utilisation de bots ou de scripts.
- Les collaborateurs s'engagent également à éviter les actions suivantes:
  - l'affichage, l'envoi, la réception ou le stockage de contenus obscènes ou inappropriés;
  - la menace, le harcèlement, la persécution, la diffamation sans preuve ou l'abus de confiance d'une personne physique ou morale;
  - la promotion directe ou indirecte, le soutien ou la commercialisation de tout produit, service, solution commerciale ou autre technologie de tiers;
  - la tentative de collecte, d'enregistrement ou de publication de données personnelles via nos sites Web et/ou nos profils sans la connaissance et le consentement de la personne concernée;
  - l'envoi de renseignements trompeurs ou faux concernant la source, y compris l'usurpation d'identité ou l'hameçonnage;
  - la participation à ou la promotion d'activités illégales ou criminelles, telles que la pornographie infantile, le jeu ou le piratage;

- l'autorisation ou l'encouragement des tiers à prendre l'une des mesures ci-dessus.

L'utilisation des données

Il tient particulièrement à cœur à BMS que l'entreprise, et donc ses collaborateurs, utilisent avec diligence les données et les informations qui leur sont confiées,
non seulement parce que la loi sur la protection des données et d'autres réglementations nous y contraignent, mais surtout parce il nous importe de protéger la vie privée de nos collaborateurs et de nos clients.

Le support des données (papier ou ordinateur) ne joue aucun rôle.

Les points suivants doivent être respectés dans ce cadre:

Traitement des données
Avec votre compte utilisateur, vous avez accès à des données de l'entreprise qui sont critiques et fiables. La consultation, le traitement et la sauvegarde de ces données sont uniquement prévus à des fins professionnelles indépendamment du lieu de l'accès (bureau ou accès à distance).

La consultation, le traitement et la sauvegarde de données ne sont autorisés que sur des appareils appartenant à des entreprises de BMS. La synchronisation de données d'e-mails et d'intranet fait exception.

Il incombe systématiquement aux collaborateurs de traiter adéquatement les données de l'entreprise.

Mise sous clé des informations confidentielles
Les papiers et les autres supports de données contenant des informations confidentielles ne doivent pas traîner plus longtemps que nécessaire et doivent être mis sous clé après leur utilisation.

Toute information et tout document qui décrit des réalités internes ou qui pourrait s'avérer précieux pour la concurrence est considéré comme confidentiel. Ce principe s'applique également aux informations personnelles.

Sécurité dans les salles de réunion
Les collaborateurs ne doivent laisser ni papiers de travail confidentiels, ni données confidentielles, sur des tableaux à feuilles et des tableaux blancs dans les salles de réunion. Des données confidentielles ne doivent pas non plus se trouver dans les poubelles.

Elimination sûre de données physiques
Il faut de préférence détruire les documents confidentiels à l'aide d'un broyeur ou tout du moins les rendre illisibles en réduisant leur taille.

Sauvegarde de données
Les données doivent être sauvegardées sur les systèmes centraux et non pas localement sur l'ordinateur. Sur ces systèmes, BMS est en mesure de garantir que les strictes exigences en matière de protection et de sécurité des données peuvent être correctement mises en œuvre et donc que les produits du travail des collaborateurs sont encore intégralement disponibles après une reconfiguration ou le remplacement d'un appareil. Dans le cas contraire, les données sont perdues en cas de défaillance ou de vol d'un appareil, ou de fausse manipulation.

Accès à distance (VPN)

- Chaque VPN d'accès à distance doit être demandé par un supérieur auprès du helpdesk informatique dans le système de tickets.

- L'accès à distance doit impérativement faire l'objet d'une authentification bifactorielle. Le service informatique fournit une application de smartphone en vue de cette authentification. Le client VPN «Global Protect» est installé sur les ordinateurs portables et les tablettes de BMS.

- L'utilisateur d'un VPN doit disposer d'un compte utilisateur BMS, d'une version Windows à jour, d'une version à jour de Citrix Workspace et d'une bonne connexion à Internet ou d'une large bande passante si plusieurs appareils nécessitant une forte bande passante (par exemple, une box TV, une console de jeu, etc.) sont connectés en même temps.

- Les règles ordinaires relatives à la consultation, au traitement et à la sauvegarde de données de l'entreprise s'appliquent également aux accès à distance. L'utilisateur du VPN est tenu de s'assurer que son ordinateur est à jour et protégé (antivirus actuel, etc.).

La sécurité sur le lieu de travail

De nombreuses personnes externes entrent et sortent chaque jour dans les entreprises de BMS: clients, visiteurs, artisans, techniciens, personnel de nettoyage et de gardiennage. L'ordre sur le lieu de travail constitue donc un aspect important de la sécurité.

Suivre la politique Clean Desk

Une politique Clean Desk est en vigueur chez BMS. En d'autres termes, les collaborateurs sont tenus de ranger tous leurs documents lors d'interruptions prolongées et au plus tard à la fin de chaque journée de travail. Si les collaborateurs quittent leur poste de travail pour une période prolongée, ils doivent mettre sous clé les informations confidentielles présentes sur du papier, des supports de données, des ordinateurs portables et des tablettes.

Prudence en présence de personnes inconnues

Il faut bien fermer les portes. Dans les bâtiments dépourvus d'espace d'accueil, les collaborateurs ne doivent ouvrir la porte à des personnes étrangères à l'entreprise que s'ils se sont assurés que celles-ci sont autorisées à accéder aux locaux. Les collaborateurs doivent signaler les personnes suspectes ou les incidents à leur supérieur ou au responsable du bâtiment.

L'ordinateur dans l'espace de vente

Dans les succursales de BMS, des ordinateurs et des systèmes de caisse se trouvent en partie dans l'espace de vente, ce qui rend BMS vulnérable, car n'importe quel client ou visiteur peut potentiellement accéder à ces appareils. Il convient d'empêcher tout accès potentiel:

- en condamnant l'accès à l'appareil (Ctrl-Alt-Delete) au moment de quitter le poste de travail, même pour une courte durée;

- en faisant preuve de prudence lors de la saisie du mot de passe (s'assurer que personne d'autre disposant d'une vue dégagée sur l'écran ne se trouve à proximité immédiate);

- en s'assurant que seules des personnes qui ont accepté le règlement du personnel et la présente directive peuvent utiliser les appareils et les services de BMS;

- en prévenant tout travail non supervisé sur un PC par des visiteurs et/ou des clients, même pour de courtes recherches sur Internet.

Compte utilisateur personnel

Chaque collaborateur dispose de son propre compte utilisateur
Personne d'autre n'a le droit d'accéder à ce compte. Les collaborateurs ne doivent utiliser que leur propre compte, à l'exception des comptes utilisateur génériques, tels que ceux disponibles au comptoir de nos magasins où jusqu'à trois utilisateurs ont le droit d'utiliser le même.

Tout soupçon d'abus d'un compte utilisateur et du mot de passe correspondant par des tiers doit être immédiatement signalé au service informatique par le biais du helpdesk informatique.

Verrouillage de l'ordinateur
Il faut verrouiller l'ordinateur, même en cas de courtes absences (Ctrl-Alt-Delete). Les collaborateurs qui quittent leur poste de travail doivent se déconnecter (réunions, pauses, de midi, etc.).

Utilisation correcte du mot de passe

- Seul le collaborateur doit avoir connaissance du mot de passe associé à son compte utilisateur. Il ne doit communiquer son mot de passe à personne, pas même à son supérieur, à un agent d'assistance informatique, au helpdesk informatique, à un collaborateur des RH, etc.).

- Il doit changer de mot de passe régulièrement et au plus tard à chaque fois que le système l'y invite. Il doit choisir une combinaison entièrement nouvelle à chaque fois. Le mot de passe ne doit pas se rapporter au collaborateur lui-même, à son département ou à sa fonction.

- Le collaborateur doit le saisir lorsque personne ne l'observe. Si cela s'avère impossible, il doit le changer dès que possible.

- Il ne doit jamais le stocker sur l'appareil de BMS.

- Il ne doit jamais le consigner sur un papier qu'un tiers pourrait consulter.

Le choix d'un mot de passe efficace
Dans l'idéal, il faut choisir un mot de passe facile à retenir, mais difficile à deviner. Le collaborateur doit tenir compte des points suivants lors de son choix:

Choses à ne pas faire...

- Le mot de passe ne doit pas se rapporter au collaborateur lui-même. Les mots de passe contenant des noms de famille, des prénoms, les dates de naissances des enfants, le nom des animaux, le travail, un hobby sont faciles à deviner!

- Il vaut mieux ne pas utiliser de noms de personnalités, d'animaux, de personnages de BD, de marques de voitures, de lieux, de régions, etc.

- Il ne faut pas utiliser de termes figurant dans des dictionnaires, quelle que soit la langue.

- Il faut éviter les séquences de lettres de l'alphabet («ABCD») ou les combinaisons de touches consécutives («azerty»).

- Il ne faut jamais numéroter les mots de passe (mot-de-passe-1, mot-de-passe-2, mot-de-passe-3).

Choses à faire..

- Le mot de passe doit comporter au moins 8 lettres et chiffres.

- Le mot de passe doit contenir des minuscules et des majuscules.

- Le mot de passe doit contenir au moins un caractère spécial tel que ! ou #.

- Nous déconseillons l'utilisation des lettres suivantes qui n'existent que dans certaines langues: é à è ü ö ä ç.

- Le mot de passe doit contenir au moins un chiffre.

- Le mot de passe ne doit contenir aucun mot parlant tel que le nom de famille de l'utilisateur.

- Les cinq derniers mots de passe ne doivent pas être utilisés.

- Utiliser un moyen mnémotechnique lors du choix du mot de passe. Exemple:
  - Mot de passe initial: posteprivee
  - Majuscules/minuscules: PostEPrivee
  - Insertion de chiffres: P0stEPr1vee
  - Insertion de caractères spéciaux: P0stEPr1vee?

Obtention frauduleuse de données/Social Engineering

Les espions économiques, les hackers et d'autres personnes se font souvent passer pour quelqu'un d'autre pour pouvoir accéder aux systèmes internes en posant habilement des questions relatives aux numéros de téléphone internes, aux noms de collaborateurs, aux mots de passe ou à des informations similaires. Cette approche, appelée Social Hacking, contourne toutes les mesures de sécurité techniques et cible le maillon le plus faible de la chaîne de sécurité: l'être humain.

Faire preuve de méfiance

Le collaborateur doit vérifier l'identité de personnes inconnues qui posent des questions et leur demander de déposer leur requête par écrit s'ils cherchent à se renseigner au sujet d'une personne ou de l'entreprise. S'il semble que quelqu'un se fait passer pour un collaborateur du service informatique de BMS, il faut raccrocher le combiné et contacter immédiatement le helpdesk informatique au numéro de téléphone indiqué sur BMSmobile.

Signaler les incidents suspects

Les incidents suspects doivent être immédiatement signalés au supérieur et au helpdesk informatique.

Ordinateurs portables et autres appareils mobiles

Ne laisser aucune chance aux voleurs

Il ne faut jamais laisser traîner d'ordinateurs portables, de tablettes ou de smartphones sans surveillance. Il faut faire particulièrement attention dans les gares, à bord de trains ou dans d'autres

espaces publics. Il faut toujours transporter les ordinateurs portables dans ses bagages à main. Il faut immédiatement signaler tout vol éventuel à la police, au supérieur, au helpdesk informatique et au département Legal & Compliance.

Réservés à l'usage professionnel
Les appareils mobiles sont des instruments de travail à usage professionnel. Des tiers ne doivent pas les utiliser, pas même des amis ou des membres de la famille.

A domicile et en déplacement
Cette directive s'applique également à l'utilisation des appareils de travail mobiles indépendamment du lieu et de l'horaire, à domicile ou en déplacement.

Entrée en vigueur

Cette directive entre en vigueur le 7 juin 2021 et remplace toutes les versions antérieures de la directive informatique et les autres documents informatiques pertinents.