Politique de cybersécurité

Contexte et portée

Contexte : Sustana produit des fibres et des papiers recyclés et durables de qualité supérieure. Nous travaillons de concert avec des marques de premier plan, de grandes entreprises et les consommateurs pour créer des solutions d'emballage et d'impression haut de gamme et écologiques. Nos produits sont fabriqués à base de matières recyclées postconsommation afin de réduire au maximum leur empreinte carbone. Nos installations, nos opérations et notre main-d'œuvre, de même que la majorité de nos consommateurs et fournisseurs, sont situés aux États-Unis et au Canada.

Portée : La présente politique s'applique à Sustana, et à l'ensemble de ses filiales, de ses employés et des entités travaillant au nom de Sustana, y compris les contractants, les sous-traitants, les bénévoles et toute personne qui pourrait avoir accès, de façon temporaire ou permanente, à tout matériel informatique ou logiciel de nos systèmes, dans nos installations physiques ou dans le nuage.

Résumé et objectifs

La présente politique de cybersécurité (politique de technologies de l'information) définit les lignes directrices et les mesures prises par Sustana pour protéger son infrastructure informatique ainsi que la sécurité et la confidentialité de ses données.

Comme nous dépendons de plus en plus de la technologie pour recueillir, stocker et gérer les informations commerciales, nous sommes de plus en plus exposés aux risques informatiques, et aux atteintes à la sécurité ou à la confidentialité. Les erreurs humaines, les cyberattaques et les défaillances techniques peuvent entraîner des dommages financiers et réputationnels considérables pour notre entreprise.

Pour ces raisons, Sustana a mis en place plusieurs mesures qui jettent les bases d'un environnement informatique plus sécuritaire. Nous avons également élaboré des politiques et des instructions d'ordre général pour contribuer à réduire les menaces informatiques.

Éléments de base de la politique de cybersécurité

- Données nominatives ou confidentielles
- Politique du « bureau propre »
- Protection des appareils de l'entreprise
- Protection automatique des appareils et mesures de contrôle
- Protection des courriels
- Gestion des mots de passe
- Transfert sécuritaire des données

- Surveillance et signalement du piratage, des activités suspectes et des atteintes à la confidentialité
- Utilisation des outils d'intelligence artificielle
- Mesures de sécurité supplémentaires
- Considérations et politiques en matière de télétravail
- Gouvernance de la sécurité des employés
- Mesures disciplinaires

Informations et données nominatives ou confidentielles

Les informations et les données nominatives ou confidentielles sont précieuses et doivent être adéquatement protégées. Celles-ci comprennent notamment :

- Les informations financières ou personnelles non publiées ou confidentielles d'une entreprise ou d'une personne.
- Les données des clients, des partenaires d'affaires ou des fournisseurs.
- Les nouvelles technologies, les brevets, et les compositions ou les formules de produits.
- Les listes de clients (existants ou potentiels).
- Toute information permettant d'identifier un employé ou un membre de la direction.
- Toute information dont la publication pourrait nuire à la réputation de l'entreprise.

Tous les employés sont tenus de protéger les données informatiques et les informations de l'entreprise. Plusieurs mesures usuelles devraient être prises pour éviter de compromettre la sécurité des données. Les pirates informatiques et autres criminels sont de plus en plus organisés, et nous faisons souvent l'objet de menaces de la part du crime organisé et de pirates informatiques parrainés par l'État. De même, les menaces personnelles et les cyberattaques sont de plus en plus fréquentes, et nous avons observé de nombreux exemples de ces tendances chez nos entreprises affiliées et nos concurrents. Il est donc impératif de faire preuve de vigilance et de participer activement à la protection des données personnelles ou confidentielles auxquelles vous avez accès, qu'il s'agisse de vos renseignements personnels ou de ceux d'un client, d'un fournisseur ou d'un partenaire. En tant qu'entreprise, nous avons la responsabilité de protéger les informations nominatives, ainsi que toute donnée confidentielle que nous possédons ou stockons dans nos systèmes. La sécurité des données est une responsabilité collective, tout particulièrement en ce qui concerne la sécurité des données de tiers et de nos partenaires commerciaux.

Politique du « bureau propre »

Pour faciliter la protection des données personnelles et confidentielles, nous demandons à nos employés et aux utilisateurs de nos systèmes de ne jamais laisser de documents contenant des informations personnelles ou confidentielles à la vue, sur leur bureau ou sur l'écran de leur ordinateur.

Vos systèmes informatiques, vos ordinateurs Windows/Mac/Android, vos ordinateurs portables, vos téléphones cellulaires ou vos tablettes doivent toujours être sécurisés en mode veille ou verrouillage lorsque vous n'êtes pas présent ou que vous vous éloignez de votre bureau. Par défaut, et dans la mesure du possible, notre politique force vos systèmes à se verrouiller ou à se mettre en veille après 10 minutes d'inactivité.

Protection des appareils de l'entreprise

Les employés ne sont pas autorisés à utiliser leurs appareils numériques personnels pour accéder aux courriels ou aux systèmes de l'entreprise. L'accès aux courriels et à d'autres systèmes tels que MS Teams à l'aide d'un appareil personnel n'est autorisé qu'avec l'approbation préalable de la direction et du service informatique, et uniquement à l'aide des méthodes sécurisées recommandées par ce dernier.

Nous vous recommandons fortement de protéger les ordinateurs, les tablettes et les cellulaires appartenant à l'entreprise à l'aide des méthodes suivantes (les mêmes précautions s'appliquent à tout appareil personnel autorisé par l'entreprise) :

- Protégez vos appareils à l'aide d'un mot de passe; Sustana assure une gestion sécurisée des mots de passe.
- Ne laissez jamais vos appareils exposés ou sans surveillance.
- Installez les mises à jour de sécurité des navigateurs. Sustana exige la mise à jour obligatoire des appareils; vous pouvez toutefois choisir le moment d'installation.
- Utilisez toujours des réseaux sécurisés et des méthodes de cryptage pour vous connecter à vos comptes. Sustana exige la connexion à un réseau privé virtuel (VPN) et l'authentification multifactorielle pour tous les accès à distance aux systèmes de l'entreprise.

Nous vous déconseillons fortement d'accéder aux systèmes de l'entreprise et aux comptes internes à l'aide d'appareils tiers, et de prêter vos propres appareils à qui que ce soit.

Ne rechargez jamais votre cellulaire à l'aide du port USB de votre ordinateur; veuillez plutôt utiliser les prises électriques fournies par l'entreprise.

Il est interdit d'installer ou d'utiliser tout logiciel ou matériel informatique non autorisé ou non destiné à un usage professionnel sur un appareil appartenant à l'entreprise.

Protection automatique des appareils

Tous les appareils utilisés à des fins professionnelles, qu'ils soient fournis par l'entreprise ou qu'ils vous appartiennent, doivent être équipés du logiciel standard de sécurité de l'entreprise, qui sera fourni et installé automatiquement lors de la première connexion aux réseaux de l'entreprise.

Certaines restrictions concernant l'installation de logiciels ou de matériel peuvent s'appliquer pour les systèmes fournis par l'entreprise, et certaines mises à jour de sécurité s'appliqueront régulièrement et automatiquement. Si vous recevez un message vous demandant d'accepter la mise à jour automatique de votre système informatique, vérifiez que le message provient d'une source fiable avant de confirmer. Les mises à jour automatisées de notre système n'exigent jamais la saisie d'un mot de passe ou d'informations personnelles. Vous pouvez reporter une mise à jour automatique uniquement si le moment ne vous convient pas. Si vous désirez installer sur tout appareil appartenant à l'entreprise un logiciel ou du matériel informatique qui n'a pas été préalablement approuvé, veuillez communiquer avec notre service des TI et en faire la demande officielle sur le portail d'assistance informatique ou par un appel à la ligne d'assistance informatique.

Protection des courriels

Aujourd'hui, les courriels indésirables, les tentatives d'hameçonnage et les liens vers des logiciels malveillants (les vers informatiques, par exemple) sont de plus en plus communs. Pour éviter d'infecter vos appareils informatiques et, éventuellement, le réseau de l'entreprise, nous vous demandons de faire preuve de vigilance :

- Évitez d'ouvrir des pièces jointes ou de cliquer sur des liens HTML lorsque le contenu n'est pas explicitement décrit, et vérifiez toujours l'adresse électronique réelle de l'expéditeur plutôt que son nom affiché (par exemple, un objet semblable à <regardez cette vidéo incroyable> est douteux).
- Méfiez-vous des titres et des liens accrocheurs (par exemple, une offre de prix, un conseil ou un téléchargement gratuit).
- Vérifiez toujours la provenance des courriels (@nom de domaine) et assurez-vous de reconnaître le nom de l'expéditeur.
- Recherchez les incohérences rédactionnelles (par exemple, des fautes d'orthographe, une mauvaise utilisation des majuscules ou un nombre excessif de points d'exclamation).
- Signalez tout courriel suspect au service des TI par courriel, à l'aide de l'option « Cyber incident » du portail d'assistance informatique en ligne, ou par téléphone, à l'aide de la ligne d'assistance informatique.
- Les employés ne sont pas autorisés à utiliser la messagerie textuelle (SMS) dans le cadre de leurs activités professionnelles.

En cas de doute quant à la légitimité d'un courriel, veuillez vous adresser à l'équipe des TI.

Programme de sensibilisation à la cybersécurité

De temps à autre, vous pourriez recevoir des courriels ou des appels non sollicités provenant de la plateforme de sensibilisation à la cybersécurité de notre service des TI. Ces tests seront réalisés régulièrement en cours d'année afin d'évaluer et de renforcer notre capacité collective à gérer l'hameçonnage informatique et vocal. Il s'agit de simulations d'incidents réels qui se produisent couramment dans l'industrie. Cette initiative vise à mesurer notre degré collectif de sensibilisation aux menaces courantes qui circulent en ligne, sur les médias sociaux et dans les réseaux d'entreprise.

Après ces évaluations, le service des TI de Sustana proposera des formations et un encadrement ciblés en matière de cybersécurité. Il se peut que nous vous proposions d'améliorer vos compétences dans le cadre de l'un de ces programmes parrainés par l'entreprise.

Gestion sécuritaire des mots de passe

Les fuites de mots de passe sont courantes au sein de toutes les organisations. Celles-ci peuvent être hautement dommageables pour l'entreprise, voire compromettre l'ensemble de notre infrastructure informatique. Les mots de passe doivent non seulement être sécurisés afin de prévenir le piratage, mais doivent également demeurer secrets et afficher un degré minimum de complexité. Pour ces raisons, nous demandons à nos employés de respecter les règles suivantes :

- Choisissez un mot de passe comptant au moins 12 caractères, dont au moins 3 figurent parmi les catégories suivantes : lettres majuscules, lettres minuscules, chiffres et symboles. Évitez les mots de passe faciles à deviner, tels que votre date de naissance ou le nom de votre animal de compagnie.
- Modifiez vos mots de passe au moins une fois par année. Sustana pourrait avoir des exigences plus rigoureuses (p. ex. tous les 90 jours pour les systèmes principaux).
- Évitez d'entrer vos identifiants de connexion aux systèmes et aux réseaux de l'entreprise à partir d'un réseau public, et assurez-vous toujours que personne ne regarde par-dessus votre épaule.
- N'approuvez jamais une demande de connexion ou d'ouverture de session sur l'application Microsoft Authenticator si vous n'en avez pas fait la demande vous-même. Si vous êtes responsable d'approuver les connexions au nom d'un fournisseur externe ou d'un partenaire avec lequel vous travaillez pour lui permettre de se connecter à nos systèmes à distance, assurez-vous d'abord que la demande provient bel et bien de la personne autorisée. En cas de doute, appelez la personne pour vous assurer de la validité de la demande de connexion.

Transfert sécuritaire des données

Le transfert des données commerciales comprend toujours un certain degré de risque sécuritaire. Les employés qui transfèrent des données doivent suivre les règles suivantes :

- Aucune information confidentielle ne doit être transmise à l'extérieur de l'entreprise ni à aucune adresse courriel privée. Le transfert d'informations confidentielles à un tiers via des canaux sécurisés n'est autorisé que sur approbation de la direction.
- Utilisez uniquement les outils de partage et de transfert approuvés par l'entreprise (p. ex. Keeper Security Vault) pour le transfert de données vers d'autres appareils ou des comptes ou des systèmes externes, tout particulièrement s'il s'agit de données nominatives ou confidentielles (p. ex. les informations relatives aux clients ou les fichiers des employés). Le recours à des services de transfert externes, tels que Dropbox, Box, ou autre doit être préalablement approuvé par le service des TI, et sera traité au cas par cas.
- Lors du partage de données, et tout particulièrement de données confidentielles, utilisez toujours les réseaux de l'entreprise plutôt qu'un réseau WiFi, un réseau public, ou même une connexion privée externe sans mesures de sécurité supplémentaires fournies par le service des TI (par exemple, un VPN ou l'authentification multifactorielle).
- Assurez-vous toujours que le destinataire des données (qu'il s'agisse d'une personne ou d'une organisation) est dûment autorisé à les recevoir, et qu'il dispose de mesures de sécurité et de protection des données adéquates.
- Évitez d'envoyer tout contenu sensible par courriel; optez plutôt pour un lien de partage sécurisé et crypté.
- N'envoyez jamais d'identifiants ni de mots de passe par courriel.
- En cas de doute, communiquez avec le service des TI, qui pourra vous fournir la formation et les outils nécessaires.

Signalement des tentatives de fraude ou de piratage, et de la divulgation d'informations privées

Afin de protéger notre infrastructure informatique collective, veuillez informer le service des TI de toute tentative de fraude, d'hameçonnage, de violation de la vie privée ou de l'utilisation du réseau de l'entreprise, ou de tout soupçon de contamination par un logiciel malveillant. Veuillez informer le service des TI dès que vous estimez que la sécurité, l'intégrité ou la confidentialité de vos données ont été compromises. Notre service des TI mènera rapidement une enquête afin de détecter toute menace réelle, d'y remédier et, si nécessaire, d'envoyer des alertes appropriées à l'échelle de l'entreprise.

Nos spécialistes de la sécurité peuvent vous conseiller sur les meilleurs moyens de détecter et d'éliminer les courriels frauduleux, les logiciels malveillants et les vers informatiques. Nous vous invitons à communiquer avec eux pour toute préoccupation ou question relative à la cybersécurité.

Mesures supplémentaires

Pour réduire la possibilité de brèches de sécurité informatique, nous demandons à tous les employés de :

- Mettre leur écran en mode veille ou verrouillage lorsqu'ils s'éloignent de leur bureau.
- Signaler tout vol de matériel informatique ou tout dommage à celui-ci au service des TI.
- Changer tous leurs mots de passe en cas de vol d'un appareil.
- Signaler toute menace perçue ou toute faille de sécurité possible dans les systèmes d'entreprise.
- Ne jamais installer tout logiciel suspect, illégal ou non approuvé sur l'équipement de l'entreprise ou sur ses systèmes informatiques virtuels ou non virtuels.
- Ne jamais accéder à des sites suspects, illégaux ou non autorisés.
- Signaler toute activité suspecte dans leur région.

Les employés ne doivent, en aucun cas, mener des activités ou se comporter sur les réseaux de l'entreprise de manière qui pourrait nuire directement ou indirectement à la disponibilité ou à la performance des ressources informatiques de l'entreprise. Ces activités comprennent notamment l'envoi de courriels non professionnels (p. ex. des chaînes de courriels), l'abonnement à un nombre excessif de listes de diffusion personnelles non liées à l'entreprise, les jeux en ligne, le visionnement de vidéos ou de chaînes de diffusion en continu non liées à l'entreprise, l'utilisation de réseaux ou d'ordinateurs poste à poste, ou toute autre activité susceptible d'entraîner un trafic excessif sur le réseau ou une activité informatique inhabituelle. Nos professionnels des TI surveillent le trafic du réseau de l'entreprise en permanence. L'accès à sites web interdits ou la pratique d'activités interdites pourraient vous exposer à des comportements illégaux ou non autorisés.

Utilisation des outils d'intelligence artificielle

Les outils d'intelligence artificielle (IA) comme ChatGPT et autres peuvent ajouter de la valeur à votre travail, lorsqu'ils sont utilisés adéquatement. Lors de l'utilisation d'outils d'IA, assurez-vous de n'entrer aucune information confidentielle; seules les informations de Sustana publiquement accessibles

peuvent être utilisées. Gardez à l'esprit que les informations privées ou confidentielles deviennent publiques une fois qu'elles sont entrées dans un outil d'IA.

Télétravail

Les employés qui sont autorisés à travailler à distance doivent se conformer à tous les règlements définis dans la présente politique. Lorsqu'ils accèdent aux comptes ou aux systèmes de l'entreprise à distance, les employés doivent respecter toutes les règles de cryptage et de protection des données, et s'assurer d'utiliser des réseaux sécurisés et privés. La connexion aux réseaux de l'entreprise à distance doit toujours se faire à l'aide d'une configuration VPN. L'accès doit être approuvé par votre supérieur direct ou un membre de la direction, et la connexion doit être protégée par l'une des méthodes d'authentification multifactorielle approuvées par l'entreprise.

Votre supérieur ou le service des TI pourront vous fournir des conseils et de plus amples informations à ce sujet.

Ne jamais négliger la sécurité

Nos clients, nos partenaires, nos employés et nos sous-traitants doivent pouvoir compter sur le respect de protocoles et de mesures de pointe, qui garantissent la sécurité des données personnelles ou confidentielles qu'ils nous confient. La seule façon de mériter leur confiance est de protéger nos systèmes et nos bases de données par des procédés et des technologies de pointe. Tous les employés peuvent y contribuer en faisant preuve de vigilance et en faisant de la sécurité une priorité dans l'exercice de leurs activités professionnelles usuelles.

Mesures disciplinaires

La violation de la présente politique pourrait entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement de l'employé. Les violations involontaires peuvent faire l'objet d'un simple avertissement verbal, tandis que les violations fréquentes de même nature pourraient donner lieu à un avertissement formel par écrit. Les violations intentionnelles pourraient conduire à la suspension de l'employé ou à l'annulation de son contrat de travail, selon les circonstances propres à chaque cas.

Signalement

Toute violation de la présente politique et toute préoccupation ou question à son sujet devraient être communiquées par l'intermédiaire des canaux appropriés dans les plus brefs délais au service des TI ou à la direction de Sustana.

Gouvernance

La présente politique a été révisée par le vice-président des technologies de l'information, et est soutenue et approuvée par le chef de la direction, le chef commercial et le chef des ressources humaines de Sustana. Le vice-président des technologies de l'information la révisera sur une base

annuelle afin d'améliorer continuellement nos initiatives de cybersécurité à la lumière des leçons tirées, des dernières connaissances et des pratiques exemplaires.

Communication et transparence

La présente politique devra être accessible au public sur le site web de Sustana et transmise à tous les employés.

Avis juridique

Sustana se réserve le droit de modifier la présente politique à sa discrétion. Les politiques mises à jour seront diffusées en temps opportun.

Date d'entrée en vigueur : 1er août 2023

Contrôle du document

La présente politique doit être revue et approuvée par le Comité ESG sur une base annuelle.

Mesure	Révisions majeures et commentaires (le cas échéant)	Version et date
Première édition	Première version rédigée par le vice-président des technologies de l'information, et révisée par le chef de la direction, le chef commercial et le chef des ressources humaines.	Version 1.0, 1er août 2023

Fabian de Armas
Président et chef de la direction, Sustana

Par la présente, je reconnais avoir lu, compris et accepté les mesures et les règlements de cybersécurité du Sustana, tel qu'ils sont contenus et définis dans le présent document (version 1.0, en date du 1er août 2023).

_____ _____

Signature Date (JJ-MM-AAAA)

_____

Nom (en lettres majuscules)