Vous envisagez de mettre en place un programme « Apportez votre propre appareil » (AVPA)? Conseils utiles

1 Obtenez l'appui de la haute direction pour protéger les renseignements personnels dans le cadre du programme AVPA

En recevant l'aval de la haute direction, vous vous assurerez d'obtenir les ressources nécessaires pour planifier et mettre en œuvre avec succès un programme AVPA permettant de protéger les renseignements personnels.

2 Évaluez les risques d'atteinte à la vie privée

Effectuez une évaluation des facteurs relatifs à la vie privée avant d'adopter le programme en vue de cerner, hiérarchiser et atténuer les risques associés à la collecte, à l'utilisation, à la communication, au stockage et à la conservation de renseignements personnels, et de vous aider à déterminer si les bénéfices d'un programme AVPA sont plus importants que les risques pour votre organisation.

3 Élaborez une politique d'AVPA

Une politique d'AVPA devrait régir les utilisations acceptables des appareils; la surveillance exercée par l'organisation; le partage des appareils avec la famille/les amis; la gestion des applications; l'accès aux serveurs de l'organisation; ainsi que la responsabilité des fonctions de sécurité et des forfaits données-voix.

4 Faites un projet pilote

Avant de lancer votre programme AVPA dans toute l'organisation, faites-en l'essai avec quelques employés choisis et avec une seule plateforme mobile pour commencer.

5 Formez le personnel

Élaborez du matériel de formation et assurez-vous que les utilisateurs comprennent votre politique d'AVPA et que les professionnels des TI sont prêts à la mettre en œuvre, ainsi que tous les contrôles techniques de sécurité appropriés qui en découlent.

6 Faites preuve de responsabilité

Les défis propres à un programme AVPA nécessitent une approche exhaustive et globale pour protéger les renseignements personnels et les autres données sur tous les appareils mobiles sur le réseau. Envisagez de mettre en œuvre un logiciel de gestion des appareils mobiles et des outils axés sur les rôles dans le cadre de vos contrôles en matière de vie privée et de sécurité. Rendre des comptes, cela signifie également être prêt à montrer aux employés, aux citoyens et aux organismes de réglementation que votre programme est conforme aux lois et aux politiques de protection de la vie privée applicables.

7 Atténuez les risques grâce à la conteneurisation

Envisagez de segmenter les appareils pour séparer les applications approuvées et les données de l'organisation de celles de nature personnelle. Les entreprises devraient pouvoir effacer à distance et en toute sécurité le conteneur où est stockée leur information si un appareil est perdu ou volé ou si un employé quitte l'organisation.

8 Mettez en place des politiques de stockage et de conservation

Par exemple, envisagez d'utiliser un système de TI « client léger », afin que les employés puissent uniquement afficher sur leurs appareils les renseignements personnels se trouvant sur le serveur de l'organisation, mais non les y stocker.

9 Chiffrez les appareils et les communications

À tout le moins, utilisez les algorithmes de chiffrement standard et à jour de l'industrie pour les communications entre deux appareils. Lorsqu'un appareil est connecté au réseau de l'organisation, l'accès devrait se faire au moyen d'une connexion sécurisée, par exemple sur un réseau privé virtuel.

10 Prémunissez-vous contre les faiblesses logicielles

Songez à gérer les mises à jour logicielles de manière centralisée pour faire en sorte que les systèmes soient à jour et protégés contre les activités malveillantes.

11 Gérez les applications efficacement

Fournissez une liste des applications approuvées qui peuvent être installées, ainsi qu'une politique sur comment les applications devraient être installées, mises à jour et effacées. Souvenez-vous : une application mal configurée peut entraîner une fuite de données ou une communication non autorisée de renseignements personnels.

12 Adoptez des pratiques efficaces en matière d'authentification et d'autorisation

Songez à adopter un système d'authentification solide et géré de façon centralisée pour authentifier les utilisateurs et les appareils mobiles qui se connectent au réseau de l'organisation. Cela inclut tous ceux qui cherchent à avoir accès au conteneur d'entreprise d'un appareil mobile ou à brancher leur appareil au serveur d'entreprise.

13 Veillez à vous protéger contre les maliciels

Faites en sorte que votre sécurité soit régulièrement vérifiée, testée et mise à jour pour empêcher des attaques par maliciels sur les appareils mobiles. Les participants au programme AVPA devraient savoir réduire les risques en évitant de cliquer sur des liens suspects et de lire des messages textes louches, et en faisant preuve de bon jugement lorsqu'ils choisissent de consulter des sites Web.

14 Établissez un plan au cas où les choses tourneraient mal

Ayez un processus de gestion des incidents en bonne et due forme énonçant clairement les attentes et les responsabilités afin que les incidents liés à la sécurité ou les atteintes à la vie privée soient détectés, circonscrits, déclarés, examinés et corrigés rapidement et selon une approche uniforme. Tenez à jour une liste des appareils mobiles et des applications autorisés dans le cadre du programme AVPA. Cette liste est particulièrement utile pour atténuer les dommages en cas de perte ou de vol d'un appareil.

Commissariat à la protection de la vie privée du Canada

Office of the Information and Privacy Commissioner of Alberta

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.