Politique d'accès à distance

CIO sur demande

Présentée à

Politique d'accès à distance

Pour utiliser ce modèle, remplacez simplement le texte en gris foncé par des informations personnalisées pour votre organisation. Une fois terminé, supprimez tout le texte d'introduction ou d'exemple et convertissez tout le texte restant en noir avant la distribution.

Propriétaire de la politique	Nommez la personne / le groupe responsable de la gestion de cette politique.
Approbateur (s) de la politique	Nommez la personne / le groupe responsable de l'approbation de la mise en œuvre de cette politique.
Politiques connexes	Nommez d'autres politiques d'entreprise connexes à l'intérieur ou à l'extérieur de ce manuel.
Procédures associées	Nommez d'autres procédures d'entreprise connexes à l'intérieur ou à l'extérieur de ce manuel.
Emplacement de stockage	Décrivez l'emplacement physique ou numérique des copies de cette politique.
Date effective	Indiquez la date à laquelle cette politique est entrée en vigueur.
Date de la prochaine révision	Indiquez la date à laquelle cette politique doit être revue et mise à jour.

Objectif

Décrivez les facteurs ou les circonstances qui rendent obligatoire l'existence de la politique. Indiquez également les objectifs de base de la politique et ce qu'elle est censée atteindre.

Le but de cette politique est de définir des normes, des procédures et des restrictions pour la connexion aux réseaux internes de [nom de l'entreprise] à partir d'hôtes externes via la technologie d'accès à distance, et / ou pour l'utilisation d'Internet à des fins commerciales via un tiers fournisseurs de services Internet sans fil (également appelés «points d'accès sans fil»). Les ressources de [nom de l'entreprise] (c'est-à-dire les données d'entreprise, les systèmes informatiques, les réseaux, les bases de données, etc.) doivent être protégées contre toute utilisation non autorisée et / ou attaque malveillante pouvant entraîner une perte d'informations, des dommages aux applications critiques, une perte de revenus, et des dommages à notre image publique. Par conséquent, tous les privilèges d'accès à distance et mobiles pour les employés de [nom de l'entreprise] vers les ressources de l'entreprise - et pour l'accès Internet sans fil via des hotspots - doivent utiliser uniquement des méthodes approuvées par l'entreprise.

Portée

Définissez à qui et à quels systèmes cette politique s'applique. Énumérez les employés requis pour se conformer, ou indiquez simplement «tous» si tous doivent se conformer. Indiquez également des exclusions ou des exceptions , à savoir les personnes, les éléments , ou des situations qui ne sont pas couvertes par la présente politique ou si une attention particulière peut être faite.

Cette politique s'applique à tous les employés de [nom de l'entreprise], y compris le personnel à temps plein, le personnel à temps partiel, les sous-traitants, les indépendants et les autres agents qui utilisent des ordinateurs personnels ou appartenant à l'entreprise pour accéder à distance aux données et aux réseaux de l'organisation. L'emploi chez [nom de l'entreprise] ne garantit pas automatiquement l'octroi de privilèges d'accès à distance.

Tous les travaux effectués pour [nom de l'entreprise] sur lesdits ordinateurs par tous les employés, via une connexion d'accès à distance de toute nature, sont couverts par cette politique. Le travail

peut comprendre (mais sans s'y limiter) la correspondance par courrier électronique, la navigation sur le Web, l'utilisation des ressources intranet et toute autre application d'entreprise utilisée sur Internet. L'accès à distance est définie comme toute connexion au réseau et/ou autres applications de [nom de l'entreprise] à partir d' emplacements hors site, comme la maison de l'employé, une chambre d'hôtel, aéroports, cafés, bureau satellite, les appareils sans fil, etc.

Définitions

Définir les termes clés, acronymes, ou des concepts qui seront utilisés dans la politique. Une approche standard du glossaire est suffisante.

Lois et règlements applicables

Le cas échéant, énumérez toutes les lois ou réglementations qui régissent la politique ou auxquelles la politique doit se conformer. Confirmez auprès du service juridique que la liste est complète et exacte. S'il n'y a aucune loi ou réglementation applicable, supprimez cette section.

Énoncés de la politique

Décrivez les règles qui composent la politique. Cela prend généralement la forme d'une série de courtes déclarations prescriptives et proscriptives. Il peut être nécessaire de subdiviser cette section en sous-sections en fonction de la longueur ou de la complexité de la politique.

Il est de la responsabilité de tout employé de [nom de l'entreprise] disposant de privilèges d'accès à distance de s'assurer que sa connexion d'accès à distance reste aussi sécurisée que l' accès au réseau au sein du bureau. Il est impératif que toute connexion d'accès à distance utilisée pour mener des activités [nom de l' entreprise] soit utilisée de manière appropriée, responsable et éthique. Par conséquent, les règles suivantes doivent être respectées:

1. Les employés utiliseront des procédures d'accès à distance sécurisées. Cela sera appliqué par le biais de mots de passe forts chiffrés à clé publique / privée conformément à la politique de mot de passe de [nom de l'entreprise]. Les employés conviennent de ne jamais divulguer leurs mots de passe à quiconque, en particulier aux membres de la famille si le travail professionnel est effectué à domicile.

2. Tous les équipements et appareils informatiques distants utilisés à des fins commerciales, qu'ils soient personnels ou privés, doivent afficher des mesures de sécurité physiques raisonnables. Les ordinateurs ont installé tous les logiciels antivirus est jugé nécessaire par [nom de la société] de service informatique.

3. Les utilisateurs distants qui utilisent des points d'accès publics pour accéder à Internet sans fil doivent utiliser pour leurs appareils un pare-feu personnel, un VPN et toute autre mesure de sécurité approuvés par l'entreprise jugés nécessaires par le service informatique. Les VPN fournis par le fournisseur de services sans fil doivent également être utilisés, mais uniquement conjointement avec les mesures de sécurité supplémentaires de [nom de l'entreprise].

- Les points d'accès et les utilisateurs distants doivent déconnecter les cartes sans fil lorsqu'elles ne sont pas utilisées afin d'atténuer les attaques des pirates, des gardiens et des écoutes indiscrètes.
- Les utilisateurs doivent appliquer de nouveaux mots de passe à chaque voyage professionnel / personnel où les données de l'entreprise sont utilisées via un service sans fil hotspot, ou lorsqu'un appareil de l'entreprise est utilisé pour la navigation Web personnelle.

5. Toute connexion à distance (c. -à- point d'accès, RNIS, relais de trames, etc.) qui est configuré pour accéder à [nom de l'entreprise] doit se conformer aux exigences d'authentification de [nom de la société]. En outre, toutes les configurations de sécurité matérielle (personnelles ou appartenant à l'entreprise) doivent être approuvées par le service informatique de [nom de l'entreprise].

6. Les employés, les sous-traitants et le personnel temporaire n'apporteront aucune modification d'aucune sorte à la connexion d'accès à distance sans l'approbation expresse du service informatique de [nom de l'entreprise]. Cela inclut, mais sans s'y limiter, le tunneling fractionné, les configurations matérielles ou de sécurité non standard, etc.

7. Les employés, les sous-traitants et le personnel temporaire disposant de privilèges d'accès à distance doivent s'assurer que leurs ordinateurs ne sont pas connectés à un autre réseau lorsqu'ils sont connectés au réseau de [nom de l'entreprise] via un accès à distance, à l'exception évidente de la connectivité Internet.

8. Afin d'éviter la confusion entre les affaires officielles de l'entreprise avec des communications personnelles, les employés, les entrepreneurs et le personnel temporaire avec privilège d'accès à distance ne doit jamais utiliser d'autres comptes de messagerie (Gmail, Yahoo, etc.) pour la conduite des affaires de [nom de l'entreprise].

9. Aucun employé ne doit utiliser l'accès à Internet via les réseaux de l'entreprise à des fins de transactions illégales, de harcèlement, d'intérêts de concurrents ou de comportements obscènes, conformément aux autres politiques existantes des employés.

10. Conformément aux politiques de sécurité de [nom de l'entreprise], les sessions d'accès à distance expireront après […] minutes d'inactivité et se termineront après […] heures de connexion continue. Les deux délais d'expiration obligeront l'utilisateur à se reconnecter et à s'authentifier à nouveau pour entrer à nouveau dans les réseaux de l'entreprise. Si le compte d'un utilisateur distant est inactif pendant une période de […] jours, les privilèges d'accès au compte seront suspendus jusqu'à notification au service informatique.

11. Si un ordinateur appartenant à une personne ou à une entreprise ou un équipement connexe utilisé pour l'accès à distance est endommagé, perdu ou volé, l'utilisateur autorisé devra immédiatement en informer son responsable et le service informatique de [nom de l'entreprise].

12. L'utilisateur d'accès à distance s'engage également à signaler immédiatement à son responsable et au service informatique de [nom de l'entreprise] tout incident ou incident suspecté d'accès non autorisé et/ou de divulgation des ressources, bases de données, réseaux, etc. de l'entreprise.

13. L'utilisateur d'accès à distance accepte que son accès et/ou sa connexion aux réseaux de [nom de l'entreprise] puisse être surveillé afin d'enregistrer les dates, heures, durée d'accès, etc., afin d'identifier les modèles d'utilisation inhabituels ou autre activité suspecte. Comme pour les ordinateurs internes, cela est fait afin d'identifier les comptes / ordinateurs qui peuvent avoir été compromis par des parties externes.

14. [Nom de l'entreprise] [remboursera / ne remboursera pas] les employés pour les connexions d'accès à distance liées à l'entreprise effectuées sur un service Internet privé. Toutes les demandes de remboursement doivent être accompagnées d'une documentation suffisante et appropriée (c.-à-d. Facture de service originale). Les employés qui demandent un remboursement seront également invités à certifier par écrit avant le remboursement qu'ils n'ont pas utilisé la connexion d'une manière contraire à la politique de l'entreprise.

Procédures pertinentes

Envisagez de créer des documents de procédure officiels qui renforcent et soutiennent les déclarations de politique ci-dessus. Remarque, il est recommandé de conserver les politiques et procédures dans des documents séparés afin de garder le contenu concentré et réduire le nombre de fois que la politique doit être approuvée de nouveau par la haute direction.

- Tous les employés qui nécessitent l'utilisation de l'accès à distance à des fins commerciales doivent suivre un processus de demande qui explique clairement pourquoi l'accès est requis et de quel niveau de service l'employé a besoin si sa demande est acceptée. Les formulaires de demande doivent être approuvés et signés par le chef d'unité, le superviseur ou le chef de service de l'employé avant d'être soumis au service informatique.

- Les employés peuvent utiliser des connexions privées (sous « Technologie prise en charge ») à des fins commerciales. Si tel est le cas, le service informatique doit approuver la connexion comme étant sécurisée et protégée. Cependant, le service informatique de l'entreprise ne peut pas et ne prendra pas techniquement en charge une connexion Internet tierce ou une connexion sans fil hotspot. Tous les formulaires de dépenses pour le remboursement des coûts (le cas échéant) engagés en raison de l'accès à distance à des fins commerciales (c'est-à-dire les frais de connectivité Internet) doivent être soumis au chef d'unité ou de département approprié. Le remboursement financier de l'accès à distance n'est pas à la charge du service informatique.

Non-conformité

Décrivez clairement les conséquences (juridiques et / ou disciplinaires) du non-respect par l'employé de la politique. Il peut être pertinent de décrire le processus d'escalade en cas de non-conformité répétée.

Les violations de cette politique seront traitées comme les autres allégations d'actes répréhensibles à [nom de l'entreprise]. Les allégations de faute seront jugées conformément aux procédures établies. Les sanctions pour non-conformité peuvent inclure, mais sans s'y limiter, un ou plusieurs des éléments suivants:

1. Action disciplinaire conformément aux politiques [nom de l'entreprise] applicables ;
2. Cessation d'emploi; et / ou
3. Action en justice conformément aux lois applicables et aux accords contractuels.

Accord

Inclure une section qui confirme la compréhension et l'accord de se conformer à la politique. Les signatures et les dates sont obligatoires. Un exemple de déclaration est fourni ci-dessous.

J'ai lu et compris le [nom de l'entreprise]. Je comprends que si j'enfreins les règles expliquées dans le présent document, je peux faire l'objet de poursuites judiciaires ou disciplinaires conformément aux lois applicables ou à la politique de l'entreprise.

_____
Nom de l'employé

_____
Date de signature de l'employé

Historique des révisions

ID de version	Date de changement	Auteur	Commentaires