Politique de télétravail

CIO sur demande

Présentée à

Contents

Titre : Politique de télétravail en cas de crise

1. Objectifs

Décrire 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.

Cette politique de télétravail en cas d'urgence (ci-après la «politique») soutient le mandat de [nom de l'organisation] pour un plan de travail à distance en cas d'urgence, un programme visant à soutenir la gestion des crises de [nom de l'organisation] et la résilience aux perturbations commerciales. [Nom de l'organisation] prendra les mesures appropriées pour minimiser et gérer l'impact des événements perturbateurs en maintenant la continuité des activités sous forme de travail à distance. À la discrétion de [nom de l'organisation], cette politique entrera en vigueur immédiatement et restera en vigueur jusqu'à ce qu'elle soit remplacée par [soit un plan de continuité des activités à plus long terme, soit la résiliation totale de la politique].

La politique a les objectifs suivants :

- Améliorer la résilience de [nom de l'organisation] contre la perturbation de sa capacité à atteindre ses objectifs [commerciaux ou de service] clés.
- Offrir des capacités éprouvées pour gérer les perturbations de l'entreprise et protéger les activités créatrices de valeur de [nom de l'organisation], telles que: [augmentation de la part de marché; générer des revenus; fournir des services clés; et protéger les intérêts des parties prenantes, leur réputation et leur image de marque].
- Restaurer la capacité de [nom de l'organisation] à livrer les processus clés à un niveau convenu dans un délai convenu après une interruption.

La politique doit être comprise comme un document évolutif, qui doit être revu, mis à jour et signé sur une base [semestrielle, annuelle, semestrielle] par [le responsable désigné du travail à distance]. Cela garantit que chaque aspect de cette politique est conforme aux pratiques actuelles de l'industrie afin que [nom de l'organisation] soit aussi raisonnablement préparé que possible pour mettre en œuvre cette politique.

La politique d'accès à distance complémente la présente politique

2. Envergure et public cible

Définir 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 toutes les exclusions ou exceptions qui sont hors de portée, c'est-à-dire les personnes, les éléments ou les situations qui ne sont pas couverts par cette politique ou où une considération particulière peut être faite.

Cette politique s'applique à l'ensemble de [nom de l'organisation], y compris toutes les filiales [locales, régionales ou mondiales], et à toute externalisation ou coentreprise conclue par [nom de l'organisation] ou ses filiales.

Les tiers, y compris les prestataires de services dont [nom de l'organisation] dépend de manière critique pour la fourniture de services, doivent être considérés comme un élément essentiel de la politique, et des dispositions d'urgence appropriées doivent être assurées au moyen d'accords contractuels garantissant la continuité des activités des parties externes dans conformément aux normes de [nom de l'organisation].

3. Définitions

Définir les termes, acronymes ou concepts clés qui seront utilisés dans la politique ou les procédures d'accompagnement. Une approche glossaire standard suffit. Exemples de définitions :

Travail à distance : L'employé exécute les tâches et les responsabilités de son poste et d'autres activités autorisées à partir d'un lieu de travail approuvé autre que l'endroit où l'employé travaillerait autrement.

Heures d'ouverture régulières : [08: 00–17: 00 (ET)] avec lunch d'une heure. Les employés doivent être accessibles au moins par téléphone et par courriel pendant les heures normales d'organisation.

Bureau à domicile : terme général qui fait référence à l'espace de travail distant désigné de l'employé. (Remarque: cet espace de travail peut ne pas se trouver littéralement au domicile de l'employé.)

Résiliation : Cette politique peut être annulée en plein effet à la discrétion de [nom de l'organisation], avec une période d'une semaine dans un plan de continuité des affaires à plus long terme ou un retour aux fonctions normales.

4. Non-conformité

Décrire 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.

5. Responsabilités

Identifier dans cette section les responsabilités des intervenant impliqués dans cette procédure. Les exemples présentés ici s'appliquent à la crise COVID19 et sont énumérés en guise de pense-bête. Ces items de responsabilités devront être revus par l'organisation

5.1.Responsabilités de l'organisation

5.1.1. Considérations pour les Ressources Humaines

- Établir des normes de sécurité physique et de sécurité pour les bureaux à domicile, en créant une enquête sur la sécurité des bureaux à domicile et/ou en mettant en place une politique d'accès à distance (impliquer le département informatique)
- Clarifier aux gestionnaires et aux employés que toutes les règles habituelles du lieu de travail sont attendues selon une norme professionnelle.
- En fonction de l'urgence, distribuez les conseils et les orientations des organismes locaux, régionaux, nationaux et mondiaux concernés aux gestionnaires et aux employés.
- Ajuster les plans de sécurité physique des immeubles de bureaux lorsqu'ils sont vides.
- Les dépenses seront remboursées pour [les activités qui relèvent habituellement des activités normales de l'employé].
- Les gestionnaires et les employés doivent signer la politique d'accès à distance (si mise en place)
- L'assurance des entreprises couvrira: [les téléphones portables; comprimés; ordinateurs portables; et d'autres équipements qui accompagnent normalement l'employé tout au long de la journée].
- L'assurance ne comprend [rien au-delà du bureau à domicile de l'employé].
- Les dépenses ne seront pas remboursées pour [les frais d'utilisation des ordinateurs privés, les coûts des services publics associés à l'utilisation du téléphone, de l'ordinateur ou de l'occupation de l'espace de travail désigné].

5.1.2. Considérations pour les affaires

- Les gestionnaires et les employés doivent remplir le sondage sur la sécurité des bureaux à domicile. L'espace de travail sera documenté avec des photos et des vidéos. Les gestionnaires distribueront l'enquête à leurs équipes.
- Mettre en place de bonnes pratiques de gestion du travail à distance en ce qui a trait aux objectifs et livrables que les employés doivent atteindre chaque jour-semaine.
- Les gestionnaires responsables de sous-traitants feront quelque chose d'équivalent et pertinent pour les sous-traitants.

5.1.3. Considérations pour le département informatique

- Fournir un système de gestion de l'utilisation des actifs informationnels [ou fournir une synchronisation de fichiers en ligne et partager un document] pour surveiller quels gestionnaires et employés prennent le matériel de bureau nécessaire.
- Assurer la liaison avec les gestionnaires afin de recueillir des informations sur les exigences nécessaires des employés pour une continuité des activités minimalement viable (matériel, logiciels et équipements non informatiques).
- Fournir l'équipement nécessaire (matériel, logiciel et non informatique) dans les [48 heures].
- Distribuez des informations sur les bonnes habitudes de sécurité (voir la section 6 de cette politique pour plus d'informations).
- Documenter les leçons apprises dans la section 7 de cette politique en prévision d'une crise future.

5.2.Responsabilités des gestionnaires

5.2.1. Considérations pour les Ressources Humaines

- Distribuer le sondage sur la sécurité du bureau à domicile aux membres de l'équipe.
- Recueillir et examiner les enquêtes sur la sécurité des bureaux à domicile et fournir des recommandations pour améliorer.
- Suivre les conseils et les orientations des organismes locaux, régionaux, nationaux et mondiaux concernés.
- Respecter toutes les règles du lieu de travail de [nom de l'organisation] conformément aux normes professionnelles attendues.

5.2.2. Considérations pour les Affaires

- Déléguer l'autorité aux membres de l'équipe pour la poursuite des projets.
- Agir comme agent de liaison entre les mandats des employeurs et les membres de l'équipe.
- Mettre en place de bonnes pratiques de gestion du travail à distance en ce qui a trait aux objectifs et livrables que les employés doivent atteindre chaque jour-semaine. S'inspirer des pratiques Agiles telles SCRUM meeting chaque matin entre les superviseurs et employés. Maintenir les réunions d'équipe et maintenir un contact quotidien avec chaque membre de l'équipe.
- Envoyer et consulter les journaux des affectations de travail à distance.

5.2.3. Considérations pour le département informatique

- Comprendre les plans d'urgence de [nom de l'organisation] ([plan de continuité des activités et plan de gestion des crises]) et les rôles de gestion dans l'exécution de ces plans.
- Collecter des informations sur le matériel nécessaire (matériel, logiciel et non informatique) requis pour que les membres de l'équipe travaillent à leur bureau à domicile.
- Signaler à l'employeur les capacités nécessaires pour une continuité d'activité minimale viable, y compris les problèmes de capacité de l'équipe concernant l'équipement (matériel, logiciel et non informatique).
- Tenir à jour le système de gestion de l'utilisation des actifs informationnels pour documenter l'équipement nécessaire qui a été retiré du bureau.
- Informer les employés sur les outils de communication/collaboration approuvés
- Fournir des informations sur les bonnes habitudes de sécurité.
- Faire des tests de pénétration ([intrusion])sur quelques postes en télétravail selon un échantillonnage basé sur des différences de configuration.

5.3.Responsabilités des employés

5.3.1. Considérations pour les Ressources Humaines

- Assurez-vous que la police d'assurance du propriétaire ou du locataire est à jour.
- Sondage complet du bureau à domicile.
- Déterminez quel équipement est couvert par la police d'assurance commerciale de [nom de l'organisation].
- Vérifiez les règles locales pour les restrictions sur l'utilisation de la propriété et pour les taxes commerciales potentielles. [L'employé est responsable des frais occasionnés par les amendes.]
- Retirez les aliments du réfrigérateur / garde-manger / bureaux, verrouillez les tiroirs / armoires de bureau et ramenez à la maison les dossiers nécessaires qui peuvent être retirés du bureau.
- Respectez toutes les règles du lieu de travail de [nom de l'organisation] conformément aux normes professionnelles attendues.
- Suivez les conseils et les orientations des organismes locaux, régionaux, nationaux et mondiaux concernés.

5.3.2. Considérations pour les Affaires

- Compléter les journaux quotidiens d'affectation de travail à distance.
- Maintenir un horaire normal dans la mesure du possible et être accessible pendant les heures normales (sauf indication contraire avec l'approbation de la direction).

5.3.3. Considérations pour le département de l'informatique

- Tenir à jour le système de gestion des actifs informationnels pour documenter l'équipement nécessaire qui a été retiré du bureau.
- Indiquer à votre supérieur immédiat les capacités nécessaires pour assurer une continuité d'activité minimale viable.
- Consulter les informations sur les bonnes habitudes de sécurité et/ou suivre la politique d'accès à distance.

6. Matériel et logiciel

6.1.Matériel

Affecté à l' informatique.

- Les appareils personnels «Bring your own» sont autorisées . Le service informatique lancera des outils de diagnostic pour que les utilisateurs les exécutent sur des appareils personnels avant leur approbation à des fins professionnelles.
- Les employés recevront les équipements de bureau nécessaires pour répondre aux besoins reliés à l'exécution de leurs tâches, notamment [casques d'écoute, câbles CAT5, cordons, moniteurs, souris, ordinateurs portables et ordinateurs de bureau] .
- Une mise à disposition du matériel nécessaire sera prête à être livré à [insérer localisation pick-up] avec des feuilles d'inscription de suivi d'utilisation
- [nom de l'organisation] a identifié [fournisseur, magasin d'informatique local , ou une combinaison] pour la fourniture d'urgence de matériel.
- Le département soutien aux utilisateurs (Help Desk) a prévu la capacité de soutenir le volume accru de problèmes d'utilisateur final.

6.2.Logiciel

Affecté à l'informatique.

- [nom de l'organisation] utilisera les outils de collaboration suivants: [outils de communication, comme Slack, Microsoft Team ou Zoom] .
- Des comptes corporatifs des versions basées sur le Web des outils de collaboration ci-dessus seront activées et vos emails professionnels doivente être utilisés pour accéder aux outils.
- Des wikis pour chaque outil de collaboration approuvé peuvent être trouvés à [insérer le lien Web] pour garantir une utilisation viable minimale.
- L'informatique Shadow sera surveillée et empêchée. Il est essentiel d'utiliser les outils spécifiés.
- Le département soutien aux utilisateurs (Help Desk) a prévu la capacité de soutenir le volume accru de problèmes d'utilisateur final.

6.3.Réseau

Affecté à l'informatique.

- Confirmer le nombre maximal d'utilisateurs qui ont besoin d'un accès à distance et traduire en bande passante supplémentaire requise.
- Optimiser la bande passante avec des technologies alternatives [telles que la compression de données] .
- Appliquer le VPN de [nom de l'organisation] à tous les utilisateurs distants.
- Gérer les surcapacités des demandes d'accès au réseau via [l'accès local, les FAI et les fournisseurs de services WAN] .
- Fournir un approvisionnement d'urgence en licences réseau et ports auprès des [fournisseurs d'équipements réseau] dans les [48 heures].
- Mettre à jour les niveaux de requis de services (SLAs) avec [fournisseurs] pour respecter les délais de livraison d'urgence.
- [Vendor] fournira une prestation de continuité des affaires infonuagique variable (Cloud base DR-as-a-service comme plan B aux composants réseau.
- Si nécessaire, [nom de l' organisation] combinera les infrastructures sur site (on-Prem) avec des composantes basées sur le cloud pour une solution hybride.

- Dans la mesure du possible, toutes les applications d'utilisateur final auront des versions Web.
- En cas de déplacement du centre informatique, [insérer l'emplacement] agira comme un emplacement informatique hors site.
- La réduction des demandes d'accès à distance nécessitera [l'examen des SLA des fournisseurs et de l'expiration des licences].
- [Des cartes Wi-Fi pour les systèmes Internet de secours seront distribuées aux employés éligibles .]
- Déterminer si le fournisseur externe de services T.I. (MSP) peut fonctionner efficacement en mode centre d'appels et selon le potentiel de croissances des appels à venir

6.4.Sécurité

Affecté à l'informatique.

- Mettre en œuvre la politique d'accès à distance
- Mettre en œuvre un processus normalisé pour traiter les situations de sécurité informatique [comme la façon de mettre en œuvre les demandes d'accès].
- Mettre en place les dispositifs de sécurité requis par les employés, tels qu'identifiés par l'enquête sur les bureaux à domicile et/ou la politique d'accès à distance
- Signalez les incidents via [insérer le nom du journal].
- Les utilisateurs finaux à haut risque pour la sécurisation des points finaux sont identifiés et hiérarchisés.
- L'utilisation du VPN est obligatoire et la procédure VPN de [nom de l'organisation] sera distribuée.
- Implémenter des zones sécurisées (DMZ) et des boîtes de saut (Jump Box) pour les informations hautement sensibles.
- Le trafic de données sera surveillé à l'aide d'analyses de comportement pour surveiller les comportements suspects.
- Les outils de sécurité sont standardisés, notamment [anti-virus, pare-feu, cryptages, gestion des correctifs et authentification multifacteur].
- Des mots de passe de connexion sécurisés seront utilisés sur tous les systèmes contenant des informations sur l'organisation.
- Des informations sur les bonnes habitudes de sécurité [comme éviter le harponnage ciblé] seront distribuées dans les [48 heures].
- Le matériel sensible contenant toutes les informations sera retourné à [emplacement du bureau] pour une manipulation ou une élimination appropriée.
- Les outils de collaboration et de communication non approuvés seront désactivés.
- Les employés sauvegardent les informations critiques toutes les [24 heures] dans [la solution de stockage désignée] OU Les employés utilisent et sauvegardent les informations critiques obligatoirement dans l'environnement documentaire infonuagique officiel [DropBox,OneDrive, Sharepoint] de [nom de l'organisation]

7. Leçons pour crises futures

Le tableau suivant doit être rempli régulièrement pour surveiller les problèmes survenus lors de la mise en œuvre du plan de travail à distance d'urgence de [nom de l' organisation]. Ces problèmes peuvent ensuite être examinés et résolus ultérieurement pour une solution plus permanente. Cette solution devrait alors être mise en politique.

Problème	Surveillé par	Résolution potentielle
Les clients ne veulent pas utiliser l' outil de collaboration approuvé de [nom de l' organisation].	P. N	Explorez l' interopérabilité avec les outils préférés des employés .
Les employés ne peuvent pas accueillir plus de 20 personnes dans une salle de conférence Web.	P. N.	Cherchez à obtenir un niveau premium pour répondre aux besoins des employés.
Un employé inéligible pour travailler dans [pays] organise à distance des ateliers dans [pays], soulevant des problèmes de travail à l'étranger et de fiscalité.	Ressources humaines	Vérifiez auprès de [avocat en commerce international] quelles règles régissent correctement cette interaction.

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.

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