GOUVERNANCE & REVUE DES ACCÈS PROTECTION DES DONNÉES D'ENTREPRISE MICROSOFT 365

GUIDE D'UTILISATION DE L'ASSISTANT PERSONNEL CARE # MY DATA SECURITY

GROUPE PASTEUR MUTUALITÉ

SOMMAIRE

1. CONTEXTE

GROUPE PASTEUR MUTUALITÉ

1. CONTEXTE (1/2)

Déploiement massif des outils collaboratifs Microsoft 365

Transformation en profondeur des usages métier

81%

DES SALARIÉS SOUHAITENT BÉNÉFICIER D'UN TABLEAU DE BORD INDIVIDUEL LEUR PERMETTANT DE SAVOIR EN TEMPS RÉEL QUI ACCÈDE À LEURS OUTILS NUMÉRIQUES

Source : Sondage IFOP 2020 « Les salariés et la sécurité de leurs données »

1. CONTEXTE (2/2)

L'absence de visibilité et de maîtrise de ces outils peut compromettre la sécurité des données d'entreprise

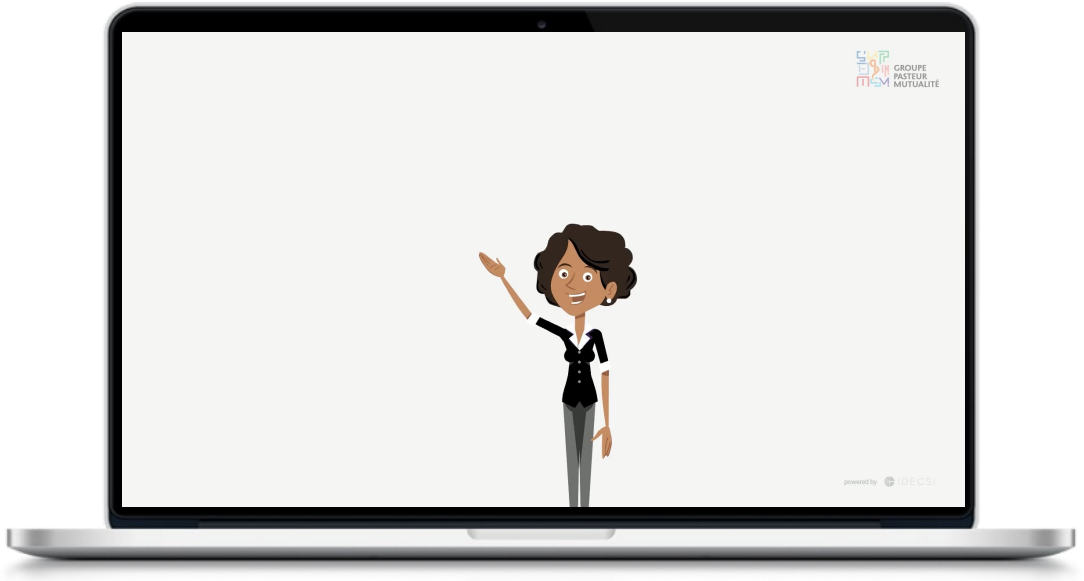
La gestion des données d'entreprise devient une réelle nécessité : maitriser, certifier les accès, les droits et les partages dans l'usage des outils collaboratifs

L'assistant personnel CARE # My Data Security va accompagner les collaborateurs à mieux détecter les anomalies sur leurs données et à faciliter la remédiation par le support informatique

2. VIDÉO # MY DATA SECURITY

GROUPE PASTEUR MUTUALITÉ

DÉCOUVREZ
MY DATA SECURITY
EN VIDÉO



2. CARE # MY DATA SECURITY

GROUPE PASTEUR MUTUALITÉ

3. CARE # MY DATA SECURITY (1/3)

Fournir un support clé en main aux utilisateurs et faciliter la compréhension des enjeux liées à l'utilisation des ressources

Apporter du sens dans la démarche de protection dans l'usage des outils collaboratifs

L'assistant personnel CARE # My Data Security met à disposition un tableau de bord et adresse des notifications aux utilisateurs en cas d'anomalie

3. CARE # MY DATA SECURITY (2/3)

Tableau de bord personnel vous permettant de suivre et de maîtriser la sécurité de vos ressources Microsoft 365 en corrigeant toutes anomalies que vous constaterez.

Notifications vous permettant de valider ou de signaler directement aux équipes de sécurité en cas de comportement anormal sur vos ressources protégées Microsoft 365

Lien de consultation : **https://care.gpm.fr**

3. CARE # MY DATA SECURITY (3/3)

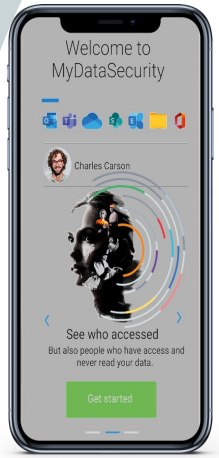


Tableau de bord personnel simple et interactif vous permettant de suivre et de maîtriser la sécurité de vos ressources Microsoft 365 Réalisation de contrôles efficaces sur vos ressources Microsoft 365

Configuration générale

Identification des pays habituels de connexion et de vos appareils synchronisés sur votre compte *(ex : 2 appareils synchronisés sur votre compte « Ipad et Iphone »)*

Boîte mail et calendrier

Identification des autorisations et des règles de configuration *(ex : transfert automatique)*

Espace de stockage personnel OneDrive

Identification des partages *(ex : partage d'un document confidentiel à des externes)*

Bibliothèques Teams et SharePoint

Identification des autorisations *(ex : collaborateurs ayant accès à une équipe Teams)*

UN DASHBOARD INTERACTIF

L'utilisateur GPM est un acteur engagé dans la sécurité à apporter sur ses propres ressources

- L'utilisateur a de la visibilité sur l'ensemble de ces données ?
- L'utilisateur a de l'information sur les droits d'accès appliqués sur ces ressources ?
- Quelles sont les données qui ont fait l'objet d'un partage ?
- Ces partages sont-ils toujours nécessaires ?
- Quelles sont les autorisations sur ma boîte mail ?
- Quels sont mes équipements mobiles synchronisés ?
- À quoi dois-je faire attention ?

Quel est le but d'une notification ?

- Permettre à un utilisateur de valider un accès inhabituel ou de signaler directement aux équipes de sécurité un comportement anormal sur sa ressource
- Notifications immédiates par e-mail permettant à l'utilisateur d'alerter les équipes de sécurité pour réagir efficacement en menant des investigations en cas d'activité suspecte

Quels sont les cas d'utilisation ?

Ma boîte mail et mon calendrier sont accessibles à des collaborateurs de l'entreprise.
Est-ce légitime ?

Un nouveau partage externe via OneDrive contenant des données sensibles, est réalisé.
Est-ce légitime ?

Je me connecte habituellement depuis la France, et il est constaté une connexion depuis la Suède.
Est-ce légitime ?

4. FOIRE AUX QUESTIONS

GROUPE PASTEUR MUTUALITÉ

FOIRE AUX QUESTIONS

FLASH CYBERSECURITE

L'accès aux applications Outlook, Teams, OneDrive, … est fondamental pour un collaborateur pour exercer son activité.
La compromission de vos identifiants est un risque réel et il en devient critique de maîtriser l'accès à vos données.
Cette foire aux questions a pour but de répondre à vos interrogations sur des éventuelles situations à risque.

Outlook : Application offrant les fonctionnalités courrier et calendrier, qui permettent d'envoyer, de recevoir et gérer des courriels. Le calendrier intégré d'Outlook permet quant à lui, de suivre les rendez-vous (*professionnels ou personnels*) et les événements.

Exemples de situations à risque : accès à votre compte Microsoft 365 par un nouvel utilisateur, faisant suite à configuration illégitime sur votre boîte (**opération d'administration, modification de permissions ou vol d'identifiants**). Ceci afin d'accéder à vos courriels ou de réaliser une campagne d'hameçonnage en interne ou à l'extérieur de l'organisation.

OneDrive : Application permettant aux collaborateurs d'accéder à des fichiers, de les partager et de collaborer :

- accès aux travaux en toute simplicité à partir de tous les appareils,
- partage rapide et collaboration intelligente à l'intérieur ou à l'extérieur de votre organisation,
- facilitation du stockage de fichiers et d'accès

Exemples de situations à risque : modification involontaire de la configuration d'un partage ou **accès à un partage anonyme** permettant à un tiers non autorisé d'accéder aux données .

PROGRAMME DE
CYBERSÉCURITÉ CARE

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

Office 365

FOIRE AUX QUESTIONS

FLASH CYBERSECURITE

L'accès aux applications Outlook, Teams, OneDrive, … est fondamental pour un collaborateur pour exercer son activité.
La compromission de vos identifiants est un risque réel et il en devient critique de maîtriser l'accès à vos données.
Cette foire aux questions a pour but de répondre à vos interrogations sur des éventuelles situations à risque.

Mode d'accès : Microsoft 365 est un espace collaboratif, accessible selon des modalités d'accès :

- accès en ligne
- accès depuis un poste de travail
- accès appareil mobile

Exemples de situations à risque : synchronisation d'un nouvel appareil mobile par un tiers ou un **accès en ligne inhabituel** permettant ainsi à un cybercriminel ou à un utilisateur malintentionné d'accéder à l'ensemble des données.

Origine des localisations : Identification des localisations (*principalement la France pour les utilisateurs de GPM*) lors d'une connexion aux outils Microsoft 365.

Exemples de situations à risque : connexion à votre compte depuis une nouvelle localisation (*Nigéria, pays d'Asie ou Russie, …*) ou **connexion simultanée** depuis diverses localisations (*France et Egypte*). Ces actions sont généralement réalisées par un cybercriminel mais peuvent être légitimes lors d'un déplacement d'un collaborateur (*exemple lors de la période estivale*).

PROGRAMME DE
CYBERSÉCURITÉ CARE

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

Office 365

FOIRE AUX QUESTIONS

FLASH CYBERSECURITE

L'accès aux applications Outlook, Teams, OneDrive, … est fondamental pour un collaborateur pour exercer son activité.
La compromission de vos identifiants est un risque réel et il en devient critique de maîtriser l'accès à vos données.
Cette foire aux questions a pour but de répondre à vos interrogations sur des éventuelles situations à risque.

Transfert automatique : Fonctionnalité permettant de transférer ou de rediriger vos messages électroniques vers une autre boîte mail (*interne ou externe à l'organisation*).

Exemple de situation à risque : transfert automatique par un cybercriminel de courriels vers une boîte externe lors d'une campagne d'hameçonnage pour effacer les traces des messages envoyés.

Faisant suite à la constatation d'une déviance par un utilisateur, quels sont les étapes que je vais devoir suivre ?
Pour rappel, une déviance peut être un accès non autorisé à votre compte, une synchronisation d'un nouvel appareil mobile ou toute autre action effectuée sur votre environnement qui ne serait pas à votre initiative.

1. **Cliquer sur le bouton Corriger :** ceci permettra de signaler la déviance
2. **Remédier :** l'équipe technique analysera la situation puis procédera à la remédiation si nécessaire pour remédier
3. **Valider le profil :** à l'issue de la remédiation globale, il sera demandé de valider votre profil afin que vous puissiez être alerté en temps réel

PROGRAMME DE
CYBERSÉCURITÉ CARE

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

Office 365

5. COMMUNICATION FLASH CYBERSÉCURITÉ

GROUPE PASTEUR MUTUALITÉ

FLASH CYBERSECURITE

ACTIVATION DU NOUVEAU DASHBOARD SUR LA PROTECTION DE VOTRE ENVIRONNEMENT MICROSOFT 365

GROUPE PASTEUR MUTUALITÉ

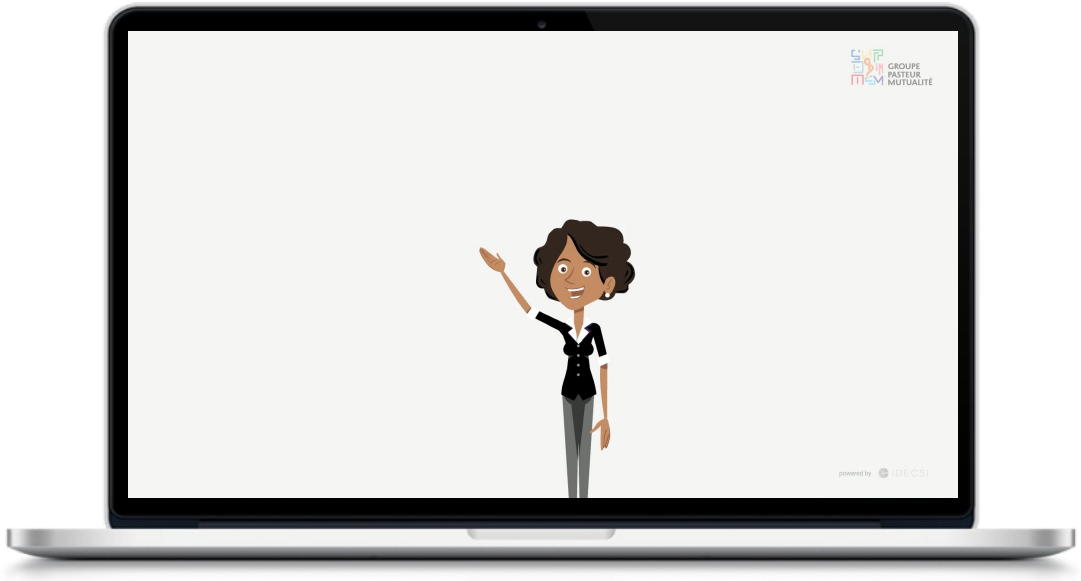
Dans le cadre de la mise en œuvre du projet de sécurisation de l'accès aux données d'entreprise, une nouvelle version interactive voit le jour. Aujourd'hui, tout le monde est concerné par la sécurité des données

En effet, grâce à votre implication, vous pourrez signaler toutes activités qui vous paraitront suspectes sur votre environnement Microsoft 365, ensuite des investigations seront menées pour s'assurer de la légitimité de ces accès.

Cette nouvelle version de protection des données, vous permettra d'être acteur de votre propre sécurité et celle de vos accès, tout en étant averti en temps réel, lors d'une situation pouvant être à risque :

Chacun peut voir ses sources de données et suivre sa sécurité

Analyser les risques qui doivent vous mettre la puce à l'oreille



PROGRAMME DE
CYBERSÉCURITÉ CARE

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

Office 365

FLASH CYBERSECURITE

ACTIVATION DU NOUVEAU DASHBOARD SUR LA PROTECTION DE VOTRE ENVIRONNEMENT MICROSOFT 365

GROUPE PASTEUR MUTUALITÉ

Dans le cadre de la mise en œuvre du projet de sécurisation de l'accès aux données d'entreprise, une nouvelle version interactive voit le jour.
En cette occasion, nous avons établi un échantillonnage chez GPM, pour effectuer un test utilisateur, afin de récolter le ressenti de nos collaborateurs.

Vous avez donc été sélectionné, pour tester cette nouvelle application qui fera de vous le garant de la sécurité de vos données mais également celle de votre entreprise.

Votre collaboration dans ce test nous sera très utile, c'est pourquoi nous vous serons très aimable de nous faire parvenir toutes vos remarques à l'adresse suivante monsupport@gpm.fr :

Voici l'adresse de la nouvelle version du tableau de bord de votre sécurité des données. https://care.gpm.fr

Chacun peut voir ses sources de données et suivre sa sécurité

Analyser les risques qui doivent vous mettre la puce à l'oreille

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

PROGRAMME DE
CYBERSÉCURITÉ CARE

Office 365

MERCI

GROUPE
PASTEUR
MUTUALITÉ