2

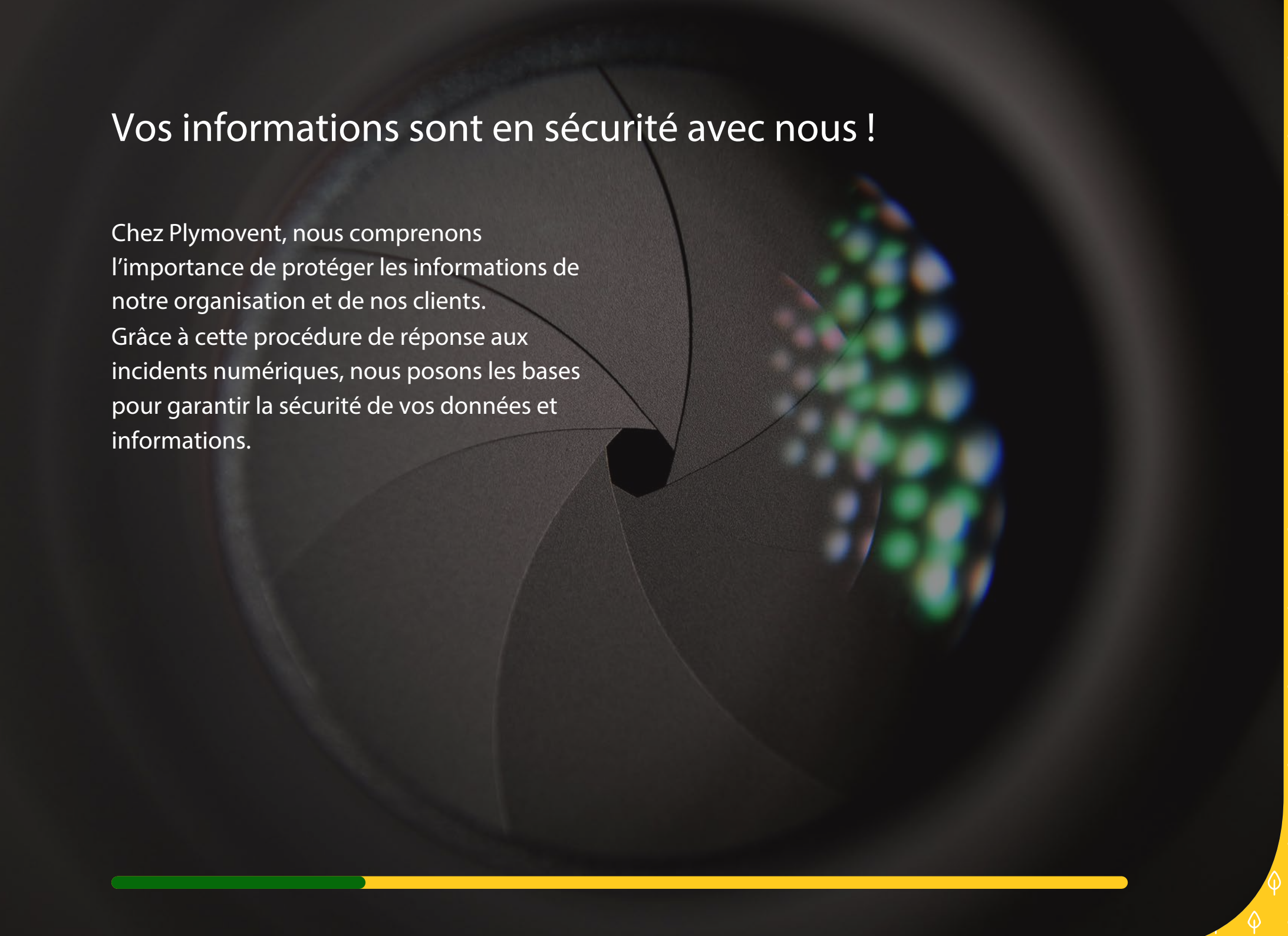
Plymovent

Procédure de réponse aux incidents numériques

PLYMOVENT®
clean air at work

Vos informations sont en sécurité avec nous !

Chez Plymovent, nous comprenons l'importance de protéger les informations de notre organisation et de nos clients. Grâce à cette procédure de réponse aux incidents numériques, nous posons les bases pour garantir la sécurité de vos données et informations.



Maintenir un environnement de travail sûr, sécurisé et résilient

Façonner le destin numérique de Plymovent

Cette procédure de réponse aux incidents numériques guide les employés en fournissant une approche étape par étape pour gérer et signaler les violations de données ou les incidents de sécurité, garantissant une résolution rapide, des dommages minimes et le maintien de la confiance que nos clients nous accordent.

Cette procédure concerne tous ceux qui participent à la construction du destin numérique de Plymovent, de nos employés férus de technologie à nos sous-traitants de confiance et partenaires tiers. Elle couvre toute situation susceptible de mettre en péril la confidentialité, l'intégrité ou la disponibilité de nos données. Chaque personne associée à Plymovent, quelle que soit sa fonction, a le droit et la responsabilité de signaler tout incident, verbalement ou par écrit.

L’approche étape par étape de Plymovent

Gérer et signaler les violations de données ou les incidents de sécurité

Gérer et signaler les violations de données ou les incidents de sécurité

1 Première étape : rapportez ce que vous avez observé.

Commencez par un rapport verbal à votre supérieur immédiat et au responsable informatique de Plymovent.

Gérer et signaler les violations de données ou les incidents de sécurité

2 Ensuite, nous enquêtons.

Nos rouages d'enquête commencent à tourner et incluent ce qui suit :

1. Rapport initial : Adressez votre rapport verbal ou écrit à votre supérieur ou au responsable informatique du Groupe.
2. Évaluation initiale : nous évaluons la gravité de votre incident. Si possible, nous essaierons de résoudre le problème.

Nous traiterons l'affaire sans ouvrir d'enquête formelle. Si le supérieur ou le responsable informatique du Groupe ne procède pas à une enquête formelle, la personne qui a fait le signalement sera informée par écrit des motifs de la plainte dans un délai de deux semaines. Nous discuterons également personnellement des menaces potentielles ou clarifierons tout malentendu, si nécessaire.

3. En cas d'enquête formelle :

■ Le supérieur ou le responsable informatique du Groupe décrit la procédure d'enquête et les actions possibles. Informations concernant tout soutien ou ressources externes.

■ Le supérieur et/ou le responsable informatique du Groupe mène une enquête approfondie, interroge les personnes concernées et examine les documents ou données associés.

■ Nous vous tiendrons au courant de l'avancement une fois que nous serons absolument certains du résultat. Nous vous tiendrons certainement informé de tout progrès ou retard, si nécessaire.

Gérer et signaler les violations de données ou les incidents de sécurité

3 Trouvons une solution.

Le résultat de l'enquête sera communiqué à toutes les parties concernées, soit verbalement, soit par écrit.

- Nous nous assiérons pour partager ce que nous avons découvert et les prochaines étapes à suivre.
- Nous établirons un plan d'action qui décrit comment nous allons régler les problèmes, le calendrier et les mesures correctives que nous devons mettre en place.

A propos de cette procédure

Restons fidèles à notre procédure !

Dans le cas contraire, et si quelqu'un choisit de ne pas tenir compte de notre politique, nous devrons peut-être prendre les mesures appropriées, par exemple :

- Avertissement formel
- Formation obligatoire (corrective)
- Rupture de l'emploi ou du contrat
- Actions en justice

Des questions ? Veuillez contacter le responsable de cette politique.

PLYMOVENT®
clean air at work

Nom Rene Bakker

Fonction Group Finance & IT

Date 01.01.2024

Lieu Alkmaar

Signature