Directive relative à la sécurité informatique

La présente directive relative à la sécurité informatique définit les mesures techniques et d'organisation actuelles de LucaNet.

1 Organisation

Mesure	Description
Responsabilité relative à la sécurité	• LucaNet a nommé un délégué à la sécurité qui est responsable de la conception, la coordination et la surveillance de la présente directive relative à la sécurité informatique. • Le délégué à la sécurité de LucaNet contrôle au moins une fois tous les douze mois la présente directive relative à la sécurité informatique ainsi que l'ensemble des mesures techniques et d'organisation afin de proposer, le cas échéant, des mesures d'amélioration.
Directives	• LucaNet dispose de directives dans lesquelles sont décrites les mesures de la présente directive relative à la sécurité informatique ainsi que les procédures et les responsabilités pertinentes des personnes ayant accès aux Données clients. • LucaNet conserve ses directives une fois que celles-ci ne sont plus effectives.
Gestion des risques	• LucaNet a effectué une analyse des risques avant la fourniture du service et le traitement des Données clients.
Confidentialité	• Les collaborateurs de LucaNet ayant accès aux Données clients sont soumis à des obligations de confidentialité.

Formations	• LucaNet informe ses collaborateurs sur :
	  • Fondements de la protection des données
	  • Mesures techniques et d'organisation de la présente directive relative à la sécurité informatique
	  • Leurs tâches respectives relatives à la sécurité informatique
	  • Conséquences personnelles en cas de Violation de la protection des données et/ou de la présente directive relative à la sécurité informatique

2 Sécurité physique

Mesure	Description
Accès aux installations	• LucaNet limite l'accès aux installations dans lesquelles se trouvent les systèmes informatiques qui traitent les Données clients aux seules personnes autorisées mentionnées.
Protection contre les pannes	• LucaNet utilise des systèmes conformes aux normes du secteur afin d'éviter toute perte de données en raison de pannes d'alimentation ou de perturbations de lignes.
Plans de procédure d'urgence	• LucaNet maintient des plans de procédure d'urgence pour les installations dans lesquelles sont situés les systèmes informatiques traitant les Données clients. • En cas de restauration des données, LucaNet reconstitue les Données clients dans leur version originelle ou dans leur dernière version répliquée à compter de la date de leur perte ou de leur destruction.
Travail mobile	• Les collaborateurs de LucaNet doivent obtenir l'autorisation de ce dernier avant d'enregistrer des Données clients sur des supports de stockage mobiles, d'accéder à distance aux Données clients ou de traiter des Données clients en dehors des installations de LucaNet.

3 Accès

Mesure	Description
Authentification	• LucaNet utilise des procédures conformes aux normes du secteur pour authentifier les utilisateurs qui accèdent aux systèmes informatiques. • LucaNet s'assure que les mots de passe sont conformes aux exigences minimales définies et sont régulièrement renouvelés ou en donne la possibilité au client. • LucaNet utilise des procédures conformes aux normes du secteur pour protéger les mots de passe. • LucaNet surveille les tentatives répétées d'accéder à ses systèmes informatiques à l'aide de mots de passe invalides ou en donne la possibilité au Client. • LucaNet s'assure que les comptes utilisateurs verrouillés ne sont attribués à aucune autre personne ou en donne la possibilité au Client. • LucaNet annule les droits d'accès de tout collaborateur qui quitte l'entreprise.
Autorisation	• LucaNet tient et met à jour des registres relatifs aux collaborateurs qui sont autorisés à accéder aux systèmes informatiques contenant des Données clients. • LucaNet désigne les collaborateurs autorisés à octroyer, modifier ou retirer l'accès autorisés aux données et aux ressources. • LucaNet limite l'accès aux Données clients aux seules personnes qui en ont besoin pour exécuter leur activité professionnelle.
Verrouillage de l'ordinateur	• LucaNet demande à ses collaborateurs de verrouiller leur ordinateur lorsqu'ils le laissent sans surveillance.

4 Fonctionnement

Mesure	Description
Restauration de données	• LucaNet génère régulièrement mais au moins une fois par semaine des copies des Données clients, à partir desquelles ces dernières peuvent être restaurées, et les conserve dans un autre site. • LucaNet dispose de procédures régissant l'accès aux copies de Données clients. • LucaNet contrôle la procédure de restauration des données au moins une fois tous les douze mois. • LucaNet documente les mesures de restauration des données.
Logiciels malveillants	• Le réseau de l'entreprise est protégé du réseau public par le biais de pare-feu. • LucaNet utilise des scanners antivirus actuels lors des accès au réseau de l'entreprise (pour les comptes e-mail) ainsi que sur l'ensemble des serveurs fichiers et des ordinateurs individuels. • LucaNet n'autorise aucune installation de logiciels qu'il n'a pas approuvés.
Chiffrement des Données clients	• LucaNet chiffre les Données clients ou donne la possibilité au Client de chiffrer les Données clients qui sont transférées par le biais du réseau public. • LucaNet chiffre les supports qui contiennent des Données clients et sont utilisés en dehors des bureaux de LucaNet.
Effacement de Données clients	• LucaNet régit par le biais d'une directive correspondante la façon dont les données et les supports de données sont effacés ou détruits lorsqu'ils ne sont plus nécessaires.
Impression de Données clients	• LucaNet définit par le biais d'une directive correspondante les restrictions s'appliquant à l'impression de Données clients ainsi que la façon dont les supports imprimés contenant des Données clients doivent être conservés et supprimés.

Violations de la protection des données	• Chaque incident considéré comme une Violation de la protection des données doit faire l'objet d'une signalisation immédiate à LucaNet.
	• LucaNet tient des registres relatifs aux Violations de la protection des données contenant au moins les éléments suivants :
	  • Description de l'incident
	  • Période
	  • Nom de la personne ayant signalé l'incident
	  • Nom de la personne à qui l'incident a été signalé
	  • Mesures