Working With Your Insurance Provider During a Cybersecurity Incident

You're in control, not your insurance provider.
If you are breached and wish to work with GoSecure, you have the right to choose us as your Incident Response provider. Insurers may suggest vendors, but they cannot require them.

What to Say to Your Insurer:
"We are electing to work with GoSecure for incident response. Please confirm that this is covered under our policy."

This gets explicit confirmation of coverage — before work begins — and ensures transparency between all parties.

Why GoSecure?

- Recognized by major insurers & breach coaches (incl. Northbridge)
- GIAC-certified experts in forensics and incident response
- Trusted first-call responder for many clients
- Award-winning service delivery
- Clear scope, no surprise billing

Quick Reference:
Emergency Hotline: 888-287-5858
Email: breach@gosecure.net
Website: www.gosecure.ai

Proactively share this document with legal, compliance, and executive teams, before an incident occurs.

GoSecure

Votre allié
pour consolider,
évoluer et prospérer

Travailler avec votre assureur lors d'un incident de cybersécurité

C'est vous qui avez le contrôle, pas votre assureur.
Si vous êtes victime d'une brèche de données et souhaitez collaborer avec GoSecure, vous avez le droit de nous choisir comme fournisseur de services d'intervention en cas d'incident. Les assureurs peuvent suggérer des fournisseurs, mais ne peuvent pas les imposer.

Ce qu'il faut dire à votre assureur :
« Nous avons choisi de collaborer avec GoSecure pour la gestion des incidents. Veuillez confirmer que ceci est couvert par notre police. »

Cela permet d'obtenir une confirmation explicite de la couverture, avant le début des travaux, et assure la transparence entre toutes les parties.

Pourquoi GoSecure ?

- Reconnu par les principaux assureurs et entraîneurs en matière d'infractions (dont Northbridge)
- Experts certifiés GIAC en analyse médico-légale et en réponse aux incidents
- Intervenant de confiance pour de nombreux clients
- Prestation de services primée
- Portée claire, facturation sans surprise

Référence rapide :
Ligne d'urgence : 888-287-5858
Courriel : breach@gosecure.net
Site Web : www.gosecure.ai/fr

Partagez ce document de manière proactive avec les équipes juridiques, de conformité et de direction, avant qu'un incident ne se produise.

13220 Evening Creek Dr. S Suite 107
San Diego, CA 92128

How to Engage GoSecure During a Cybersecurity Incident

You've been breached — now what?
This document explains how to notify your insurer and activate GoSecure immediately to begin triage and containment.

Step 1: Notify Your Insurer
Tell them:
"We are electing to work with GoSecure for incident response. Please confirm coverage approval."

Step 2: Contact GoSecure immediately
888-287-5858
breach@gosecure.net
We will coordinate directly with your insurer, begin evidence gathering, and activate the tools remotely.

Critical Preservation Warning
DO NOT POWER OFF DEVICES – REMOVE ALL NETWORK CONNECTIVITY TO PRESERVE EVIDENCE.
Do not re-image or restore systems until GoSecure has completed initial forensic collection. Premature cleanup can destroy critical artifacts.

Step 3: Gather & Share the Following:
- Ransom note or attacker message
- Incident timeline or internal notes
- Logs: VPN, firewall, antivirus, DUO, Microsoft 365 / Azure
- Existing forensic tool output (if any)

Step 4: Prepare Access & Tools
- We'll send you a consent form for EDR deployment
- Use our secure SFTP to upload evidence
- Grant a temp M365/Azure account (Global Reader + Exchange Admin)

GoSecure EDR & Forensics:
Our tools run silently, collect key artifacts, and support rapid containment. We'll guide your team every step of the way.

Print and store this document with your IR playbook and distribute it to IT, Legal, and Leadership.

Comment impliquer GoSecure lors d'un incident de cybersécurité

Vous avez été victime d'une intrusion ; quoi faire ?
Ce document explique comment avertir votre assureur et activer GoSecure immédiatement pour commencer le tri et le confinement.

Étape 1 : Informez votre assureur
Dis-leur :
« Nous avons choisi de collaborer avec GoSecure pour la gestion des incidents. Veuillez confirmer l'approbation de la couverture. »

Étape 2 : Contactez GoSecure immédiatement
888-287-5858
breach@gosecure.net
Nous coordonnerons directement avec votre assureur, commencerons la collecte de preuves et activerons les outils à distance.

Avertissement de conservation critique
NE PAS ÉTEINDRE LES APPAREILS – SUPPRIMER TOUTE CONNECTIVITÉ RÉSEAU POUR PRÉSERVER LES PREUVES.
Ne pas réimager ni restaurer les systèmes tant que GoSecure n'a pas terminé la collecte de prescription initiale. Un nettoyage prématuré peut détruire des artéfacts critiques.

Étape 3 : Rassemblez et partagez ce qui suit :
- Demande de rançon ou message de l'attaquant
- Chronologie de l'incident ou notes internes
- Journaux : VPN, pare-feu, antivirus, DUO, Microsoft 365/Azure
- Résultats de l'outil d'enquête existant (le cas échéant)

Étape 4 : Préparer l'accès et les outils
- Nous vous enverrons un formulaire de consentement pour le déploiement de l'EDR
- Utilisez notre protocole SFTP sécurisé pour télécharger les preuves
- Accordez un compte M365/Azure temporaire (Global Reader + Exchange Admin)

GoSecure EDR et criminalistique :
Nos outils fonctionnent silencieusement, ramassent les artefacts clés et permettent un confinement rapide. Nous accompagnons votre équipe à chaque étape.

Imprimez et conservez ce document avec votre guide de réponse aux incidents et distribuez-le aux services informatiques, juridiques et de direction.