1. Tous problèmes techniques ou incidents doivent être communiqués au service Support GOSIS, soit

1.1. Pour tout incident excepté les incidents liés à la sécurité de l'information

- Par téléphone au 04 66 45 33 13
- Soit par mail à l'adresse suivante : support@gosis.com

1.2. Pour tout incident lié à la sécurité de l'information

- Par téléphone au 04 66 45 33 13
- Soit par mail à l'adresse suivante : abuse@gosis.com

1.3. Informations à nous communiquer

Pour nous permettre de vérifier que nous communiquons avec les personnes habilitées :

- Nom utilisateur
- Prénom utilisateur
- Adresse mail pro

Pour nous permettre de qualifier votre ticket et de prioriser le mieux possible notre intervention :

- Une description du problème technique rencontré ou de l'incident survenu

2. Comment qualifier un incident lié à la sécurité de l'information

Catégorie d'incident	Type d'incident	Description
Atteinte à la disponibilité	DOS	Attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. La disponibilité peut également être affectée par des actions locales (destruction, perturbation de l'alimentation électrique,
	DDOS	
	Sabotage	
Infection	Virus, Ver, Trojan, Ransomware, Backdoor…	Un code malicieux qui est intentionnellement inclus ou inséré dans un système à des fins nocives. L'interaction de l'utilisateur est normalement nécessaire pour activer le code.
Tentatives d'intrusion	Exploitation des vulnérabilités	Une tentative de compromettre un système ou de perturber un service en exploitant des vulnérabilités (ex. Buffer overflow, XSS, Sql injection, file upload etc.).
	Tentatives de connexion	Plusieurs tentatives de connexion (deviner / craquer des mots de passe, force brute).
	Phishing	le but est de dérober des informations personnelles des utilisateurs ou de les piéger à installer un malware
	Nouvelle signature d'attaque	Une tentative d'exploit inconnu.
Intrusion	Compromission d'un compte	Contrôle réussi d'un compte
		Ajout d'un compte
		Changement des droits d'accès ou de mot de passe
	Défiguration d'un site web	Insertion, modification ou suppression d'un contenu web
Collecte d'informations	Scan	Attaques qui envoient des requêtes à un système pour découvrir des points faibles. Ce type d'attaque inclut certains types de processus de test pour collecter des informations sur les hôtes, les services et les comptes. Exemples: fingerd, requête DNS, ICMP, SMTP (EXPN, RCPT, ...)
	Sniffing	Capture et enregistrement du trafic réseau.
	Ingénierie sociale	Collecte des informations d'un être humain dans un environnement non technique
		(P. Ex. Mensonges, astuces, pots de vin ou menaces)
Atteinte à la sécurité des données	Accès ou modification non autorisée des informations	
	Exfiltration des données	Récupération des données et leur transfert vers une destination externe non légitime.
Autres	Tous les incidents qui ne correspondent pas à l'une des catégories données ci-dessus doivent être classés dans cette classe	Demande de réinitialisation d'un mot de passe