Incident Response Services

Thank you for contacting Conscia Incident Response Services. We will do everything in our power to contact you regarding a prompt investigation and resolution of your incident.

Contact Information

Phone:	+386 1474 6555
Email:	soc-ir@conscia.com
Secure phone:	Signal App with your IR handler
Secure email:	soc-ir@conscia.com / PGP / A999 B749 8D1A 8DC4 73E5 3C92 309F 635D AD1B 5517
Secure file exchange:	https://ncbox.nil.com

Resolve the incident faster - prepare following information

1. What is the nature of the incident as observed so far?
2. What is the current and possible future business impact of the incident to your organization?
3. What is the scope of the incident? Does it only concern your organization?
4. How, when, and by whom was the problem initially detected?
5. Have you observed any other incidents in your organization recently?
6. What actions have you taken so far to address this incident?

Service Prerequisites

Conscia requires the following steps to be strictly followed:

1. SECURE COMMUNICATION PLATFORM
It is imperative that the equipment, software, and services used for communication with Conscia is NOT COMPROMISED AND/OR INVOLVED IN THIS INCIDENT.

2. IDENTITY VERIFICATION

We will require you to prepare information in order to authenticate the organisation involved in the incident, as well as your association with them.
We suggest utilizing one of the following options:

a. A common trusted third party (for example, a Conscia Group employee) whom we can contact to vouch for your identity and association.
b. A video call with Conscia Incident Response Services where we can clearly see your passport or personal identification card details, and an uncompromised published phone number or email address associated with the organization that we can contact you on.
c. A video call with a top-management representative (CISO, CIO, CFO, CEO...) of your organization, where we can clearly see their passport or personal identification card details.

3. SERVICE AGREEMENT

Our hourly rates for incident response activities have been or will be communicated to you by our SOC personnel. Before we proceed, you should confirm the billing rates and our data processing policy: Please click this link to fill the consent form, to agree with basic terms of Conscia incident response services

DOs	DON'Ts
Assemble an incident resolution team at your organization. Consider inviting management, legal, PR, as well as engineering experts that have administrative access to resources.	Do not shut down or reboot the affected systems. If there is an urgent need to isolate a system, disconnect it from the network.
Document all your activities related to the incident and put a timestamp next to each entry.	Do not change anything on the affected systems unless critical further damage is imminent due to malicious activities.
Prepare for the initial interview with our incident handler by examining the questions above.	Do not panic, we will handle this together.