MindSonar
Cyber Security Policy

And Incident Response Plan

Version 5.0 - November 2021

MindSonar coordinates

Owner:
Metaprofiel B.V., owner of the brand, trademark and technology referred to as ‘MindSonar’

Address:

Metaprofiel B.V.
Staringstraat 1
6511 PC Nijmegen
The Netherlands

Policy brief & purpose

MindSonar's cyber security policy outlines our guidelines for preserving the security of our data and technology infrastructure.

Technology to collect, store and manage information, is at the heart of MindSonar. Human errors, hacker attacks and system malfunctions could cause financial damage and jeopardise MindSonar's reputation. Being careful and attentive, maintaining good cyber protection and keeping the MindSonar system running smoothly, will allow our customers to relax and focus on their main task: understanding, coaching, teaching and managing people.

Scope

This policy applies to all our Distributors, Professionals, Developers, and anyone who has permanent or temporary access to our systems. All MindSonar Distributors, Professionals and Developers are obliged to protect MindSonar data.

A. General Security Measures

Protect personal and company devices

We urge our Distributors, Professionals, Developers to keep both their computers, tablets and cell phones secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.

- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems as soon as they become available.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we urge our Distributors, Professionals and Developers to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g. offering prizes or outrageous claims.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If a Distributor, Professional or Developer isn’t sure that an email they received is safe, they are advised to Google the email subject line. Websites run by anti-virus software companies, like sophos.com keep a detailed record of hoaxes, phishing mails and other threats and will usually identify a malicious email quickly.

Fishing emails

In the past fishing emails have been sent, supposedly coming from a MindSonar e-mail address, signed with names of people that have never been employed by MindSonar Global.

So if you receive an email supposedly coming from a MindSonar e-mail address be aware of these signs of phishing:

- Signed by people you have never heard of before in the MindSonar context.
- Instead of addressing you directly, using generic names like “Dear Customer” or “Hi Friend”.
- Showing unusual phrases, spelling, capital letters and so on. Unusual syntax is often a sign that something is wrong.

- Use of alarming wording (such as saying your MindSonar account has been hacked) to trick you into moving fast.
- Asking you to contact them regarding some financial matter, either payments due or checking your account or even you receiving some payment.

If you receive a suspicious email, do not respond to it and send it to MindSonar Global.

Manage passwords well

Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advice our Distributors, Professionals and Developers to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)

  If you are not sure of the strength of your password, please check it here.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, Distributors, Professionals and Developers should choose the phone instead of email, and only if they personally recognise the person they are talking to.
- Change your passwords regularly.
- Remembering a large number of passwords can be daunting. We recommend a password management tool which generates and stores passwords. A well reviewed password tool is f.i. Dashlane, which has a free version.
- The premium option of Dashlane can monitor the dark web to see if your email address and other information has been gathered in a data breach and sold. This service will then send you a warning. Alternatively, you can go to the free Firefox Monitor page regularly to check if your passwords have been compromised.

Transfer data securely

Transferring data introduces security risk. Distributors, Professionals and Developers are urged to:

- Avoid transferring MindSonar Profiles to other devices or accounts except of course for downloading the profile to their computer and sending it to their client. Avoid mass transfer of profiles. If you absolutely need to transfer large numbers of profiles, then a USB-stick is the safer option.
- Share MindSonar Profiles over secure networks and never over public Wi-Fi's like in restaurants or hotels.
- Report scams, privacy breaches, hacking attempts and phishing attempts to MindSonar Global, e-mail: jh@iepdoc.nl.

B. Security Measures Restricting Access

- Access is limited to the one MindSonar Professional who has been granted explicit permission by the respondent (Data Subject). All others are restricted from accessing the personal data of this particular respondent, except for the MindSonar admin.
- Access to personal data is protected with separate passwords issued to all MindSonar Professionals who are allowed to download this data. The passwords cannot be retrieved by others, not even by MindSonar employees.
- Each MindSonar professional agrees to a personalised GDPR contract with MindSonar. (GDPR = the European Union's General Data Protection Regulation).
- In terms of GDPR, Metaprofiel B.V., MindSonar's owner, is the 'Data Controller' since Metaprofiel gathers the data from the 'Data Subject' (the respondent who fills out the questionnaire). The MindSonar Professional is a 'Data Processor', they use the data for coaching, training, teaching or managing the Data Subject.
- In the GDPR contract the Controller and the Processor agree on how the Data Processor will handle the data.
- This contract, plus the date and time of agreement, are stored on the MindSonar server as well as in the MindSonar Professional's personal account.
- Without entering into this GDPR contract (or in case the retract the contract) a MindSonar Professional cannot access any personal data.

- Standard retention is 8 years. Individual respondents are advised of this time period before they give their permission. If individual respondents don't give permission, no personal data is gathered (the system stops gathering data and no profile will be made).
- Individual respondents may request removal of their data by sending an email, with which MindSonar will comply within 10 working days.
- Individual respondents may request a copy of their MindSonar Profile by sending an email, with which MindSonar will comply within 10 working days.
- Metaprofiel B.V. collects personal data for two purposes only: to produce MindSonar Profiles and to do research into mindsets (for which anonymised versions of the personal data are used).

C. Incident Response Plan

Brief & purpose

Our Incident Response Plan defines an organised approach we will apply when a data breach occurs or our service is interrupted. The Plan identifies the actions of our *Incident Response Team*. The Incident Response Team will put the plan into action.

Incident Response Team

The Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications. The Incident Response Team's mission is to prevent a serious loss of public confidence or information assets by providing a fast, effective and skilful response to an unexpected event involving computer information systems, networks or databases.

The Incident Response Team is authorised to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-

effective manner and reporting findings to MindSonar Global and the appropriate authorities as necessary.

Incident Response Team Members

- **Global Incident Response Communication Manager**
  Tomasz Zawadzki
- **Incident Response Technical Lead**
  Antoni Kozelski
- **Incident Response PHP Expert**
  Grzegorz Gąsak

For contact information, phone, slack and email of Incident Response Members contact MindSonar Global.

Types of Incidents

There are many types of computer incidents that may require Incident Response Team activation. Some examples include:

- Breach of Personal Information
- Denial of Service / Distributed Denial of Service
- Excessive Port Scans
- Firewall Breach
- Virus Outbreak

Breach of Personal Information

This Incident Response Plan outlines steps our organisation will take upon discovery of unauthorised access to personal information that could result in harm or inconvenience to an individual. The individual will in our case most likely be a Data Subject (respondent) who has filled out a MindSonar Profile or a Data Processor (a MindSonar Professional) who uses MindSonar for coaching, teaching or managing others.

Personal information is information about an identifiable individual. It includes any information that can be linked to an individual. For our purposes, personal information is defined as an individual's first name or first initial and last name, in combination with any of the following data:

- Meta Program (thinking style elements)
- Graves Drives (value categories)
- Age
- Profession
- Marital Status

Definitions of a Security Breach

A security breach is defined as unauthorised acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us. Good faith acquisition of personal information by a MindSonar agent like a MindSonar Distributor or Professional or a MindSonar employee for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorised disclosure.When Notification is Required

The following incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or third-party provider) has obtained unauthorised access to personal information.
- An intruder has broken into database(s) that contain personal information on an individual.
- Computer equipment such as a workstation, laptop, CD-ROM, or other electronic media containing personal information on an individual has been lost or stolen.
- An employee or contractor has not properly disposed of records containing personal information on an individual.

- A third party service provider has experienced any of the incidents above, affecting the organisation's data containing personal information.

The following incidents may not require individual notification under contractual commitments or applicable laws and regulations providing the organisation can reasonably conclude after investigation that misuse of the information is unlikely to occur, and appropriate steps are taken to safeguard the interests of affected individuals:

- The organisation is able to retrieve personal information on an individual that was stolen, and based on our investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.
- The organisation determines that personal information on an individual was improperly disposed of but can establish that the information was not retrieved or used before it was properly destroyed.
- An intruder accessed files that contain only individuals' names and addresses.
- A laptop computer is lost or stolen, but the data is encrypted and may only be accessed with a secure token or similar access device.

Incident Response Roadmap

Incident Response Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

Global Incident Response Communication Manager
The IRCM will serve as a central point of contact for reporting any suspected or confirmed breach of personal information on an individual.

After documenting the facts presented by the caller and verifying that a privacy breach or suspected privacy breach occurred, the IR Communication Manager will immediately notify the Incidence Response Technical Lead by first by phone and if they fail to reach the IR Technical Lead by phone, by Slack and E-mail.

Incidence Response Technical Lead

1. When notified by the IR Communication Manager, the IR Technical Lead performs a preliminary analysis of the facts and assess the situation to determine the nature and scope of the incident.

2. Contacts the individual who reported the problem.

3. Identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach of personal information about an individual. Every breach may not require participation of all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).

4. If a privacy breach affecting personal information is confirmed, Incident Response Team activation is warranted. Contact the IR Communications Manager and advise them to update the Incident Request with "Incident Response Team Activation – Critical Security Problem".

5. Notify the MindSonar Global of the details of the investigation and breach. Keep them updated on key findings as the investigation proceeds.

6. The IR Technical Lead is responsible for documenting all details of an incident and facilitating communication to MindSonar Global and other auxiliary members as needed.

7. Contact all appropriate database and system administrators to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach.

8. Identify and contact the appropriate Data Owner affected by the breach.

9. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all test, development and production systems and the number of individuals at risk.

10. Determine the type of personal information that is at risk.

11. Determine if an intruder has exported, or deleted any personal information data.

12. Determine where and how the breach occurred.

    - Identify the source of compromise, and the timeframe involved.

    - Review the network to identify all compromised or affected systems.

    - Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.

13. Take measures to contain and control the incident to prevent further unauthorised access to or use of personal information on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.

    - Change all applicable passwords for ID's that have access to personal information, including system processes and authorised users. If it is determined that an authorised user's account was compromised and used by the intruder, disable the account.

    - Do not access or alter the compromised system.

    - Do not turn off the compromised machine. Isolate the system from the network (i.e. unplug cable).

    - Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorised devices that may be using the corporate wireless network.

14. Monitor systems and the network for signs of continued intruder access.

15. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations.

    Document all actions taken, by whom, and the time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.

16. If an internal user (authorised or unauthorised employee, contractor, consultant, etc.) was responsible for the breach, contact MindSonar Global for disciplinary action and possible termination. In the case of contractors, temporaries, or other third-party personnel, ensure discontinuance of the user's service agreement with the company.

Incident Response PHP Expert

Will be available to be consulted on very short notice regarding PHP issues related to the security breach.