Workspace 365 Responsible disclosure policy

We consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Please do the following:

- E-mail your findings to support@workspace365.net

    1. Please provide a technical description of the concern or vulnerability.
       a) Please provide information on which specific product you tested, including product name and version number; the technical infrastructure tested, including operating system and version; and any relevant additional information, such as network configuration details.
       b) For web based services, please provide the date and time of testing, URLs, the browser type and version, as well as the input provided to the application.
    2. To help us to verify the issue, please provide any additional information, including details on the tools used to conduct the testing and any relevant test configurations. If you wrote specific proof- of-concept or exploit code, please provide a copy. Please ensure all submitted code is clearly marked as such and is encrypted with our PGP key.
    3. If you have identified specific threats related to the vulnerability, assessed the risk, or have seen the vulnerability being exploited, please provide that

- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data;

- Do not reveal the problem to others until it has been resolved;

- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties; and

- Do not be disproportionate, such as:

  a) Using social engineering to gain access to the system.

  b) Build your own backdoor in an information system with the intention of then using it to demonstrate the vulnerability, as doing so can cause additional damage and create unnecessary security risks.

  c) Utilizing a vulnerability further than necessary to establish its existence.

  d) Copying, modifying or deleting data on the system. An alternative for doing so is making a directory listing of the system.

  e) Making changes to the system.

  f) Repeatedly gaining access to the system or sharing access with others.

  g) Using brute force attacks to gain access to the system. This is not a vulnerability in the strict sense, but rather repeatedly trying out passwords; and

- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

- If the issue involves AI-generated responses or search results revealing unintended data (e.g., private or indexed content), please include a screenshot or copy of the prompt/output that triggered it.

- If the vulnerability is actually in a 3rd party component which is part of our product/service, we will refer the report to that 3rd party and advise you of that notification. To that end, please inform us whether it is permissible in such cases to provide your contact information to the 3rd party.

What we promise:

- We will respond to your report within 2 business days with our evaluation of the report and an expected resolution.
- We will provide you with a unique tracking number for your report.
- We will assign a contact person to each case.
- We will keep you informed on the status of your report approximately every 2-3 weeks.
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission;
- We will keep you informed of the progress towards resolving the problem;

We aim to resolve all issues as swiftly as possible, followed by a clear communication once the matter has been resolved.

By sharing information with us, you agree that it will be treated as non-proprietary and non-confidential, and that we may use it freely, in whole or in part, without restriction. You also acknowledge that providing such information does not create any rights for you, nor any obligations for us.