Responsible Disclosure notifications

The legal entities belonging to the Royal Schiphol Group, with its registered office in the Netherlands, are part of the country's essential infrastructure. For this reason we consider it of the greatest importance that our IT systems are secure. Despite all the security measures that have already been taken, it cannot be ruled out that our digital systems have a weak spot. If you find one, you can help us in this regard by making a Responsible Disclosure notification. This document lays out the most important rules concerning the identification of a security issue and the making of a Responsible Disclosure notification.

What to do if you find a vulnerability in our system

If you find a vulnerability in our IT system we would like you to tell us about it immediately, so that we can take whatever measures are necessary to solve the problem as quickly as possible. We take all notifications of security issues in our IT systems very seriously. To be able to respond to these notifications responsibly, we would like to make the following agreements with you. Have you found a problem, and you are wondering how it should be reported? We would like to hear about it immediately, in the following way.

- Email your findings as quickly as possible to responsible [full stop] disclosure [at] schiphol [full stop] nl. If possible, encrypt this email using Schiphol's PGP key; this will prevent your information from falling into the wrong hands.
- In the email explain how you encountered this issue, so that we can reproduce it. Describe the problem and provide the relevant IP address or URL.
- Include your own contact details, such as an email address or telephone number. We can then get in touch with you to work together on a secure solution.
- We will respond as quickly as possible to report on ongoing progress.

We trust you to deal responsibly with information about a security issue. We would expect that you share this information with no-one except Schiphol; we would ask that you perform no more actions to demonstrate the problem; and we would also ask that if this security issue has resulted in your obtaining confidential information, that you immediately and irreversibly delete this data.

Be careful not to break the law

As soon as you have discovered a security issue, it is important to report it and not to research into it further. This is because even well-intentioned research can result in illegal acts; that is to say, actions that are against the law. For instance, it is not permitted:

- to share the problem with others before it has been solved;
- to install malware;
- to copy, modify, or remove system data (an alternative to this is to make a directory listing of a system);
- to make any changes to the system;
- to obtain repeated access to the system, or share this access with others;
- to make use of 'brute force' attacks to gain access to a system;
- to make use of denial-of-service or social engineering;
- to misuse the situation by, for instance, downloading more data than is necessary to demonstrate the issue; or by reading, altering or erasing other people's data;

- to make use of attacks on physical security, social engineering, distributed denial-of-service, spam, or third-party applications;
- to use your investigations to reveal client data or other personal details;
- to use techniques that might affect the availability of Schiphol's online services.

What types of problem can you report? It is helpful if you can identify the problem as one of the following:
 Remote Code Execution
 Cross Site Scripting (XSS)
 Cross Site Request Forgery (CSRF)
 Injection vulnerability
 Broken authentication and session management
 Encryption vulnerability
 Unauthorised access to data
 Inadequately protected APIs

What is responsible disclosure *not* intended for?
 Submitting a question, comment, or complaint about the airport
 Questions or complaints about the availability of Schiphol websites or mobile applications

International law and regulations

Legal frameworks surrounding the discovery and reporting of such vulnerabilities may differ from country to country. We recommend that you take account of these laws. It is possible that your investigations break an national (or international) law, and that you risk legal prosecution as a result. If you have discovered a vulnerability in our IT systems then you must remember that the law stands above the rules that Schiphol itself employs. Nevertheless, if you act in good faith and in accordance with Schiphol's rules, we will not report your actions to the authorities unless we are required by law to do so.

What can you expect from us?

- If you adhere to the conditions described above in submitting your notification of a vulnerability in a IT system at Schiphol, Schiphol will attach no legal consequences to this notification.
- Schiphol will handle your notification in confidentiality and will not share private data with third parties without your express permission, unless required to do so by law.
- We will send you an acknowledgement of receipt within five working days.
- You can expect us to send you, in the short term, a response in which we state our assessment of your notification and an expected date for a solution to the problem.
- We will keep you informed of our progress in solving the problem.
- If your notification identifies a genuine security problem, Schiphol will solve this problem as quickly as possible. Our aim is to do so within 90 days. After having solved the problem we will decide, in consultation, whether and in what way to communicate this problem externally.
- Should you desire it and give your permission, Schiphol may publish your name as the discoverer of the reported vulnerability in the 'Royal Schiphol Group Responsible Disclosure Hall of Fame'.

The Royal Schiphol Group Responsible Disclosure Hall of Fame

In our Responsible Disclosure Hall of Fame we can publish:

- your first name, surname, and/or pseudonym (your choice)
- a description of the identified vulnerability
- the number of identified vulnerabilities per reporter

The conditions for the publication of your name are as follows:

- you agree to the general privacy conditions of the Schiphol Group (shown here);
- you are the first person to have reported the vulnerability / bug;
- we determine whether the notification identifies a genuine vulnerability, by reference to industry standards such as the Common Vulnerability Scoring System (https://www.first.org/cvss/calculator/3.0);
- you adhere to the Schiphol rules with regard to responsible disclosure;
- the disclosure must be solved before your name and details can be published. This means that your name will not be published if Schiphol chooses not to (immediately) solve the problem;
- every notification published in the Hall of Fame is automatically removed after two years;
- the reporter has the right to correct, alter or remove their personal details;
- in the event of a dispute on (the nature of) the notification, Schiphol Group reserves the right to remove the notification from the Hall of Fame or not to place it in the first place.