# Policy - Responsible Disclosure

NFOrce Entertainment B.V. (referred to as NE) considers the security of our (and your) systems a top priority. We therefore value your input, should an immediate security vulnerability be present in our systems. If you discover such an immediate security vulnerability, we would like to know about it so we can take immediate steps to prevent collateral damages.

As a token of our gratitude for your assistance, we offer a reward for every applicable reported security vulnerability.

## Applicability

It is applicable if **all** of the following applies:

1. It is an immediate security vulnerability (i.e. data leaks / damage to infrastructure);
2. It applies to NE infrastructure services;
3. It is not a software limitation from our vendor;
4. It was previously unknown to us.

It is not applicable in any of the following cases:

1. Version disclosure of (web)services;
2. Error notices on (web)services;
3. Open directory/folder listings;
4. iFrame / Clickjacking;
5. HTTP (non SSL) services being enabled;
6. Brute force;
7. Social engineering;
8. Distributed denial of service;
9. Spam / Phising.

## Reporting

1. E-mail your findings to noc@nforce.com as soon as possible, noting down any pertinent information that may be of use closing up the vulnerability and preferably a way to reproduce;
2. Do not take advantage of the vulnerability you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data;
3. Treat the problem as confident information and refrain from revealing it to others until it has been resolved;
4. Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties;
5. Do not disclosure this information to anyone else other than NE.
6. Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible.

## Handling

1. We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date;
2. If you have followed the instructions above, we will not take any legal action against you concerning the report;
3. We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission;
4. We will keep you informed of the progress towards resolving the problem;
5. In case we wish to publish this case publicly, we will give your name as the discoverer of the problem (unless you desire otherwise, this information is requested before said report is published publicly);
6. The amount of the reward will be determined based on the severity of the security vulnerability and the quality of the report. If applicable, the minimum reward is a €50 account credit, **usable for any of NE services**. The credit is valid for 12 months.