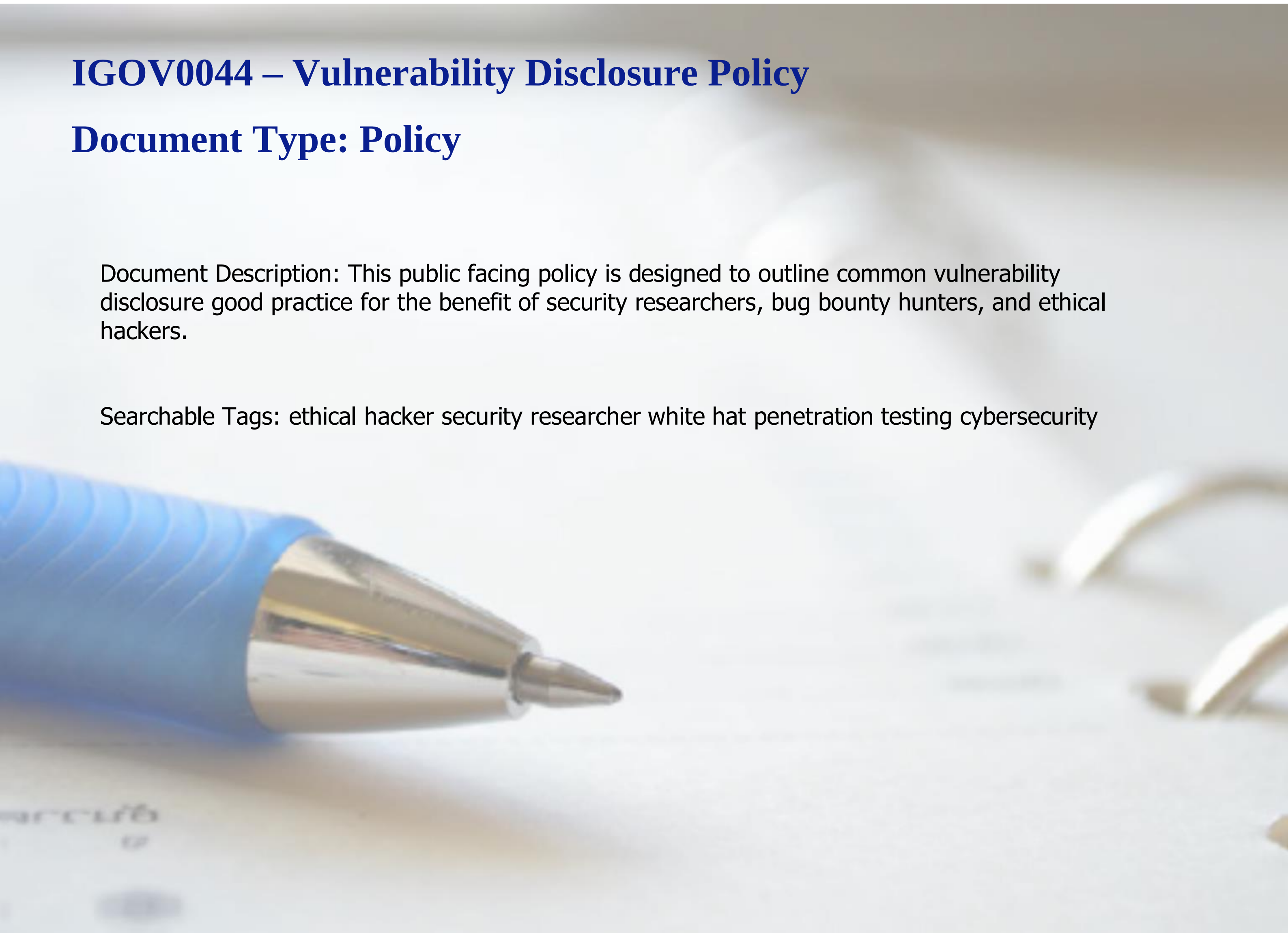
Information Governance



IGOV0044 – Vulnerability Disclosure Policy

Document Type: Policy

Document Description: This public facing policy is designed to outline common vulnerability disclosure good practice for the benefit of security researchers, bug bounty hunters, and ethical hackers.

Searchable Tags: ethical hacker security researcher white hat penetration testing cybersecurity

Last Reviewed: 10 November 2023

Next Review Due: 10 November 2024

Version: 1

Classification: **Public Document**

Idox. Do more.

Contents

1 Introduction

This vulnerability disclosure policy applies to any vulnerabilities you are considering investigating and potentially reporting to us (the "Organisation"). We recommend reading this vulnerability disclosure policy fully before you investigate or report a vulnerability and always act in compliance with it.

We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

2 Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following link:

Report a vulnerability

In your report, please include details of:

- the website, IP or page where the vulnerability can be observed
- a brief description of the type of vulnerability, for example; "XSS vulnerability"
- the steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

3 What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. We'll also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your vulnerability has been resolved, we welcome requests to disclose your report. We'd like to unify guidance to affected users, so please do continue to coordinate public release with us.

4 Guidance

4.1 You must NOT:

- break any applicable law or regulations
- access unnecessary, excessive, or significant amounts of data
- modify data in the Organisation's systems or services
- use high-intensity invasive or destructive scanning tools to find vulnerabilities

- attempt any form of denial of service, for example, overwhelming a service with a high volume of requests
- disrupt the Organisation's services or systems
- submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practice", for example missing security headers
- submit reports detailing TLS configuration weaknesses, for example "weak" cipher suite support or the presence of TLS1.0 support
- communicate any vulnerabilities or associated details other than by means described in this Policy and where applicable, the published security.txt
- social engineer, 'phish' or physically attack the Organisation's staff or infrastructure
- demand financial compensation in order to disclose any vulnerabilities
- violate the privacy of the Organisation's users, staff, contractors, services or systems
- share, redistribute or fail to properly secure data retrieved from the systems or services.

4.2 You must:

- always comply with data protection rules
- securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

5 Legal

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the Organisation or partner organisations to be in breach of any legal obligations.

However, if legal action is initiated by a third party against you and you have complied with this policy, we can take steps to make it known that your actions were conducted in compliance with this policy.

Thank you for helping keep Idox and our users safe!