UNIVERSITY OF HULL

Vulnerability Disclosure and Reporting Policy

Classification:	Policy
Version Number:	1.0
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval Date:	11 October 2021
Effective from:	11 October 2021
Next Review Date:	Biennual
Document Authors:	Steph Jones
Document Owner:	Security and Architecture Manager, ICT (Steph Jones)
Department/Contact:	ICT/support.hull.ac.uk
Summary:	This policy outlines the vulnerability disclosure and reporting policy in order to protect the University and its assets from compromise or breach
Scope:	All systems hosted within the University domain/public address space
Related legal frameworks:	See relevant section of overarching Information Governance and Assurance Policy
Related documents:	Information Security Controls Policy
Published locations:	Public website (www.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.
All printed versions of this document are classified as uncontrolled. A controlled version is available on the support portal.	

Vulnerability Disclosure and Reporting Policy

1. Introduction

1.1. This policy outlines the use of vulnerability disclosure and reporting policy in order to protect the University and its assets from compromise or data breach.

1.2. Protecting systems and data from security vulnerabilities is of the upmost importance to the University. This involves identifying and addressing any weaknesses that could compromise the integrity, availability, or confidentiality of University services.

1.3. This policy supports the objectives of the overarching **Information Governance and Assurance Policy** and **Information Security Controls Policy**.

2. Scope

2.1. All systems hosted within the University domain/public address space (hull.ac.uk, 150.237.0.0/16).

3. Disclosure and Reporting

3.1. University members or security researchers that discover a vulnerability in a University system or service should report it to csirt@hull.ac.uk.

3.2. When reporting a vulnerability, it is asked that the reportee does not remain anonymous so that we can proactively engage in order to confirm the vulnerability and acknowledge the effort.

3.3. If when reporting a vulnerability, there is a concern about the confidentiality of the information sent, then it is recommended that the report and any information is encrypted through GPG/PGP.

3.4. When reporting a vulnerability, in all cases the reportee must:

- **Respect University members privacy:** Contact the University immediately if anyone else's data, personal or otherwise has been accessed. This includes usernames, passwords and other credentials. This information must not be saved, stored or transmitted.
- **Act in good faith:** The vulnerability should be reported with no conditions attached.
- **Work with the University:** Promptly report any initial findings and then request permission prior to continuing any testing. This allows the University a reasonable amount of time to respond and mitigate the vulnerability before any public disclosure might occur.

3.5. When reporting a vulnerability, the reportee must not:

- Exfiltrate data: Use a proof of concept to demonstrate the vulnerability.
- Use a vulnerability to disable further security controls.
- Perform social engineering.
- Perform any testing of physical security.
- Use brute force or forceful means.
- Break the law, or any agreements that may be in-place with the University of Hull or third parties.

3.6. Note that the following issues are not considered security vulnerabilities:
- Missing security headers that may be best-practice but do not impact on the security of the system.
- Support for older, but non-exploitable, protocols and cipher suites such as TLS 1.1.
- Fingerprinting and version detection.
- Out of date software, with no exploitable vulnerability.

4. Engagement

4.1. The University will respond to the reportee and acknowledge the initial report and its findings within 14 working days.

4.2. Ask the reportee to provide any further information to investigate the vulnerability if required.

4.3. Work with the reportee to confirm the vulnerability, the extent to which it affects the University, and provide an estimate of when the vulnerability may take to mitigate. Although it is the aim of the University to mitigate vulnerabilities within 90 days, some services/systems may be provided by partners or third parties and these could take longer.

4.4. Notify the reportee when the vulnerability has been mitigated or is still under investigation.

4.5. The University will acknowledge, and/or be happy to provide a reference to the reportee, for any proven and mitigated vulnerability.

4.6. Where appropriate, the University will release information to University members, partners, third parties, or the public to help others determine whether they are also affected by the reported vulnerability.

4.7. Review the vulnerability and update practises and processes in order to improve the security of systems and services.

4.8. The University will promise to not take any legal action against the reportee for accessing (or attempting to access) systems and services, as long as this policy has been followed.

4.9. Treat both the report and the data of the reportee as confidential, according to the **Data Protection Policy** available at hull.ac.uk/policies. The University will not pass personal data onto any third parties without permission.