Vulnerability Disclosure and Reporting Policy

Document Reference: IT-POL-105

Document Classification: Policy

Data Classification: Public

Version number: 3.0

Relevant CIS Control(s): 7.1, 7.2, 7.7

Status: Approved

Approved by (Board): University Leadership Team

Approval date: 03 June 2025

Effective from: 03 June 2025

Review Frequency: Annual

Next review date: 03 June 2026

Document author: Cyber Security

Document owner: Director of Technology

Contact: IT Services

Collaborative provision: No

State whether this document is applicable to the University's collaborative partners

Related documents: Information Security Controls Policy, Data Breach Policy

University document: No

A University document applies across the institution, is approved by a committee of Council or Senate and is held in the University Policy Directory on SharePoint.

Published location: Public Website

- The University has adopted the principles of Designing for Diverse Learners, and all policy documents should be written with reference to these principles. Further information is available at the Designing for diverse learners website.
- An Equality Impact Assessment (EIA) must be considered for all new and amended policies. Further information is available from the EIA section of SharePoint.
- This document is available in alternative formats from policy@hull.ac.uk.

Vulnerability Disclosure and Reporting Policy

Table of Contents

Vulnerability Disclosure and Reporting Policy

1 Introduction

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

1.2 Protecting systems and data from security weaknesses, or vulnerabilities, is of the upmost importance to the University. This involves identifying and addressing anything 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 or public internet protocol (IP) address space.

3 Disclosure and Reporting

3.1 University members that discover a vulnerability in a university system or service should report it via the support portal or via csirt@hull.ac.uk.

3.2 Security researchers, and non-University members, that discover a vulnerability in a university system or service should report it to csirt@hull.ac.uk.

3.3 When reporting a vulnerability, it is asked that the reportee does not remain anonymous so that we can proactively engage to confirm the vulnerability.

3.4 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.

3.5 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.

3.6 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.

3.7 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.
- 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 The University will ask the reportee to provide any further information to investigate the vulnerability if required.

4.3 The University will work with the reportee to confirm the vulnerability, the extent to which it affects the University, and provide an estimate of how long it may take to mitigate the vulnerability. 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 The University will 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 The University will review the vulnerability and update practises and processes 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, providing this policy has been followed.

4.9 The University will treat both the report and the data of the reportee as confidential, according to the **Data Protection Policy** available at hull.ac.uk/policies.

4.10 The University will not pass personal data onto any third parties without permission.

5 Responsible, Accountable, Consulted, and Informed (RACI) Matrix

5.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[1]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[2]. A brief definition of each role is given in the table below.

5.2 The table below outlines the roles that are involved in ensuring this policy is adhered to, enforced, and kept up to date.

	Definition	Role
Responsible (R)	Answerable for the correct completion of the task	End Users / the 'reportee' *(Section 3: Disclosure and Reporting)* IT Services *(Section 4: Engagement)*
Accountable (A)	Delegates and must sign off (approve) the work that those *responsible* provide	Director of Technology
Consulted (C)	Provide input based on how this will impact their domain of expertise	Information Governance Committee
Informed (I)	Those who are kept up to date on progress	End Users / the 'reportee'

6 Version Control

Version	Author	Date approved	Relevant section(s)
1.0	Steph Jones	11 October 2021	All
2.0	Hollie Huxstep	02 January 2024	All
3.0	Hollie Felice, Carl McCabe	08 May 2025	All

[1] https://www.forbes.com/uk/advisor/business/software/raci-chart/
[2] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/