APPENDIX 3

Vulnerability Disclosure Procedure

Date: December 2021

Version: V1.0

APPENDIX 3

Document Version Control

Document Version Control		
Version	**Date**	**Approved by**
1.0	November 2021	Information Governance Group – 2 December 2021
1.0	March 2022	Audit Panel – 15 March 2022

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. INTRODUCTION

1.1 This vulnerability disclosure procedure applies to any vulnerabilities you are considering reporting to us Tameside Metropolitan Borough Council (the "Council"). We recommend reading this vulnerability disclosure procedure fully before you report any vulnerabilities. This helps ensure that you understand the procedure, and act in compliance with it.

1.2 We actively encourage and support working with ethical security researchers and security professionals to improve our online security.

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

2. REPORTING

2.1 Please report any security vulnerabilities to us via the contact method(s) below: security@tameside.gov.uk

Please do not include any sensitive information in your initial message, we will provide a secure communication channel in our reply to you.

2.2 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”; and
- Steps to reproduce the vulnerability.

3. WHAT TO EXPECT

3.1 After you report a vulnerability to the Council, you will receive an acknowledgement reply usually within 5 working days of your report being received.

3.2 The team will triage your report and respond as soon as possible to let you know whether further information is required, whether the vulnerability is in or out of scope, or is a duplicate report. If remediation works are necessary, it will be assigned to the Council’s appropriate teams and/or supplier(s), supported by the Council’s Cyber Security Team.

3.3 Priority for bug fixes and/or mitigations will be assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage and/or address. You are therefore welcome to enquire on the status of your report, but should avoid doing so more than once every 14 days; this will allow our teams to focus on the reports and mitigation work as much as possible.

3.4 When the reported vulnerability is resolved, or remediation work is scheduled, the Council’s Cyber Security Team will notify you; in some case’s you may be invited to confirm that the remediation work carried out covers the vulnerability adequately.

3.5 You are particularly invited to give us feedback on our disclosure handling process, the clarity and quality of the communication relationship, and of course the effectiveness of the vulnerability resolution. This feedback will be used in strict confidence to help us improve our processes for handling reports, developing services, and resolving vulnerabilities.

4. GUIDANCE

4.1 **You must not:**

- Access unnecessary amounts of data. For example, 2 or 3 records is enough to demonstrate most vulnerabilities, such as an enumeration or direct object reference vulnerability;
- Use high-intensity invasive or destructive technical security scanning tools to find vulnerabilities;
- Violate the privacy of Council users, staff, contractors, services or systems. For example by sharing, redistributing and/or not properly securing data retrieved from our systems or services;
- Communicate any vulnerabilities or associated details using methods not described in this procedure, or with anyone other than their assigned Council security contact;
- Modify data in Council's systems or services, which do not belong to the researcher.
- Disrupt Council services or systems;
- Social engineer, 'phish' or physically attack the Council's staff or infrastructure;
- Disclose any vulnerabilities in the Council's systems or services to third parties or the public, prior to the Council confirming that those vulnerabilities have been mitigated and/or rectified;
- This is not intended to stop you notifying a vulnerability to 3rd parties for whom the vulnerability is directly relevant;
  (An example would be where the vulnerability being reported is in a software library or framework. Details of the specific vulnerability as it applies to the Council must not be referenced in such reports. For clarification about whether or when you can notify third parties, contact us, making sure the subject is "VDP"); and
- Require financial compensation in order to disclose any vulnerabilities (such as holding an organisation to ransom).

4.2 **You must:**

- Delete securely any and 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; and
- If at any time you are unsure if your intended or actual actions are acceptable, you should contact the Council's Cyber Security Team for guidance.

5. LEGALITIES

5.1 This procedure is designed to be compatible with common good practice among well-intentioned security researchers. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the Council to be in breach of any of its legal obligations, including but not limited to (as updated from time to time):

- The Computer Misuse Act (1990);
- The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018; and
- The Copyright, Designs and Patents Act (1988).

5.2 The Council affirms that it will not seek prosecution of any security researcher who reports any security vulnerability on a TMBC service and/or system, where the researcher has acted in good faith and in accordance with this disclosure procedure.

6. FEEDBACK

6.1 If you wish to provide feedback or suggestions on this procedure, contact the Cyber Security Team. The procedure will be updated from time to time; your input is therefore welcome and

will be valued to ensure that the procedure remains clear, complete, and relevant. This procedure was originally adapted from the MoJ Vulnerability Disclosure Policy, which is made available under the Open Government Licence v3.0.