VULNERABILITY DISCLOSURE PROCEDURE

Purpose and Scope

This procedure is intended to cover research activities that lead to the discovery of previously unknown technical vulnerabilities in software, hardware, or related computer systems. If such a vulnerability is discovered during research, the steps below should be followed to ensure a consistent approach prior to any public disclosure. Public disclosure can include the submission of a research paper, a public presentation, or any similar actions where information about the vulnerability is made available outside the University.

If any discovery relates specifically to University systems, contact QUB Information Services.

This procedure is intended to cover cyber security vulnerabilities. It is not intended to manage issues around experiments involving human participants, clinical trials, processing of personal data, etc. Established University ethics procedures apply in such circumstances.

Disclosure Procedure

A summary of the vulnerability disclosure procedure is outlined in the flowchart in Figure 1.

1. **Vulnerability Discovered**
   Researcher discovers a security vulnerability during their research activities which they intend to publicly disclose (e.g. through a research publication).
2. **Inform Line Manager/Supervisor**
   The researcher who discovered the vulnerability will:
   - Provide their line manager/supervisor documentation describing the vulnerability.
   - Consult with their line manager/supervisor before commencing each subsequent step in the procedure and retain documentation about actions taken at each step.
3. **Identify Contact Point**
   The researcher should identify an appropriate contact in the organisation/vendor, to whom they can report the vulnerability. Contact methods could include but are not limited to using the contact information in the Coordinated Vulnerability Disclosure policy of the owner or vendor, the security.txt contact information, emailing security reporting emails (e.g. security@ or secure@ email addresses), or filing support tickets.
4. **Notify CSIT Ops Committee**
   The line manager/supervisor will notify the CSIT Ops Committee that a vulnerability has been found, a summary of the vulnerability and impact, details about the vendor of the affected system, and the contact point that will be used.

   Initial notification can be made by emailing csit@qub.ac.uk

   If any concerns arise during subsequent stages, CSIT Ops should be consulted.
5. **Send First Disclosure Notification**
   Send notification using the template provided (Appendix A), copying line manager/supervisor in CC when email is used. The principal aims are to communicate in an open and non-confrontational way that:

- a vulnerability was found in a scientific environment during a research project,
- a deadline for publication of the reported issue is being proposed to prevent an impasse if no response is received,
- you are willing to negotiate the publication date, pending response and remediation actions.

6. **Send Follow-up Reminders After 21 Days and 60 Days**
   If there is no response after 21 days and again after 60 days, send a reminder using the template provided (Appendix B & Appendix C), copying line manager/supervisor in CC.

   At Day 21, in addition to contacting the vendor, distributor reporting mechanisms, if available, should be used to report the vulnerability. For example, if a vulnerability is found in an app, Apple can be informed using this link and Google Play via this link (links correct at time of publishing).

7. **Response Received**
   If a response is received, coordinate with vendor to set deadlines for publication or public disclosure (e.g., 90 days after disclosure to the vendor).

   Discuss and work with affected parties to design and test potential mitigation and fixes for the discovered vulnerabilities (if the required effort is reasonable).

   Depending on the nature of the vulnerability there may be different paths leading to public disclosure: 1) disclose the vulnerability publicly, 2) disclose it directly to the people using the affected system, or 3) issue a limited disclosure first, followed by a full public disclosure. Work with the contact to determine which approach is most appropriate.

   In case of mitigating circumstances, it is possible to extend the 90 day deadline. Researchers must confirm with their line manager/supervisor any decisions to extend disclosure or publication deadlines.

8. **Public Disclosure**
   Scenario 1 – A response was received and an agreement with the affected vendor has been reached regarding the timing and details of public disclosure:

   - Publication can proceed as agreed with vendor.

   Scenario 2 – A response was received but 90 days (or an agreed extended deadline) has expired without an agreed fix or other agreed input being provided by the vendor:

   - Notify the contact that the deadline has expired and that disclosure will proceed as previously communicated.

   Scenario 3 – 90 days have expired since the first disclosure to the vendor but no response has been received:

   - Notify the contact of the intent to disclose the reported issue.

   In each scenario, before disclosure, the line manager/supervisor must notify CSIT Ops of the intention to proceed with/without a response being received from the vendor.

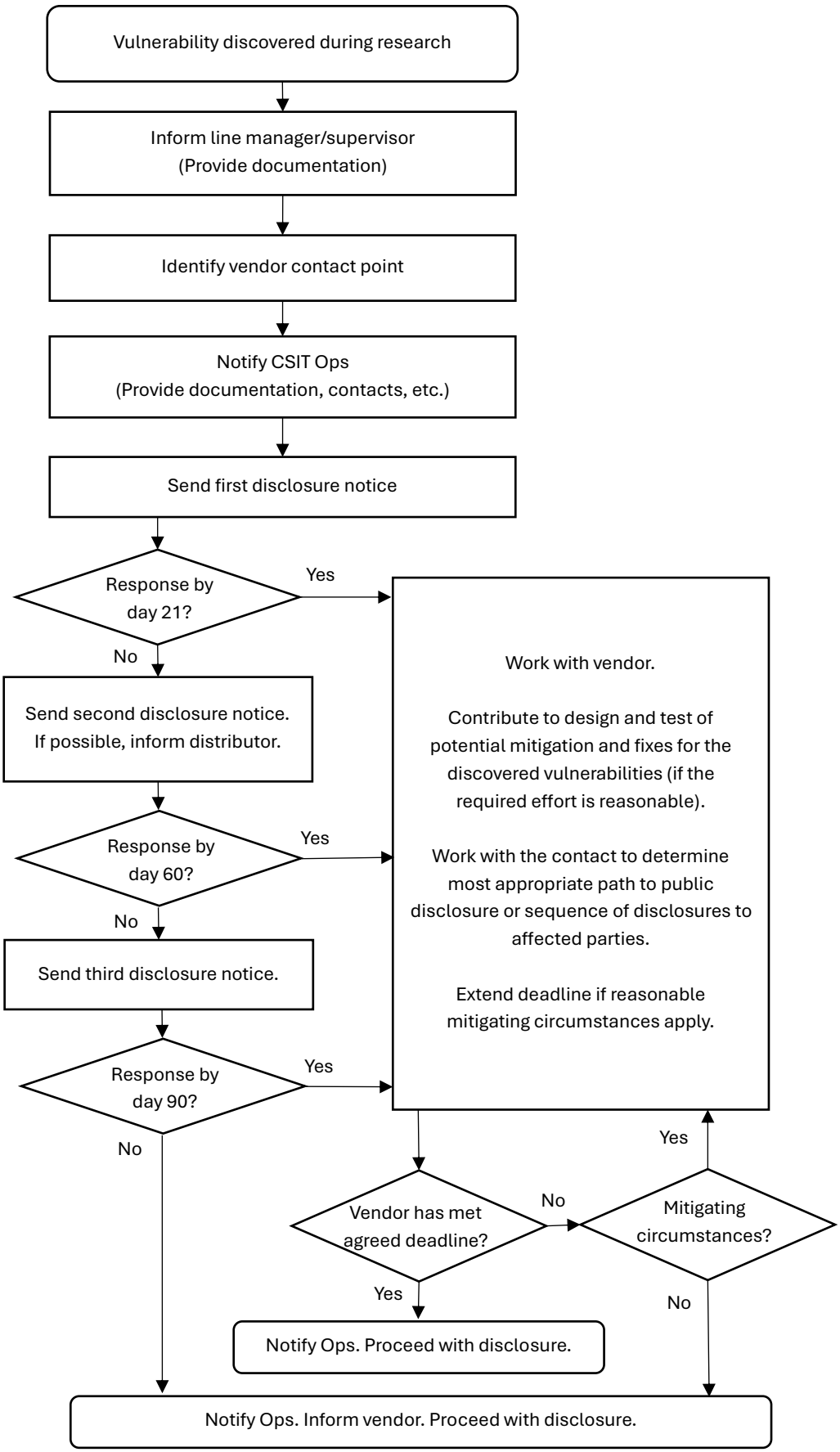

Figure 1: Flowchart summary of disclosure procedure

FURTHER NOTES:

Recording Communications
Keep a record of all steps above and all related communications. Communication must be via official University email accounts.

Advice and Internal Notification - CSIT Ops Committee
Throughout the process, the CSIT Ops Committee should be the first point of contact for a research team seeking advice.

- For further escalation, the committee will seek advice or support from appropriate University contacts, such as the Research Governance, Ethics and Integrity team, advisory boards, or the National Cyber Security Centre if required.
- If significant concerns arise at any stage, the committee may ask the research team to delay disclosure or not to publish.

APPENDIX A – FIRST CONTACT EMAIL TEMPLATE

Dear Sir/Madam,
As part of a cyber security research project at Queen's University Belfast, we have been conducting research into the security of [PRODUCTS/SERVICES], such as [THE VENDOR'S PRODUCT/SERVICE].

The study has revealed a security issue that might require your immediate attention. We think we have found a way to [GENERIC DESCRIPTION OF THE IMPACT OF THE VULNERABILITY]. These findings have been kept confidential and our aim is to align our research with the vulnerability disclosure approach recommended by the UK's National Cyber Security Centre, NCSC [1].

We would like to show these outcomes to you to enable you to resolve these issues first, prior to our planned disclosure of this information [PUBLICLY/TO AFFECTED PARTIES/IN A RESEARCH PAPER], after 90 days have expired. We are willing to work with you on [WORKAROUNDS/FIXES/TESTING]. Thus, we invite you to get in touch with us by responding to this email.

Regards,
[Researcher]

Centre for Secure Information Technologies (CSIT)
Queen's University Belfast

[1] https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit

APPENDIX B – 21 DAYS FOLLOW UP EMAIL TEMPLATE

Dear Sir/Madam,
Unfortunately, we have not received any response from you yet.

As is common practice in the disclosure of vulnerabilities discovered through research, we intend to continue with publication of our findings following 90 days since our initial email of [DATE OF FIRST EMAIL].

Should this timeline not be appropriate for you, please let us know and we can discuss a more suitable timeline.

Regards,
[Researcher]

Centre for Secure Information Technologies (CSIT)
Queen's University Belfast

APPENDIX C – 60 DAYS FOLLOW UP EMAIL TEMPLATE

Dear Sir/Madam,
Unfortunately, we have not received any response from our previous emails related to the discovery of the vulnerability described below.

As is common practice in the disclosure of vulnerabilities discovered through research, we intend to continue with publication of our findings following 90 days since our initial email of [DATE OF FIRST EMAIL], which is 30 days from today.

We emphasise that it is our intention to work with you regarding mitigation actions and appropriate timing of public disclosure of the vulnerability and would welcome a response from you.

Regards,
[Researcher]

Centre for Secure Information Technologies (CSIT)
Queen's University Belfast