UT POLICY FOR *COORDINATED VULNERABILITY DISCLOSURE* IN RESEARCH

JEROEN VAN DER HAM, ANDREA CONTINELLA, PETRI DE WILLIGEN, DENNIS REIDSMA

MARCH 22, 2023

UNIVERSITY OF TWENTE.

COLOPHON

FILENAME
University of Twente Policy for *Coordinated Vulnerability Disclosure* in Research

DATE
March 22, 2023

VERSION
1.2

STATUS
Established by Executive Board on March 27, 2023

AUTHOR(S)
Jeroen van der Ham, Andrea Continella, Petri de Willigen, Dennis Reidsma

EMAIL
ethicscommittee-cis@utwente.nl

DEPARTMENTS
Ethics Committee Computer & Information Sciences (EC-CIS, faculty EEMCS)
Strategy & Policy (SP)

POSTAL ADDRESS
P.O. Box 217
7500 AE Enschede

WEBSITE
www.utwente.nl

DOCUMENT HISTORY

Version	Date	Processed by	Changes/Remarks
0.0	28-10-2022		Discuss intended policy and decision making process between authors and SP (Te Kulve, Greven).
0.1	06-11-2022	Authors (Van der Ham, Continella, De Willigen, Reidsma), Tews	First draft version.
0.2	14-11-2022	De Willigen	Processed advice and review comments from SP (Greven) and authors (Van der Ham, Continella, Reidsma).
0.3	18-11-2022	De Willigen	Processed advice and review comments from LISA (Swaters): added reference to LISA's RD-policy. Changed Appendix A to the full website text.
0.4	29-11-2022	Reidsma	Processed advice and review comments from LISA (Swaters): added the word "research" to title to clearly distinguish from LISA's RD-policy.
0.5	5-12-2022	Reidsma	Processed advice and review comments from M&C: include types of vulnerabilities, check readability with LISA's communication advisor and students, advices on awareness of policy within faculty, advices on important role of lecturers/researchers in informing students. Positive advice from EC-HSS.
0.6	5-12-2022	Reidsma	Processed advice and review comments from LISA contract manager (Meijer) and text proposals SP (Greven): responsibility of UT and duty of care of UT towards employees, delineation of the scope of activities, what to do when disclosing a vulnerability requires consideration/consultation. Positive advice from GA (Van Roosmalen) on legal support.
0.7	5-12-2022	Reidsma, De Willigen	Processed advice and review comments from UWEC/EC-NES: role of EC-CIS (advising and maintaining policy document).
0.8.1	5-12-2022	Continella, Van der Ham, Reidsma	View on processed advice and review comments UWEC/EC-NES, LISA/Legal, M&C by authors.
0.8.2	6-12-2022	Reidsma, De Willigen	View on outstanding questions in 0.8.1 by SP (Greven).
0.9	6-12-2022	De Willigen	Processed comments on keeping a register and archive of concluded Coordinated Vulnerability Disclosure cases.
0.9.2	7-12-2022	Greven	Formatting changes, version for UC-Oz
0.10	23-12-2022	Reidsma, De Willigen, Van der Ham, Continella	Processed advice and review comments from LISA's communication adviser (Melching): include risks, rethink focus of text templates and take into account tips for implementation process. Processed input from PhD student. Processed advice and review comments HR (Hooftman en Wever): applicability to guest-WP and implementation advices. Processed advice UCOz: clarity as to which types of research are targeted by this policy; highlight relation to Dutch regulations; availability of support for researcher; and role of FB in communicating and implementing the policy. View SP (Greven) on aforementioned advices and outstanding questions.
0.10.1	13-01-2023	De Willigen	Integrated suggested changes and resolved most comments.
0.10.2	16-01-2023	Reidsma	Cleanup.
1	16-01-2023	Greven	Formatting changes, version for intended decision Executive Board.
1.1	30-01-2023	Greven	Editorial (removing abbreviation), version for U-Council.
1.2	22-03-2023	Reidsma, Greven	Version for final decision Executive Board March 27, 2023. Advices U-Council (attention to applicability, providing examples and providing a decision scheme) are taken into account in this version of the policy and the final website.

TABLE OF CONTENT

1. Scope and goal 4
2. Responsibilities 5
   2.1 Students 5
   2.2 Researchers, teachers, and supervisors 5
   2.3 UWEC and EC-CIS 5
   2.4 Faculty Boards 5
   2.5 Executive Board 5
3. Procedure for conducting the disclosure 6
4. Resources 6
5. Appendices 7
   A. Text for UT website / service portal 7
   B. Templates for notifications 8

1. SCOPE AND GOAL

This policy document gives (security) researchers and students clear guidelines for conducting vulnerability discovery activities during their research and conveys the University's preferences on coordinating with vendors to disclose and mitigate the discovered vulnerabilities. This policy is in line with the national guidelines of the National Cyber Security Centre and the guidelines of the public prosecutor's office (see Section 4). The disclosing procedure will be published on the UT website/service portal, together with frequently asked questions with more detailed example situations including applicability, a decision scheme with considerations and the available support, and a statement for vendors to ensure transparency (see Appendix A).

Terminology and examples

Vulnerabilities are (technical) security flaws in computer systems (e.g., software or hardware) that can allow malicious actors to violate the confidentiality, integrity, or availability of ICT systems. For example, a flaw in the code of a web-based application may allow cybercriminals to inject arbitrary SQL commands into an HTTP request and thus access or modify the underlying database.

Vulnerability discovery means finding out about possibly unknown vulnerabilities in ICT systems. This can, for example, be a result of research on security testing or internet network properties, or research on people's susceptibility to social engineering techniques such as spear-fishing, but many other activities can also lead to the discovery of vulnerabilities in systems.

Vulnerability disclosure refers to the process of communicating about the discovered weaknesses with affected parties, among which vendors of affected systems, organisations hosting systems and content, and end users affected by the risks of such vulnerabilities (for example, information leak or system damage). First, vendors must know about the vulnerability if they are to fix or mitigate it, and second, users of the affected systems must be aware that their systems are at risk until a solution by the vendor is deployed. The disclosure must be carried out *in coordination with* parties involved, especially the owner or vendor of a system, in order to, for example, ensure that disclosure happens in a timely manner while giving the vendor enough information and time to resolve the issue before widely publishing its existence. A procedure is described in Section 3.

The **purpose** of the disclosure is to contribute to the security of ICT systems by sharing knowledge about vulnerabilities and their mitigation. This contribution to ICT security awareness is a shared responsibility. The starting point of the policy is an equal discussion between the researcher, the University, and the affected vendors. The University has a duty of care to facilitate the researcher in this process.

The **intent** is to disclose vulnerabilities in the most helpful way to the community by ensuring confidentiality during the process, working with affected parties to find and test fixes, and aiming to inform all the impacted entities so that they can protect themselves by deploying patches and updating their systems. The researcher (student or employee) discovers the vulnerability and knows the technical details; the other party has the means and motivation to fix or mitigate the vulnerability.

This policy **applies** to all employees and students of the University of Twente conducting research at the University's premises or on behalf of or under the responsibility of the University of Twente (including, e.g., guest employees who conduct research under the responsibility of the UT or UT-employees at other locations). More detailed example situations including applicability can be found on the UT website/service portal. The policy applies to vulnerabilities discovered as part of research at the University, usually in systems of parties other than the University.

The University also has a complementary policy regarding vulnerabilities discovered in the University's own systems. That complementary policy applies to the role of the University as the owner who must resolve the vulnerability rather than as the discoverer of the vulnerability. See the ***University's responsible disclosure policy*** concerning vulnerabilities in the University's own systems.[1,2]

[1] https://www.utwente.nl/en/cyber-safety/cybersafety/legislation/responsible-disclosure.pdf

[2] If a weak spot is discovered in one of the systems of the University of Twente, you can contact LISA so that the University can take measures as soon as possible.

2. RESPONSIBILITIES

2.1 STUDENTS

Students are expected to immediately report a vulnerability to their teacher or supervisor whenever they identify a vulnerability when performing activities at or on behalf of the University of Twente (e.g., during a course or while preparing their thesis).

2.2 RESEARCHERS, TEACHERS, AND SUPERVISORS

Teachers and **supervisors** (or to whom this part of the policy applies) are responsible for making students aware of the importance of, and procedures for, Coordinated Vulnerability Disclosure. Furthermore, they are responsible for conducting the Coordinated Vulnerability Disclosure procedure for the vulnerabilities reported to them by their students. **Researchers** (or to whom this part of the policy applies) are responsible for conducting the Coordinated Vulnerability Disclosure procedure for the vulnerabilities they find. All researchers, teachers and supervisors can contact EC-CIS for advice in any part of the procedure; EC-CIS can also point them to other available support (see 2.3 and 2.5).

While conducting the procedure as described in Section 3, the staff member is expected to:

- Keep a record of all communications concerning the disclosure, stored in a secure location (also see section 3)
- Keep the details of the case confidential
- Make a reasonable effort to find and contact the owner or vendor
- Be open to negotiating with the owner or vendor about the publication date in cases where 90 days are not sufficient to release proper patches
- Discuss and work with affected parties to design and test potential mitigation and fixes for the discovered vulnerabilities
- Discuss and work with the owner or vendor to determine the most appropriate path leading to eventual disclosure (e.g., full public disclosure, limited disclosure to affected parties only, or limited disclosure followed by full disclosure)
- Disclose the vulnerabilities to all affected parties
- At least contact the EC-CIS and possibly the NCSC when the owner or vendor does not react, is unwilling to cooperate, if multiple vendors are involved, or if there are other reasons to consider the case a high-stakes procedure.

2.3 UWEC AND EC-CIS

The EC-CIS will offer advice to researchers and the other Ethics Committees where needed. The EC-CIS keeps in contact with the National Cyber Security Centre (NCSC), such that they can help the researcher ask for extra support if a case is too large, complex, or if the researcher has difficulties in reaching affected parties.

The University-Wide Ethics Committee (UWEC) is responsible for keeping a register of all concluded vulnerability disclosure cases reported by the researchers (see step 8 in the procedure in Section 3) and will report confidentially on this in their yearly report to the Executive Board. They delegate this task to the Ethics Committee Computer & Information Science (EC-CIS).

The EC-CIS is in the lead for maintaining the university-wide policy texts. This committee will keep up to date with (inter)national standards around disclosure procedures and review the disclosure policy periodically. The EC-CIS performs this role based on their expertise and on behalf of UWEC. With that, the other Ethics Committees are not burdened with extra tasks.

2.4 FACULTY BOARDS

The Faculty Boards are responsible for an appropriate level of measures to ensure implementation of the policy within the faculties, such as creating awareness in a recurring manner amongst all those involved in the process to the extent that the activities in the faculty require. The Ethics Committee facilitated by the faculty can play a role in that, and the EC-CIS can advise on how to do that. The Faculty Board EEMCS guarantees there is sufficient expertise in Coordinated Vulnerability Disclosure when appointing members of the EC-CIS.

2.5 EXECUTIVE BOARD

The EB establishes the University-wide policy. In addition to faculties, the policy will be shared with service departments involved and, if and where applicable, incorporated in UT-regulations. While performing the process, the reporter is supported in terms of M&C, HR, or legal support, as usual.

3. PROCEDURE FOR CONDUCTING THE DISCLOSURE

As mentioned above, the researcher, teacher, or supervisor conducts the Coordinated Vulnerability Disclosure procedure. In any case that the employee needs advice or support, but at least in the case that the owner or vendor does not react or is unwilling to cooperate, or if multiple vendors are involved, the researcher, teacher, or supervisor is strongly advised to contact the EC-CIS (ethicscommittee-cis@utwente.nl) for support. If necessary, the EC-CIS can help them contact the National Cyber Security Centre (NCSC).

If a weak spot is discovered in one of the systems of the University of Twente, you can contact LISA so that the University can take measures as soon as possible. For that, see the ***University's responsible disclosure policy****.*[1]

The steps within the procedure to be performed by the researcher:

1. Keep a record of all communications concerning the Coordinated Vulnerability Disclosure in a secure location. Mailing from the official UT Microsoft account may serve as a secure location.
2. Search for the right contact for reporting a vulnerability, taking steps to find the right way to securely get in touch with them. 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 (security@ or secure@), filing bugs without confidential details in bug trackers, or filing support tickets.
3. Send out the first notification and, if necessary, reminders after 21 days and 60 days. Appendix B gives templates for notifications to report vulnerabilities to affected parties. As stated in the templates, it is important that the report:
    a. includes that the vulnerability was found in a scientific environment during a research project;
    b. proposes a deadline for publication of the reported issue to prevent deadlock because of no response;
    c. states that you are willing to negotiate publication date, pending response and remediation actions;
    d. is written in a friendly and open tone.
4. In case of no reply from vendors, try to contact software distributors. For instance, in case of vulnerabilities found in an Android app present in the Google Play Store, contact Google.
5. If necessary, negotiate with the vendors to set a publication date.
6. If no fix is available at the end of the agreed publication date (e.g., after 90 days), notify the contact of the intent to disclose the reported issue. In case of mitigating circumstances, it is possible to extend the deadline.
7. When either the issue is fixed or the (extended) deadline is expired, disclose the vulnerability. Depending on the nature of the problem, there may be a few paths leading to eventual disclosure: 1) disclose the vulnerability publicly, 2) disclose it directly to the people using the project, 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 each case.
8. Register the conclusion of the Coordinated Vulnerability Disclosure procedure with all documentation with the EC-CIS.

4. RESOURCES

- Final website with updated information about the policy for Coordinated Vulnerability Disclosure in research: [link to be included here].
- Responsible disclosure policy LISA, University of Twente: https://www.utwente.nl/en/cyber-safety/responsible/
- Facebook: https://www.facebook.com/security/advisories/Vulnerability-Disclosure-Policy
- The 'Leidraad' of the National Cyber Security Centre (version of 2018 is currently being updated): https://www.ncsc.nl/contact/documenten/publicaties/2019/mei/01/cvd-leidraad
- Public Prosecutor's Office (OM): https://www.om.nl/documenten/richtlijnen/2020/december/14/om-beleidsbrief-ethisch-hacken
- OECD: http://oe.cd/security
- EU NIS2 (still in draft): https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf https://www.nis-2-directive.com/

5. APPENDICES

A. TEXT FOR UT WEBSITE / SERVICE PORTAL

POLICY FOR COORDINATED VULNERABILITY DISCLOSURE IN RESEARCH
[text based on Section 1 of the Policy, including decision scheme]

PROCEDURE FOR CONDUCTING THE PROCEDURE FOR RESEARCHERS
[see Section 3 of the Policy]

PUBLIC DISCLOSURE STATEMENT FOR VENDORS

Summary

We immediately contact the appropriate responsible party/vendor and inform them of the security vulnerabilities we found. We expect the affected party to respond within 21 days and let us know how the flaws will be mitigated to protect users. We are willing to work together with the vendor to find ways to mitigate the issue. If we don't hear back within 21 days after reporting, we will explain our publication timeline and give them another opportunity to get in touch to discuss this timeline.

If no reasonable fix or update is available after 90 days from the reporting date, we consider disclosing the vulnerabilities publicly. Nonetheless, we are willing to negotiate the publication date in cases where 90 days are not sufficient to release proper patches.

Reporting

- We make a reasonable effort to find the right contact for reporting a vulnerability, taking steps to find the right way to securely get in touch with them. We will use contact methods including but 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 (security@ or secure@), filing bugs without confidential details in bug trackers, or filing support tickets.
- We expect contacts to acknowledge our reports as soon as possible and to confirm whether we provided sufficient information.
- We also might contact software distributors in case we receive no reply from vendors. For instance, in case of vulnerabilities found in an Android app present in the Google Play Store, we will contact Google.
- Where necessary, we will request assistance from the NCSC as coordinator for multi-party disclosure processes (e.g., involving many vendors).

Mitigation & Timeline

- When possible, we discuss and work with the affected party to design and test potential mitigation and fixes for the discovered vulnerabilities.
- If no fix is available at the end of the agreed publication date (e.g., after 90 days), we notify the contact of our intent to disclose the reported issue.
- If there are no mitigating circumstances, we disclose the issue as soon as we are reasonably able to do so.

Disclosure

- Depending on the nature of the problem, there may be a few disclosure paths: 1) we disclose the vulnerability publicly, 2) we disclose it directly to the people using the project, or 3) we issue a limited disclosure first, followed by a full public disclosure. We work with the contact to determine which approach is most appropriate in each case.
- Our intent is to disclose vulnerabilities in a way that is most helpful to the community. For example, we may include guidance on workarounds, methods for validating patches are in place, and other material that helps people contain or remediate the issue.
- We include a timeline to document communication and remediation actions taken by both parties. Where reasonable, our disclosure includes suggested steps for mitigating actions.

Additional considerations

- When negotiating publication dates, we evaluate each issue on a case-by-case basis based on our interpretation of the risk to people.

FREQUENTLY ASKED QUESTIONS
[Example cases, applicability, etc.]

B. TEMPLATES FOR NOTIFICATIONS

First notification:

Dear Sir/Madam,

As part of a project {counting towards a master's degree in Cybersecurity} from the University of Twente, {students/we} have been conducting research into the security of {Class of Products/services/research question}, such as {Your 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 all the rules stated by our Dutch National Cyber Security Centre (NCSC) [1] were adhered to during this research. We are planning to follow the procedure as outlined in our public disclosure policy [2].

We would like to show these outcomes to you and give you the chance to resolve these issues first, before we disclose this information {publicly/to affected parties}. We are willing to work with you on {workarounds/fixes/testing}. During our communication process, we aim to act according to the 'Coordinated Vulnerability Disclosure Guideline' referenced above. Additionally, we would like to discuss the possibility of a written indemnification statement.

Thus, we invite you to get in touch with us promptly by responding to this email.

Regards,

(Staff member)

[1]: https://english.ncsc.nl/get-to-work/implement-a-cvd-policy/finding-vulnerabilities-in-it-systems

[2]: link to Coordinated Vulnerability Disclosure policy at UTwente website

If there is no answer after 21 days, send a reply to the previous email:

Dear Sir/Madam,

Unfortunately, we have not received any response from you yet.

We will continue with publication of our findings in nine weeks from now ($DATE), as outlined in our public disclosure policy [1]. Should this timeline not be appropriate for you, please let us know and we can discuss a more suitable timeline.

Regards,

(Staff member)

[1]: link to Coordinated Vulnerability Disclosure policy at UTwente website

If there is still no answer on the second email after 60 days, send a reply to the previous email:

Dear Sir/Madam,

Unfortunately, we have not received any response from you after repeated emails reaching out to your organisation.

We write this email to inform you that we are planning to make our findings public in four weeks from now ($DATE), as outlined in our public disclosure policy [1].

Regards,

(Staff member)

[1]: link to Coordinated Vulnerability Disclosure policy at UTwente website

UNIVERSITY OF TWENTE
Drienerlolaan 5
7522 NB Enschede

P.O.Box 217
7500 AE Enschede

P +31 (0)53 489 9111

info@utwente.nl
www.utwente.nl