Ghent University coordinated IT vulnerability disclosure policy[1]

Employees and students of Ghent University, as well as third parties external to Ghent University, are **permitted** to actively detect vulnerabilities in the security of Ghent University's ICT infrastructure, insofar as this is done **in accordance with the provisions** of this (approved by the board) coordinated IT vulnerability disclosure policy.

Ghent University can provide **incentives** or rewards (campaign-wise or permanent, potentially for a defined scope) for those who report vulnerabilities in accordance with this policy. Ghent University will not pay rewards to Ghent University employees or students for reporting vulnerabilities on systems or applications under their own management.

Vulnerability detection should only be done with good intentions. Ghent University will not impose sanctions or take legal action against those who comply with the rules of this policy and do not engage in illegal actions.

The **scope** of this policy includes **the IT infrastructure of Ghent University with the exception of** websites, applications, systems, etc. that are **explicitly excluded**. The Information and Communication Technology (ICT) Department will indicate on the central helpdesk site what falls outside the scope of this policy and is therefore not eligible for the investigation of vulnerabilities. Actively searching for vulnerabilities in information systems that are excluded from the scope of this policy is unauthorized and may result in sanctions and/or legal prosecution.

Ghent University is committed to processing reports of vulnerabilities to the best of its ability and to providing appropriate remediation based on risk analysis, both in infrastructure centrally managed by the ICT Department and in decentrally managed infrastructure. In the event of a potential data breach or other incident involving confidential information or personal data, the persons concerned (and potentially authorities) will be informed appropriately.

Ghent University reserves the right to appoint an intermediary or coordinator and/or to deploy a central technical platform (managed by the ICT department) on which rewards for detecting and reporting vulnerabilities may also be offered, with the aim of establishing and maintaining a constructive relationship between the parties or potentially guarantee the anonymity of the participant.

In accordance with the regulations for the correct use of the ICT infrastructure of Ghent University[2], all ICT managers (both those of the ICT department and those of other departments within the central administration and those of faculties and academic departments) are **responsible for the security** of the systems and applications that fall under their authority. They must therefore actively detect vulnerabilities (or have them detected) in those systems and applications and remediate them (or have them remediated).

This policy can be referred to by ICT managers of Ghent University in order to have certain websites, applications and systems searched specifically for vulnerabilities, by other Ghent University employees, by Ghent University students or by third parties external to Ghent University.

[1] Coordinated Vulnerability Disclosure Policy (CVDP)

[2] https://codex.ugent.be?regid=REG000157&lang=en

Addenda

1. Reciprocal obligations

The ICT Department (DICT) will clearly communicate this policy, the scope of its application and the exceptions to it. The following will be published on DICT's central helpdesk site:

- Instructions on how to report detected vulnerabilities.
- The applications or systems that are not eligible for an investigation of vulnerabilities and therefore fall outside the scope of this policy.
- The available incentives or rewards, potentially specific to certain applications or systems (e.g. a bug bounty program with a potential reward or an entry in a responsible disclosure "Hall of fame").

As a participant in this policy, you adhere to the following rules:

- You only target applications and systems that fall within the scope of this policy.
- You do not disclose or communicate the vulnerability with others until it has been confirmed that the problem is solved.
- You do not abuse the situation: you only do the minimum to confirm that the vulnerability is present. You do not delete, modify, read or copy more data than is necessary to demonstrate the problem.
- You do not carry out malicious attacks on external systems from Ghent University's IT infrastructure.
  You delete all data obtained through the vulnerability immediately after the notification, particularly all personal data. You must also report any viewing of personal data.
- You may not perform any of the following actions:
  – intentional attempts to intercept communications or network traffic
  – placing malware or other hacking tools
  – downloading, copying, modifying or deleting data and/or passwords
  – making permanent or irreversible changes to a system
  – accessing systems unnecessarily or sharing access with others
  – automated scans that interfere with the proper functioning of applications in production
  – attempting to brute-force access to systems
  – attacking or bypassing physical security
  – phishing, social engineering, spamming
  – (distributed) denial-of-service attacks

2. For interested participants

If you discover a vulnerability in the security of Ghent University's ICT infrastructure, you must report that vulnerability as soon as possible. Exploiting the vulnerability or further disclosing it to third parties is prohibited.

Report any vulnerabilities discovered via the appropriate channel or IT platform.
Precise instructions will be published on the website of the helpdesk of the ICT Department (https://helpdesk.ugent.be) of Ghent University. Notification can be made, for example, to the DICT helpdesk, potentially cc'd to the person responsible for the system, or via an appropriate electronic vulnerability disclosure or bug bounty platform offered by DICT.

When reporting a vulnerability, you confirm that you have read this coordinated vulnerability disclosure policy and that you are operating in accordance with its provisions.

Make sure you can be contacted.

Information you need to provide when reporting a vulnerability is, for example: type of vulnerability, configuration details, actions performed, tools used, data of the tests, evidence, IP address or URL of the affected system, screenshot, contact details, etc.
Also provide details about confidential data or personal data of Ghent University to which you may have had access.

There are indicative maximum deadlines for each stage of the handling of reports. The sending of an acknowledgement of receipt to the participant is normally done within the week, the request and communication of additional information within 2 weeks, the investigation and development of a solution and the answer to the participant within 2 months, and potentially, the granting of a reward or the admission to publication within 3 months.

The abovementioned maximum periods remain flexible and can be shortened or extended depending on the complexity of the vulnerability, the number of systems affected, and the urgency or the severity of the situation.

Publication of issues discovered will always be permitted subject to compliance with a mutually agreed sufficiently long embargo (maximum 3 months).

3. Legal fineprint

This policy applies to Ghent University's IT infrastructure. Some parts of the IT infrastructure (certain websites, applications, devices, services, systems, networks,...) can be explicitly excluded and as a result, fall outside the permitted scope of targeted investigation. Third-party infrastructure such as cloud solutions used by Ghent University is always outside the scope. Vulnerabilities in such applications that are the result of specific (errors in) configurations by Ghent University do fall within the scope, unless otherwise specified.

The precise scoping for centrally managed ICT is carried out by the ICT department (DICT) and for non-centrally managed ICT by the responsible IT manager of other departments, academic departments or faculties, in consultation with the ICT department and is published on the helpdesk pages of DICT.

Vulnerability investigations of websites, applications, devices, services, systems or networks that have been expressly excluded may result in sanctions or legal proceedings against the participant. Third-party information systems are always excluded from the scope. The ICT department or the responsible IT manager must be addressed in advance in case the scoping is insufficiently clear or if there is doubt about this amongst potential participants.

Intentional attempts to record or take cognisance of communications that are not accessible to the public or attempts to intercept electronic communications are expressly prohibited. This prohibition does not apply to the content of communications obtained strictly accidentally by participants in the context of vulnerability detection.

The participant is prohibited from using, maintaining, disclosing or publishing computer data that he or she can reasonably believe to have been obtained illegally.

It is also prohibited to install or have installed a device that allows the interception, access or recording of communications that are not accessible to the public. Such a device may, however, be used for academic teaching or investigation in a strictly controlled network environment and with the consent of all participants in the communication.

Each participant undertakes to comply with the principle of proportionality in its actions, i.e. not to disrupt the availability of the services provided by the system and not to exploit the vulnerability beyond what is strictly necessary to demonstrate the security problem. If the problem has been demonstrated on a small scale, no further action should be taken.

Ghent University data, including any personal data, may only be processed by the participant to the extent strictly necessary to demonstrate the IT vulnerability. The data may not be kept longer than necessary. The participant must report to Ghent University exactly which (categories of) data are involved, justify why they may have been processed further and ensure that this data is kept safe during this period.

The participant may not share the collected information with third parties or distribute it to third parties without the express permission of Ghent University.

This policy does not aim to enable intentional access to the content of computer, communication or personal data. Such access should only take place accidentally and occasionally in the context of the detection of vulnerabilities in the infrastructure and technologies concerned.

Ghent University undertakes to implement this policy for coordinated disclosure in good faith and to prosecute the participant who complies with its conditions neither civilly nor criminally.

On the part of the participant, there must be no fraudulent intent, intent to harm, or the will to use or cause damage to the visited system or its data.

In terms of the tools enabling a computer data breach, the participant may develop, possess or make available such tools in the context of participation in a vulnerability disclosure policy. Those actions are not unlawful as long as they are justified by legitimate purposes related to the detection of vulnerabilities with the consent of the organization of the person responsible for the computer system concerned.

Any request for a reward outside the conditions determined by the present policy or the potential bug bounty platform that coordinates the technical and administrative aspects of the reward programme can be treated as (an attempt to) commit criminal offences (e.g. extortion).

Any disclosure of the vulnerability must be coordinated and synchronised between the parties, in order to give Ghent University or other parties involved sufficient time to address the problem.

References and sources:

CCB guide on the coordinated vulnerability disclosure policy (2020)
"Part I: Good practices" en "Part II: Legal aspects"

ENISA Good Practice Guide on Vulnerability Disclosure (November 2015)

NCSC Coordinated Vulnerability Disclosure: the Guideline (October 2018, in Dutch)