This document is to be seen as a guideline to help the Expert Committee in their decision-making.
The Expert Committee is allowed to deviate from this guideline.
Abbreviations: CoCo = Computer Committee, KasCo = Audit Committee.

Guidelines Ethical hacking

What does Thor expect from a hacker?

1. **Ethical conduct:** It is assumed that the hacker wants to improve the association by uncovering any mistakes, therefore no irreversible changes shall be made. This includes the prohibition, unless explicitly stated otherwise by the Expert Committee, to:
   - **a.** Preserve obtained information after the settlement of the case
   - **b.** Make irreversible changes to data and/or systems
   - **c.** Share findings and/or access with third parties
   - **d.** Hold back relevant information

2. **Quick and clear notification:** After a successful hack the Expert Committee (expertcommissie@thor.edu) must be informed. If the hack concerns any finances, the Expert Committee will also inform the Kasco. Informing the Expert Committee means the following:
   - **a.** Delivering a concise step-by-step plan on how to reproduce the hack, including a summation of what the hacker has gained access to within 24 hours.
   - **b.** A detailed report within a week, which includes:
     - **i.** A detailed step-by-step plan on how to reproduce the hack
     - **ii.** A rough description on how the hack was found
     - **iii.** A detailed summary of what access has been obtained
     - **iv.** Possibly a suggestion for a solution

3. **Discretion**
   - **a.** The hacker keeps all information private until the Expert Committee has decided, in consultation with the CoCo, and, if relevant, the KasCo, if the knowledge can be shared.
   - **b.** Gathered information will not be shared with third parties.
   - **c.** Any obtained information or data will be deleted by the hacker after the hack has been settled with the Expert Committee. The detailed report can be saved and shared, under the condition that it does not contain any sensitive information.

What can a hacker expect from Thor

1. **Reward.** The Expert Committee decides, in consultation with the CoCo and if relevant the KasCo, the size of the reward.
2. **Professional treatment.** The Expert Committee will support the hacker in informing the association about the hack.
3. **Swift settlement.** The Expert Committee will make sure that the case is settled within 3 weeks, if at all possible, after being notified of a hack and the discovered mistakes will be solved by the responsible committee.
4. **Discretion.** In case the hacker wishes to stay anonymous, the Expert Committee will ensure the identity of the hacker will only be made known to the people to whom this is absolutely necessary. This can, for example, be the CoCo who needs to be able to discuss with the hacker about a solution.

What is the definition of a hack?

A hack is understood as an action that meets one or more of the following criteria:

- a. Granting and/or acquiring access to digital data and/or systems outside the appropriate channels
- b. Influence the availability of digital data and/or systems outside of the appropriate channels

This document is to be seen as a guideline to help the Expert Committee in their decision-making.
The Expert Committee is allowed to deviate from this guideline.
Abbreviations: CoCo = Computer Committee, KasCo = Audit Committee.

Rewards Ethical Hacking

In this system, the bugs are divided in four main categories to emphasize the impact of larger bugs and reward them in a larger fashion, but also to reward finding multiple small hacks.

Unimportant data is seen as data that is allowed to be known with all Thor-members and non-members, like quotes, memes or photos.
Important data is seen as data that should only be known by a select group of people, like finances, personal data, passwords or data from the Board.

Committee members who are (partially) responsible for the digital systems of Thor, among others the Board, the CoCo, the Expert Committee, the WebCo and the LANCo, will be excluded from the rewards mentioned below. In case of disagreement, the Expert Committee will decide.

1. Small bugs, 4 consumption units
    - Access to unimportant data
    - Retrieving debug output of individual commands
    - Significant visual bugs
2. Average bugs, 16 consumption units
    - Being able to log in as random users, excluding administrators
    - Gaining access to and/or retrieving debug logs of the entire website, server or container
    - Being able to modify or delete unimportant data
    - Gaining access to important data
3. Large bugs, 32 consumption units
    - Obtaining administrator rights to a virtual machine, Linux-container or main website: thor.edu
    - Being able to modify and/or delete important data
    - Being able to run self-chosen program code inside a virtual machine (RCE)
4. Insane bugs, 256 consumption units
    - Full acquisition of the systems or obtaining root access on the hypervisor. In case of user mode hacks, half of the reward will be awarded.

        Possible ways:

        i. Breaking out of a container or virtual machine
        ii. Obtaining CoCo SSH private keys
        iii. Black magic, please explain

The rewards as described above are a guideline. The definitive reward will be decided upon after settlement of the hack, taking into account the maximum legally allowed reward Thor can give to a single person.