Decubate

Responsible Disclosure Policy

Version	1.0	–	5	May	2025

VERSION MANAGEMENT

Version	Approved by	On	Comments
V 1.0	Board of directors	13 May 2025	First version

1 Introduction

1.1 Purpose

As Decubate B.V. (**Decubate**) is a crypto-asset service provider (**CASP**) within the meaning of Article 3(1)(15) of the Markets in Crypto-Assets Regulation (**MiCA**), it recognises the importance of maintaining robust operational resilience and transparency in the event of system vulnerabilities or security incidents.

This Responsible Disclosure Policy has been established in accordance with Article 10(2)(e) of the Regulatory Technical Standards (**RTS**) on the authorisation of CASPs under MiCAR, and outlines how Decubate engages with external stakeholders who wish to report security vulnerabilities in a responsible and constructive manner.

1.2 Responsibility

The CTO is responsible for the secure implementation of this Responsible Disclosure Policy. The Compliance Officer monitors adherence to this policy and assesses the need to notify regulators or impacted users. The CRO is consulted in case of escalation or material risk to client assets or company operations.

1.3 Questions, breaches or inaccuracies

Questions, concerns, or reports related to this policy or its implementation may be directed to support@decubate.com, or submitted via the “Responsible Disclosure” page on our website (https://www.decubate.com/responsible-disclosure), where users are guided to a secure reporting channel

2 The policy

2.1 General Principles

Decubate is committed to maintaining the security, integrity, and reliability of the systems it operates as a crypto-asset service provider. In this context, the ability to receive, assess, and act on responsible disclosures from external stakeholders is considered an important part of our operational and governance framework.

This policy is based on the principle that responsible disclosure — whereby security researchers,

users, or peers report vulnerabilities in a confidential and ethical manner — contributes meaningfully to the protection of our systems and clients. Decubate acknowledges that such disclosures may originate from individuals or organisations outside the company and therefore must be handled in a manner that is clear, respectful, and legally secure for all parties involved.

This policy provides the framework through which such disclosures are received and processed. It defines our obligations to acknowledge, assess, and act upon reported vulnerabilities in a timely and responsible manner, while also ensuring that privacy, confidentiality, and regulatory obligations are upheld at all times. It aims to create a safe and transparent channel through which the community can contribute to strengthening the resilience of Decubate's operations.

2.2 Scope of Responsible Disclosure

The responsible disclosure procedure outlined in this policy applies to all digital assets, services, and technical infrastructure managed by Decubate in connection with its MiCAR-regulated activities. This includes, but is not limited to, any vulnerabilities discovered in our public website, backend infrastructure, APIs, smart contract integrations, custody services, token management platforms, or interfaces used by projects and investors for onboarding or lifecycle management.

Furthermore, any findings related to the processing of user data, compliance with ICT security requirements under DORA, or the confidentiality, integrity, and availability of our systems fall within the scope of this policy. Vulnerabilities may be reported by clients, developers, ethical hackers, independent researchers, or members of the public who encounter unusual or unintended behaviour in our systems.

This policy does not replace or override any legal obligations Decubate has under MiCAR, DORA, GDPR, or the Wwft, but complements those obligations by facilitating external stakeholder involvement in risk detection and mitigation.

2.3 Reporting Procedure

Individuals or entities wishing to report a potential vulnerability are invited to do so via the dedicated Responsible Disclosure landing page available on our public website (https://www.decubate.com/responsible-disclosure). This page provides an overview of the policy and offers a secure method for submitting disclosures, currently routed to support@decubate.com. The submission form includes a call to action ("notify us") and is intended to provide a user-friendly entry point for non-technical reporters, while still accommodating more detailed technical

submissions.

In order to support effective investigation and remediation, we kindly request that the report include a clear description of the issue, the location or system affected, and any steps taken to identify or reproduce the vulnerability. If relevant, the reporter is encouraged to include screenshots, logs, or code snippets that support their findings. Reporters may also include their contact details, though anonymous submissions are accepted if sufficiently substantiated.

The information received through this channel will be treated with care and discretion, and all personal data will be processed in accordance with Decubate's data protection obligations under GDPR.

2.4 Acknowledgement, Assessment and Investigation

Upon receipt of a valid report, Decubate will issue an acknowledgment of the disclosure within five business days, confirming that the message has been received and is being reviewed. An internal triage process will then be initiated by the infrastructure and compliance teams, with escalation to the CTO and, where appropriate, the CRO.

Each disclosure will be assessed on its individual merits, with attention to the severity of the vulnerability, the likelihood of exploitation, and the potential impact on client funds, operational continuity, or regulatory compliance. This may involve internal testing, log analysis, or coordinated simulation in a controlled environment.

If the reported issue is confirmed, a remediation plan will be developed and executed in line with Decubate's incident response protocols. The reporter will be kept informed throughout the process to the extent possible, without disclosing confidential or internal security information.

2.5 External Communication and Disclosure

Once a reported vulnerability has been validated and appropriately mitigated, Decubate may communicate the outcome of the report to affected stakeholders or, where necessary, to the broader public. This decision will be made on a case-by-case basis, taking into account factors such as the nature of the vulnerability, whether clients were materially impacted, and whether public awareness serves a broader protective function.

In the event that the vulnerability has a regulatory reporting threshold — for example, in the case of a material ICT-related incident under DORA, or a personal data breach under GDPR — the appropriate supervisory authorities (e.g. the AFM or the Dutch Data Protection Authority) will be notified in accordance with statutory timelines and protocols.

Decubate also reserves the right to publish general, anonymised summaries of resolved disclosures in the interest of transparency and community engagement, always ensuring that no sensitive data or private communications are disclosed.

3 Exclusions

While Decubate welcomes and encourages the responsible disclosure of vulnerabilities in its systems, it is important to clearly outline the boundaries of this policy. Certain actions or reports fall outside the scope of responsible disclosure and are therefore not covered by the protections or commitments described in this policy.

This policy is not intended to provide a safe harbour for activities that could cause harm to Decubate, its users, or its infrastructure. Accordingly, the following categories are explicitly excluded:

3.1 Social Engineering and Deception-Based Techniques

Any form of social engineering, including phishing attacks, manipulation of employees, impersonation attempts, or unauthorised access through deception, falls outside the remit of ethical reporting. These activities pose direct risk to personnel and are not necessary to identify system-level vulnerabilities.

3.2 Physical Security Testing

Physical security testing is not permitted under this policy. Attempts to access Decubate's offices, hardware, or equipment through physical means — whether directly or via vendors — are not covered and may be considered trespassing or unlawful intrusion.

3.3 Denial-of-Service or Performance Disruption

Any form of Denial-of-Service (DoS) attack or stress testing, including automated scanning tools that degrade system performance, are not considered responsible behaviour under this policy. Reporters must avoid conducting tests that could affect service availability or disrupt client experience in any way.

3.4 Incomplete or Non-Actionable Reports

Submissions that merely identify outdated software versions without a concrete vulnerability, or reports based on generic best practice deviations without a direct security impact, may be reviewed but will not automatically trigger investigation unless a material risk is evident.

3.5 Illegal Access, Data Theft, or Breach of Law

Any activity that involves a breach of law, data theft, or the unauthorised use of private information — regardless of the intention — will not be protected under this policy. Decubate reserves the right to take legal or technical action in response to malicious, negligent, or harmful conduct.

3.6 Good Faith Requirement and Clarifications

Reporters are advised to conduct their activities in good faith and with minimal disruption, and to submit findings as soon as they are reasonably confirmed. Any uncertainty about whether an action falls within scope should be clarified in advance by contacting Decubate's designated support channels.

4. Evaluation

This Responsible Disclosure Policy is evaluated on a yearly basis by the CTO and CRO and reviewed by the board of directors as part of Decubate's broader risk and compliance framework. Updates will be published on the Decubate website with clear version tracking.

***