INIGO

FINANCIAL INSTITUTIONS

Digital Asset Crime

Please provide the most recent copies of the following documents with this proposal form:

- Insured's audited annual report & accounts and any additional applicable filed financials
- Organisational structure chart
- Any supplementary information which is material to the response of the questions

FINANCIAL INSTITUTIONS

Digital Asset Crime

INIGO

INSURED INFORMATION

1. Name of the Insured:

2. Name of the Parent Company (if applicable):

3. Principal address:

4. Website address:

5. Date of establishment: / /

6. Please state the total number of full-time employees and offices in each location:

	Employees	Offices	Revenues
UK			
Europe			
US			
Canada			
South America			
Africa			
Asia			
Oceania			
Middle East			
Eastern European			
Caribbean			
Total			

FINANCIAL INSTITUTIONS

Digital Asset Crime

INIGO

ACTIVITIES

7. Please describe the activities, products and/or services of your business or businesses:

8. If providing exchange services, please provide detail of daily average volume of transactions:

9. Please state the total assets from the Insured's recent annual audited financial statement:

10. Do you use any sub-contractors? **Yes** **No**
If **'YES'**, please provide details of these and controls and vetting procedures:

11. Can you provide the % split between retail and institutional customers:

	% Split
Retail	
Institutional	

12. Do you provide any custodial services? Yes No

13. Do you hold any proprietary investment in digital assets (e.g. Bitcoin)? How much in USD?

Digital Asset Crime

RISK MANAGEMENT

14. Regarding internal audit:

a. Do you have an internal audit department? **Yes** ☐ **No** ☐

If **'NO'**, please provide details of other functions that would provide this service:

b. Is there an agreed internal audit plan? **Yes** ☐ **No** ☐

c. Have all recommendations arising from the internal audit been implemented? **Yes** ☐ **No** ☐

15. Regarding external audit:

a. Please state the name of the external audit company used:

b. Have all recommendations made by the external audit company been implemented? **Yes** ☐ **No** ☐

16. Please state the Insured's primary regulator:

a. When was the Insured's most recent regulatory review?

b. Have all recommendations arising from the most recent regulatory review been implemented? **Yes** ☐ **No** ☐

17. Do you have compliance procedures to ensure all staff comply with the regulatory rules, principles, codes and guidelines? **Yes** ☐ **No** ☐

18. Do you have a business continuity plan that is regularly reviewed, updated and tested? **Yes** ☐ **No** ☐

If **'NO'** to any of the questions from 14.b to 18, please explain:

DIGITAL ASSETS EXPOSURE

19. Please provide Total Assets under Custody in USD:

20. Total AUM split by digital asset:

21. Do you provide any privacy coins/shielded transactions? **Yes** ☐ **No** ☐

Digital Assets Exposure *continues on the next page*

DIGITAL ASSETS EXPOSURE (CONTINUED)

If **'YES'**, to question 21, please explain:

22. What is the maximum potential amount that could be online or perceived to be in 'hot' storage/online at any one time?

23. Is your organisation required to conduct activities in relation to key/seed generation? Yes ☐ No ☐

24. Can you confirm that you only allow transactions from whitelisted addresses?

25. Please could you confirm whether you hold private keys? **Yes** ☐ **No** ☐

If **'NO'**, please answer questions a. to c:

a. Please advise which digital asset custodian/exchanges are utilised by the applicant:

b. If you utilise a third party for the storage of private keys, please advise the level of liability accepted by such third parties:

c. Please provide detail around the transaction process between the applicant and the above referenced third parties, including details around biometric authentication, video approval, multi-factor authentication etc.

26. Do you conduct activities in relation to wallet/key usage? **Yes** ☐ **No** ☐

a. Please outline your approach to crypto asset key storage:

b. Do you employ MPC technology in the storage of private keys? **Yes** ☐ **No** ☐

c. Please provide details of how you backup private keys and do you check to ensure these processes work accordingly?

d. Please outline your keyholder grant/revoke/retire policies and procedures:

e. Are customer assets held in segregated wallets? **Yes** ☐ **No** ☐

f. Do you keep proprietary funds separate from client funds? **Yes** ☐ **No** ☐

Digital Assets Exposure *continues on the next page*

Digital Asset Crime

DIGITAL ASSETS EXPOSURE (CONTINUED)

27. Do you use on chain screening services to monitor transactions? **Yes** ☐ **No** ☐

If **'NO'**, please provide details:

28. How are transactions initiated, validated and executed?

29. What approval processes are in place for transactions?

30. What approval processes are in place for high-value transactions?

31. Are there additional verification steps for transactions that exceed certain thresholds?

32. What are these thresholds?

INTERNAL CONTROLS – CUSTOMERS

33. Do you have procedures to verify the identity and authenticity of new customers before entering into transactions with them? **Yes** ☐ **No** ☐

If **'YES'**, please provide detail:

34. Do you investigate new customers through a credit reporting agency? **Yes** ☐ **No** ☐

35. If providing exchanging services to retail customers, how do you ensure they are sophisticated enough to trade these assets?

Internal Controls - Customers continues on the next page

Digital Asset Crime

INIGO

INTERNAL CONTROLS – CUSTOMERS (CONTINUED)

36. Do you control access to customer information in your computer systems? **Yes** **No**

If **'YES'**, please indicate whether you:

a. Implement access controls and firewalls in your database of customer information. **Yes** **No**

b. Restrict access permissions only to particular employees. **Yes** **No**

c. Require the customer to authenticate his or her identity using passwords, personal identification numbers, shared secrets, tokens or biometrics before the customer may access his or her data. **Yes** **No**

37. Do you control the dissemination of customer information? **Yes** **No**

If **'YES'**, please indicate whether you:

a. Have a company policy prohibiting the dissemination of any personally identifiable information pertaining to the customer. **Yes** **No**

b. Provide customer information only to a designated representative of the customer. **Yes** **No**

c. Require the customer requesting customer data to authenticate his or her identity using passwords, personal identification numbers, shared secrets, tokens or biometrics. **Yes** **No**

INTERNAL CONTROLS – VENDORS

38. Do you outsource the processing of any payments of client money to a third party? **Yes** **No**

39. Do you have due diligence procedures in place to select and onboard new Vendors? **Yes** **No**

40. Where you outsource any other part of your network, computer system or information security, do you require such vendor to demonstrate the adequacy of their own systems on an annual basis? **Yes** **No**

41. Do you have procedures to verify the identity, authenticity and credit strength of new vendors before entering into transactions with them? **Yes** **No**

42. Do you require vendors to maintain a crime insurance and cyber liability insurance? **Yes** **No**

SOCIAL ENGINEERING

43. Please complete the following table in regard to Fund transfers:

Average daily number of transfers	
Average value of transfers	
Largest single amount that can be transferred	
Largest single amount that can be transferred without dual authorisation	

44. What is average wallet size?

Social Engineering *continues on the next page*

Digital Asset Crime

SOCIAL ENGINEERING (CONTINUED)

45. What is the largest wallet size?

46. Do all employees receive regular training on social engineering and phishing scams, including developments in AI related fraud (e.g. 'deep faking' related scams)? **Yes** **No**

47. Do you accept funds transfer instructions from customers, vendors or suppliers over the telephone, fax, email or some other electronic communications method? **Yes** **No**

If **'YES'**, please describe your procedures to authenticate the instructions:

48. Is there a social engineering fraud risk management strategy in place? **Yes** **No**

49. Do you require review of any changes to customer, vendor or supplier bank account information (account numbers, routing numbers, bank name and address) by a supervisor and via an independent callback verification procedure before the change is made in your records? **Yes** **No**

50. Do wire transfers to an overseas account require review and approval by a supervisor? **Yes** **No**

51. Is the authority to execute wire transfers limited to specified employees? **Yes** **No**

52. Are unusual, large or one-off payment instructions followed up by an independent call-back at a pre-designated telephone number to confirm payment instructions and confirm authenticity? **Yes** **No**

If **'NO'**, to questions 46 to 52, please explain:

IT CONTROLS

53. Please detail certificates obtained to date (i.e. ISO27001, SOC2):

***IT Controls** continues on the next page*

Digital Asset Crime

INIGO

IT CONTROLS (CONTINUED)

54. Is there an IT security plan in place that is regularly reviewed, updated and tested? **Yes** **No**

55. Is annual training conducted for every employee for IT security issues and procedures? **Yes** **No**

56. Are electronic passwords used to control varying levels of security access to computer systems? **Yes** **No**

57. Are periodic password changes enforced? **Yes** **No**

58. Does all remote access to the company's network and corporate e-mail require multifactor authentication (MFA)? **Yes** **No**

59. Are user accounts and system access automatically withdrawn upon termination of employment? **Yes** **No**

60. Are all computer software changes independently approved before being implemented? **Yes** **No**

61. Is all valuable/sensitive data backed up on a daily basis, encrypted and stored off site? **Yes** **No**

62. Do you have anti-virus software on all your computer devices, servers and networks and ensure that these are updated to the software providers recommended level? **Yes** **No**

63. Are computer programs/software monitored for unauthorized access? **Yes** **No**

64. Is there an incident response plan for network intrusions, data breaches and virus incidents that is regularly reviewed, updated and tested? **Yes** **No**

65. Is a software update process currently enforced, including installation of software patches? **Yes** **No**
If **'YES'**, are critical patches installed within 30 days of release? **Yes** **No**

66. Do you have a bring your own device policy? **Yes** **No**
If **'YES'**, please provide details:

67. Do you have firewalls and intrusion monitoring detection systems in place to prevent and monitor unauthorised access? **Yes** **No**

68. Do you ensure all remote access to IT systems is secure? **Yes** **No**

If **'NO'**, to questions 54 to 68, please explain:

Digital Asset Crime

INIGO

PHYSICAL SECURITY

69. Please state the average amount of digital assets held in cold storage:

70. Do you use a 3rd party vault provider? **Yes** **No**

71. Does the 3rd party provider accept liability in the event of a theft? **Yes** **No**

If **'YES'**, please provide details:

72. Please confirm there is continuous CCTV surveillance in operation throughout all premises? **Yes** **No**

a. Is there controlled security access to all business premises? **Yes** **No**

b. Are all premises fitted with alarm systems which are connected to the Police and tested by a certified third party? **Yes** **No**

If **'NO'**, please explain:

LOSS INFORMATION

73. Please read the following statements and confirm as indicated below:

a. Please give brief details of any loss sustained by the Insured (whether insured or uninsured) during the past 5 years as follows, continue on a separate sheet if necessary:

Nature of Loss	Date of Discovery	Location	Total Loss Amount

Loss Information *continues on the next page*

Digital Asset Crime

LOSS INFORMATION (CONTINUED)

b. The Insured, after enquiry, is not aware of any act, error, omission, event, circumstance or incident which may give rise to a loss under this proposed insurance? **Yes** **No**

74. In the event that a loss has been discovered, has the Insured taken remedial action to prevent or avoid recurrence? **Yes** **No**

If **'YES'**, please provide details:

IMPORTANT NOTICE

Before commencement of any insurance policy, the Insured is required to make a fair presentation of the risk. The Insured must disclose all material circumstances which the Insured knows or ought to know or, failing that, has given us, Inigo the Insurer, sufficient information to put a prudent insurer on notice that it needs to make further enquiries for the purpose of revealing those material circumstances.

A material circumstance is one which would influence a prudent insurer's judgement of the risk. If the Insured has any questions regarding the duty to make a fair presentation of the risk, then please contact your broker for further information.

Declaration

It is declared that the Insured has made a fair presentation of the risk. This declaration is signed by the director or officer who is responsible for arranging insurance on behalf of the Insured.

Signature: **Position:** **Date:** / /

This proposal form should be signed no earlier than 30 days prior to inception of the policy.

DATA PROTECTION NOTICE

Inigo collects and uses information, including any relevant personal data, provided by the Insured in order to consider providing an insurance quote for the Insured and any other entities or individuals intended to benefit from the proposed insurance.

If Inigo needs to process or obtain any special category data not provided by the Insured within this proposal form, then Inigo will seek consent from the Insured before doing so. If the Insured is providing any personal information on behalf of an individual, then the Insured must inform that individual of this notice. Inigo may share the information collected with a number of third parties including but not limited to agents, brokers, reinsurers, regulators and law enforcement agencies. Inigo will only disclose any personal information to the extent required or permitted by law.

If the Insured or any individual wishes to contact Inigo regarding their data and rights, then please contact Inigo's Data Protection Officer at dpo@inigoinsurance.com

Full details of Inigo's privacy policy can also be found here: **inigoinsurance.com/privacy-policy**