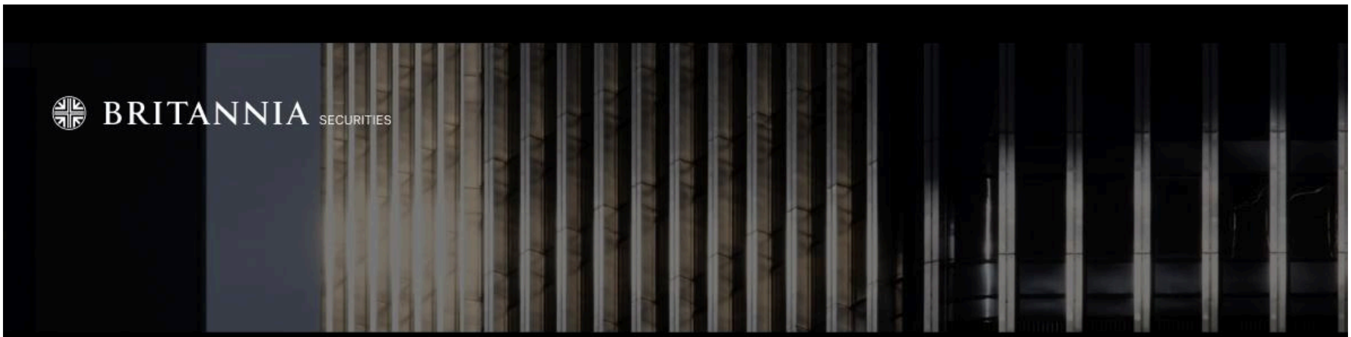
BRITANNIA SECURITIES



BRITANNIA NETWORK

Support Documentation
Client User Guide

powered by **io.**finnet

Britannia - strictly confidential

Latest update: February 4th 2025

1. Introduction to io.network

io.network enables 24/7/365 multi-currency fiat settlements for clients of the network in a safe, secure & compliant environment by leveraging our permissioned blockchain with self-custody technology via our io.vault solution.

1.1. Technology Background

io.network leverages our exclusive and innovative technology:

- **io.vault:** a cryptographically enforced signing and self-custody technology solution that offers the network users the highest level of security and scalability for digital asset transactions.

1.2 Concepts

Concept	Breakdown
io.network	A private and permissioned distributed ledger based network, can be referred as ION
Principal Member or PM	An io.network principal member is a network node operator and is capable of issuing and administering its own assets in a private sub-network for its own underlying clients on io.network
Underlying client	An io.network underlying client is a principal members direct client that wishes to transact within the PM's sub-network
Minting Tokens	The action of depositing / creating tokens within the network for an aligned underlying client
Burning Tokens	The action of withdrawing / removing tokens within the network for a specific underlying client
Enable Address	In order for any io.network address to interact with a PM administered assets it must be enable by the PM to their allowlist smart contract which governs access for network users to their administered assets
Vault	A digital wallet for any Network assets, secured and managed through secret shares
Signing Threshold	The number of secret shares required to enable the approval and signature of any request for a particular vault

Secret Share(s)	Sensitive cryptographic data that provides a user's device with an allocated level of signing power that is required when signing a digital asset transaction.
Signing Power	The number of secret shares a user controls on their linked device, as part of that particular vault signing party.
Signing Party	The collection of signers and their linked devices that contain the totality secret shares within a particular vault.
Reshare Request	Users may submit a request to amend the threshold and signing party or create a new Vault. This request must be approved, by reaching the existing vault threshold and "signed" by the resulting signing party. This is known as a reshare request.
Vault Card	A Vault Card displays the name of the Vault, assets held within the vault, Vault Threshold
Asset Card	An Asset Card displays asset quantity and equivalent US$ value and wallet address of a particular digital asset within a given Vault.
Deposit Address	A Deposit Address is the specific public address for the digital asset on the relevant blockchain/network that is cryptographically controlled by the underlying secret shares of the given vault.
Transfer Request	A Transfer Request may be submitted via the dashboard by any user within an organization and is transmitted to the devices of a Vault's signing party. The request includes the network, asset, destination address, and the quantity of asset to be sent. The request must be approved and signed by members of the Signing Party for the given Vault that have sufficient combined Signing Power to meet or exceed the Vault Threshold
PM's dedicated network account	A dedicated network account for the principal member is used for two processes; 1. Where their underlying clients will deposit funds into when they want to deposit into the network 2. Is the location where the PM will transfer fund back to the underlying client when withdrawing from the network
io.vault Dashboard	Naming convention for the dashboard accessible by Network users
Network Support Service	Naming convention for the io.network support service

1.3 Dashboard Status

Received	The transaction has been received by a vault
Pending	The transaction request is pending approval and signature
Expired	The transaction request has expired
Rejected	The transaction was rejected by enough of the vault signing party to make it impossible to reach to vault approval threshold
Signing	The transaction request has met the threshold for approval and is pending completion of the signature process
Failed	The transaction was either determined to be invalid by the blockchain node/network, or the signature process failed during signing
Contract Reverted	The associated smart contract interaction on the network has failed, this can occur for various reasons such as incorrect permissions or attempting to send an invalid quantity of tokens
Submitted	The transaction has been signed and broadcast successfully to the relevant network. Broadcast transactions may remain unconfirmed on the blockchain for some time and may still result in an incomplete transaction in certain circumstances, notably a failed smart contract interaction.
Successful	A request has been approved, signed, submitted and successfully mined on the network.

2. Getting Started with io.network

In this section of the user guide, we will walk you through all aspects of getting started with the io.network and io.vault product. As an underlying client there are five key activities to take consideration against;

1. io.network User components
2. Accessing the User dashboard
3. Registering a mobile device
4. Downloading the disaster recovery backup file
5. Recommended Steps Before Using the Network

2.1 io.network User components

1. **The io.network User dashboard:**

This is your central HUB to process all key activity within the network. This dashboard can be used to view and manage an organisation's vault/s and transactional activity, add or remove users, add your vault details to the public network, add an API key and gain any support that is required. You will also use this dashboard to process deposits and withdrawals transactions.

2. **The io.vault mobile application:**

The mobile application is used by each member of a vault signing party to review transactions or re-share requests, approve or reject them, and participate in the signing process.

Currently supported on the following devices and operating systems:

- **Apple iPhone** 12 or later with iOS 17 or newer (The use of FaceID is *required* to provide the best level of security at the device level, in addition to keeping your device updated with the most recent iOS release)
- **Android** version 12 or later is required. (To ensure optimal device-level security, enable secure biometric recognition and keep your device updated with the latest OS version).

Please note: To utilize the mobile App, you must first enable "iCloud Drive" or Google Drive on your phone.

For **iPhone** follow these steps:

1. Open “Settings”
2. Tap on “your name” at the top
3. Select “iCloud”
4. Under **Apps Using iCloud**, tap on “iCloud Drive”
5. Toggle the switch to “enable” it

For **Samsung** follow these steps:

- Enable Syncing with Google Drive:
    1. Open the Settings app on your Samsung device
    2. Scroll down and tap Accounts and Backup or just Accounts (depending on your model)
    3. Tap on your Google account from the list
    4. Ensure that the toggle for Drive or Google Drive Sync is turned on

- Enable Backup to Google Drive:
    1. Go to Settings > Accounts and Backup > Backup and Restore.
    2. Under the Google Account section, tap Back up data.
    3. Ensure that Back up to Google Drive is toggled on.
    4. Tap Back Up Now if you want to initiate a manual backup.

For any **Android Device** (Other Than Samsung) : Since Android devices may have slightly different menus and layouts depending on the manufacturer and model, follow these general tips to locate and enable Google Drive:

Step 1: Consult Your Device's Manual or Support Page

If you're unsure where to find Google Drive settings on your device:

1. Check your device manual for guidance on syncing or cloud storage settings.
2. Search online using the phrase:
   "How to enable Google Drive on [Device Name/Brand]*"

*Replace [Device Name/Brand] with the specific make and model of your device (e.g., Samsung Galaxy S23, OnePlus 10).

Step 2: Use the Settings Search Bar

1. Open your device's Settings.
2. Tap the Search Bar (usually at the top of the screen).
3. Type keywords like:
   - "Drive" to locate Google Drive sync settings.
   - "Backup" to find options for enabling backups to Google Drive.
4. Select the relevant result and follow the on-screen instructions to enable or configure Google Drive.

2.2 Accessing the User Dashboard

As an underlying Client, you will have access to the io.network user dashboard;

- The dashboard can be accessed by visiting app.iofinnet.com

Credentials - Initial login credentials will be provided by the io.finnet Customer Office team directly to your account admin user. Once the Admin user receives his login details, he will be required to reset his password upon logging in for the first time.

Please note *- You have **7 days** to access your dashboard. After this period, access will be revoked, and you will need to contact support to request new login details*

After this additional users can be added by your Administrator(s). Invitations will be sent through the portal, and new users will receive an email prompting them to create a password during their first login.

Please Note - The account admin's details are collected during your on-boarding with io.finnet.

Please note - To access the io.finnet dashboard seamlessly, we recommend using the latest versions of the following web browsers: Google Chrome, Safari, Microsoft Edge, or Firefox.

Please note - To further secure your registered device, enable two-factor authentication (2FA)

To enable two-factor authentication, follow these steps:

Process Ref.	**Process Step**
1	Go to the "Profile" section by clicking on the dropdown menu next to your avatar at the top right corner of the web dashboard
2	Scan the provided QR code or manually paste the code into an authenticator app
3	Input the resulting one-time code generated by the authenticator app into the designated section
4	Click the "Enable" button to confirm and activate two-factor authentication for your account

1. Dashboard Overview

The dashboard is designed with a user-friendly interface that includes the following key components:

Left-hand Menu:

Vaults	● Create a Vault ● Vault Settings: ❖ Manage Assets ❖ Resharet
Transfer	To create a transfer from one vault to another on the network
Address Book	To allow you to link Network addresses to specific users
Directory	List of all underlying clients authorized to transact on the network
Apps	There can be two views here; 1. if just an io.network client - a. You will see an API app to support connects via API 2. If you are a io.network and io.vault client - a. You will see all public Dapp's available to you
Teams	Allows you to see; 1. My Team - Ability to review individuals, add or remove users from the network 2. Invites - Shows current individuals who have been invited to use the network, you can revoke or resend the invite here
Settings	View of four key topic; ● Governance - User permissions via collective approvals ● API Keys - An API key enables programmatic access to the io.finnet platform

	● Security - Export User and API authentication events for security analysis and monitoring. ● Billing - Sign up to our io.vault product, given access to public chains.

Bottom-Left Corner:

Help Option	To gain support from io. against the io.vault product ● Ask Chatbot ● Raise a Ticket ● API Reference ● Support Portal ***Please Note*** *- Only available if you are a client of the io.vault product as well as io.network.*

Top-Right Corner:

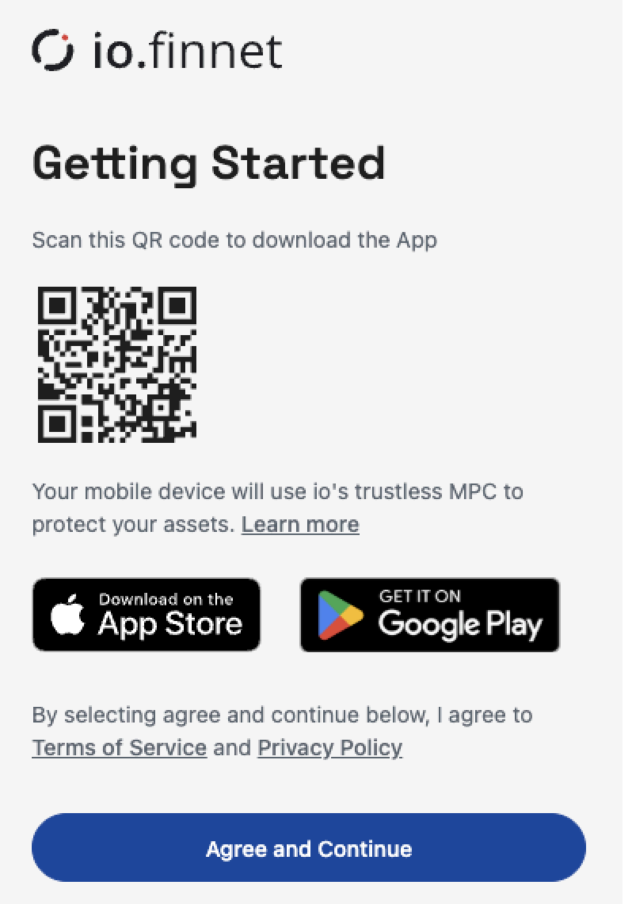
Avatar Dropdown Menu	To create a transfer from one vault to another on the network ● Profile ● Support - Links you to our support section ○ ***Please Note*** *- Only available if you are a client of the io.vault product as well* ● Sign out

2.3 Registering a mobile device

The Mobile Application: The io.finnet mobile app can be accessed by scanning the QR code displayed on the web-dashboard's “Getting Started” screen. A mobile device is required and used by each member of a Vault signing party to review user management, transfer, or resharing requests, approve or reject them, and take part in the signing process.

Please Note - The app is also available for download directly from the Apple App Store or Google Play.

Additionally - you'll need to agree to the Terms and Conditions and the Privacy Policy during this process.



io.finnet

Getting Started

Scan this QR code to download the App

Your mobile device will use io's trustless MPC to protect your assets. Learn more

By selecting agree and continue below, I agree to Terms of Service and Privacy Policy

All users who will approve any requests need to complete the following steps with their mobile device:

Process Ref.	Process Step
1	You have two options to register a signing device: 1. Use the QR code provided on the web dashboard login page. 2. Download the app from Apple App Store or Google Play
2	Open the app and click sign in
3	Login using the same credentials you login with on the web dashboard
4	After logging in, you will be prompted to register the device as a signer. ● The app will automatically assign a name to the signer, which can be easily changed later. When registering, you can choose between two security options: ● **Passphrase (Recommended)** – Provides stronger security and better protection for your account. ● **PIN code** – A simpler option but less secure than a passphrase.

	Additionally, you can configure authentication preferences, enable biometric authentication for faster access,
5	Once the signer secret phrase has been confirmed, your signer registration is complete and it is ready to be added as a signing party on a vault.
6	You can set up Disaster Recovery in the following situations: ● **When joining a vault** – Whether you are being added to a new or existing vault, you will be prompted to set up Disaster Recovery. However, you can choose to skip this step at this stage. ● **After receiving funds in a vault** – If one of your vaults receives funds and you have not yet set up Disaster Recovery, the App will prompt you to do so the next time you open it. Disaster Recovery involves securely saving a signer-specific 24-word secret phrase, which is randomly generated by the App. This step is essential for enabling signer recovery in case of an emergency. For more details, refer to the Disaster Recovery under section **2.5** .
Important Notes	Save your secret phrase or PIN code in a safe and secure location as it will be required should you need to complete signer recovery
	To ensure the integrity and security of your data, it is essential to re-download your encrypted device backup each time a new vault is created or whenever a vault reshare is completed. Please note that for the time being, and until further notice, these backups should not be saved to iCloud/Google Drive in order to ensure additional redundancy to the native functionality of the mobile application. Instead, choose an alternative storage drive for downloading these files.
Please Note - You can view all of the registered signers for your account by logging into the web dashboard, clicking on the "account" section on the left-hand side, and reviewing the list of registered signers and the vaults in which they are a member of the signing party.	

2.4 Downloading the disaster recovery backup file

If you require to further back up your disaster recovery file, the following steps need to be completed:

Process Ref.	Process Step
1	Open the mobile app and log in
2	Once logged in, click on the settings button at the top right-hand corner of the app

3	Select “Download encrypted backup file” and then “Continue”
4	Specify the file name, select the destination you would like to save the file and then select “Save”
5	Verify that file was successfully saved to the selected location (preferably on the cloud)
Please Note - To ensure all shares can be recovered from a device, the backup file must be re-downloaded each time the device participates in a request. Users will be prompted to download the backup file whenever this occurs	
Please Note - For reliable disaster recovery, always back up your files to the cloud instead of storing them directly on the device. This way, if the handset is lost, you can easily access and recover your backup without needing the physical phone	

2.5 Recommended Steps Before Using the Network

2.5.a. Create your Vault

Before you start using your network, we strongly recommend creating your vault. Please choose a unique name for your vault.

For instructions on creating this vault, please refer to the "Create a new Vault" section **6.1**

2.5.b. Share Your Vault Address

To transact on the network, the Principal Member must first authorize your vault address within the network. Please share your vault address with the principal member by completing the transaction profile questionnaire. This will be shared with you during the onboarding process.

2.5.c. Visibility on the Network

The Principal Member allows you to set your preferred visibility on the network. Choose an option below and share it with the Principal Member within the transaction profile questionnaire. Below are your options;

- **Visibility 0 - Public**: Your address is fully visible to everyone on the network, appearing in general searches and listings

- **Visibility 1 - Known Only**: Your address is partially visible; their profile appears only if the full **io.network address** is already known by the searcher

- **Visibility 2 - Hidden**: The address is completely hidden and does not appear in any search or directory listings, even if the address is known.

3. Team Management

Effective team management is crucial for maintaining a secure and organized working environment. This section provides step-by-step instructions for adding, removing, and editing users in two different workflows, depending on the level of security and oversight needed.

1. **Option 1: Direct Admin Control**
   In this default mode, administrators have full authority to directly manage users. This option is ideal for scenarios where fast and straightforward user management is necessary, without the need for additional approval.

2. **Option 2: Governance Vault via MPC-TSS Technology**
   For enhanced security, this option introduces a multi-party approval process. Here, any user management action (such as adding and removing a user) must be validated and approved by multiple designated validators. This process ensures that sensitive changes are reviewed and agreed upon by trusted team members before being enacted.

Before using the multi-party validation option, a governance vault must be created to define who will serve as validators and how many approvals are required. This guide covers both user management workflows, along with detailed instructions on setting up governance for the MPC-TSS process.

3.1 User Roles and Permissions

Admin: The Admin role is the most powerful role within the system. Admins have the authority to add, edit, or deactivate other users.

User: Regular users have limited access/permissions compared to Admins and Validators. They typically do not have the authority to manage other users or perform any administrative actions.

3.2 Governance Setup for MPC-TSS Validation

This section explains how to set up the governance structure for the MPC-TSS validation process.

Governance Vault Capabilities - more options will be available in future releases

- Invite / Deactivate users and admins
- Adding or Removing admins to the Governance Vault

Please note: Once this feature is enabled, users will not be able to turn it off. Make sure the selected threshold aligns with your business needs.

3.2.a. To create a new Governance Vault:

Process Ref.	Process Step
1	On the web dashboard, click on "Settings"
2	Underneath the "Settings" tab, click on "Governance Vault"
3	Click the "Set Up Your Governance Vault" button
4	On the "Create Governance Vault" page, specify the vault threshold ● The amount of signing power required to complete a transaction or reshare request. **Please Note** - Threshold can be updated after creation, via a reshare
5	Select the users who will be a member of the Governance Vault signing party, and specify the signing power to be allocated to each user's signing device.. ● Signing power will determine the number of secret shares a user controls with their specified signer. **Please note** - Only Admins can be added as signers in the Governance Vault **Please note** - If you wish to participate in the signing process, ensure that you are added as a signer **Please note** - The user list will only show individuals who have registered a signer; virtual signers will not be included in this list
6	After selecting the signer(s), click on "review" to examine the details of the vault creation and the signing power allocated for the Governance vault
7	Click "Submit for Approval" to send the vault creation request or if you need to amend / update the details, click "edit"
8	Once submitted, you can return to the settings page by clicking on "Back to Settings" or track the progress of the vault creation by clicking on "track progress"
9	Each user specified as a member of the Governance Vault signing party must approve the request on their device and participate in the Governance Vault creation process ● A reshare request must be approved and completed within **10 minutes**, after which the request will expire.
10	After successful completion, the vault will be visible on the dashboard, and users will be able to invite team members under the "My Team" section of the settings page.

Please Note - The name of the vault will always be Governance Vault
Please Note - A request must be approved and completed within the **10 minutes** time-out limit
Please note - All signing parties must be online and logged in with their registered devices at the same time to approve the request, unless background signing is enabled (see section 6.3.b. for details)

3.2.b. Review a Governance Vault:

Process Ref.	Process Step
1	You can review the details of your Governance Vault, including the threshold and signers, by navigating to the 'Settings' page.
2	Then selecting the 'Governance Vault' tab and clicking the settings gear icon in the top left corner.
3	This will take you to the Vault Settings page, where all current configurations can be reviewed

3.2.c. Edit a Governance Vault

Process Ref.	Process Step
1	Navigate to the Vault Settings page as described above
2	Request a reshare to edit the threshold and signers
3	At this stage, you can cancel any changes by clicking the “Cancel Edits” button or proceed with the modifications by clicking the “Request Reshare” button
4	You will follow the same signing process for this action as with any other within the vault product

3.3 Adding, deactivating, or editing team members

3.3.a. Add a team member

Process Ref.	Process Step
1	On the web dashboard, select "Teams" from the menu on the left-hand side
2	Under the "Teams" subtab, click on "My Team" to invite new users. Then, click on "Invite User" located at the top right-hand side
3	You will then be prompted to input the invite's details; - Full Name - Email Address - What role they will have (Admin or User)
4	Click "Invite" to send the invitation
5a	For **option 1** "Direct Admin Control": This process is now complete
5b	For **option 2** "Governance Vault Validation": The request will proceed to validation via MPC-TSS. See section **3.4** for additional steps.
6	At this stage, the invited team mate will receive an email invitation containing their username (which is the same as their email) and a temporary password - The invitation remains valid for **7 days**, during which the user must log in before the invite expires
7	Once the invited user logins using the temporary password within the invite email and inputs a permanent password, they will be automatically added to the Users section in the "My Team" sub-tab
8	If the user fails to login within the 7-day period, you can resend the invitation by navigating to the "Invites" subtab in the "Settings" tab at the top of the screen. From there, select the specific user, and click on "Resend Invitation" located in the top-right corner.
Please Note - You can review the status of pending invites by clicking on the "Invites" subtab at the top of the screen	
Please Note - If you'd like to add multiple users you will need to add them individually	

3.3.b. Edit a team member

Process Ref.	**Process Step**
1	On the web dashboard, select "Teams" from the menu on the left-hand side
2	Click on the specific user from the list of active users

3	Once selected, click “Edit Details” in the right-hand side
4	You will then be prompted to edit the updated user’s details; - Full Name - What role they have (Admin or User)
5	Click “Save” - At this point you have the option to either “Cancel Edit” or “Save” the new details
6a	For **option 1** “Direct Admin Control”: This process is now complete
6b	For **option 2** : “Governance Vault Validation”: This functionality **is currently unavailable** and will be introduced in a future update.
7	Once saved you will receive a notification confirming that the update was successful
Please Note - If you need to make edits for multiple users, you must individually select and update each user's details.	

3.3.c. Deactivate a team member

Process Ref.	Process Step
1	On the web dashboard, select "Teams" from the menu on the left-hand side
2	Select the specific user you wish to deactivate from the list of active users
3	Once selected, click “Deactivate User” in the top right-hand side
4	You will then be prompted to confirm the deactivation. If you wish to proceed click “Deactivate” **Note**: Deactivating this user's access may take a couple of minutes and is permanent. Please ensure you update their signing authority in the relevant vaults beforehand.
5a	For **option 1** : “Direct Admin Control” : This process is now complete
5b	For **option 2** : “Governance Vault Validation”: The request will proceed to validation via MPC-TSS. See section **3.4** for additional steps.
6	Once saved you will receive a notification confirming that the deactivation was successful

Please Note - You can review the list of deactivated users by clicking on the "Deactivated" tab under the "My Team" section
Please Note - If multiple requests are necessary, you will need to add users individually, one by one

3.3.d. Revoke an invite

Process Ref.	Process Step
1	On the web dashboard, select "Teams" from the menu on the left-hand side
2	Navigate to the "Invites" subtab via the top of the screen
3	Select an invitee. Once selected, click "Revoke Invite" in the top right-hand side
4	You will then be prompted to confirm the action. Either confirm or cancel the action
5a	For **option 1**: "Direct Admin Control" : This process is now complete
5b	For **option 2**: "Governance Vault Validation" : This functionality is currently unavailable and will be introduced in a future update.
6	Once saved you will receive a notification informing you that the revoking was successful
Please Note - Revoking an invite is not permanent. You can resend an invite to the same user even after revoking that specific user's invite previously.	

3.4 Governance Vault Validation via MPC-TSS Technology

Process Ref.	Process Step
1	After clicking the appropriate button to add, deactivate a user, the request is forwarded to the registered signers for approval
2	Open the app on your registered signer
3	Select the pending transaction request you want to review
4	Review transaction details
5	Using the sliding bar, slide across the screen to approve the transaction

6	Successfully authenticate via FaceID
Please Note	The vault threshold must be reached by any combination of users with devices that have sufficient signing power to approve the transaction

4. Address Book

The Address Book is a functionality on the Dashboard designed to simplify and secure your transactions. It allows you to link network addresses to specific users, ensuring that you send funds to the correct recipient every time. By saving and managing your contacts' addresses, you can minimize the risk of sending crypto to the wrong party, making your transactions more efficient and secure.

4.1 Add Contact

Process Ref.	Process Step
1	On the web dashboard, click on "Address Book"
2	Underneath the Address Book tab click on "+New Contact"
3	Select either “Individual” or “Corporate” to specify the type of contact you are adding
4	Enter the “First Name” and “Last Name” in the appropriate fields
5	In the “Display Name” field, enter a unique name to easily identify the contact in your Address Book
6	Click “Create Contact” to complete the process, or “Cancel” to discard the contact creation

4.2 Add Address

Process Ref.	Process Step
1	After adding the contact, you will be redirected to the Address Book page, where you can select the contact to link it to their network address(es)
2	Click on the contact to add one or more addresses
3	Select the “Network” by clicking the dropdown menu
4	Enter the network address

	Please note: Ensure you have copied and pasted the correct address
5	Enter an Alias to easily identify and differentiate the network address associated with the contact.
6	Then click "+Add Address" to add a new network address or review the existing one **Please note:** You can link multiple addresses to a single contact. Be sure to assign a unique alias to each address for proper differentiation.
7	Click "Next:Review**"** to review your entries, or "Back" to discard the address creation
8	On the review page, click "Add" to finalize the creation, or "Edit" to make changes if needed. **Please note:** Once the address is linked to the contact, you will not be able to edit the network address or the contact. You can either remove the network address and add a new one, or delete the contact along with all associated addresses and create a new one.
9	After adding the Address(es), you will be redirected to the contact page

4.3 Remove a Network Address

Process Ref.	**Process Step**
1	To remove a network address go to the Address Book page
2	Click on the contact from which you want to remove an address
3	To remove an address, click on the three dots next to the address and click the "Remove Address" button
4	You can "cancel" your action and keep the address, or click "Remove Permanently" to delete the address from your directory

4.4 Remove a Contact

Process Ref.	**Process Step**
1	To remove a contact go to the Address Book page
2	Select the contact you want to remove from your Address Book

3	To remove a contact, click the “Remove” button next to the contact's display name
4	You can “cancel” your action and keep the contact, or click “Remove Permanently” to delete the contact from your directory

5. Directory

The Network Directory acts as a central hub, allowing users to view a comprehensive list of all participants on the network. It functions like a "Yellow Pages" for the Network, providing easy access to user information based on the visibility settings defined during onboarding (See Section **2.6.c.** for reference).

From the Network Directory, users can initiate asset transfers by clicking the arrow icon next to the user’s entry. This action will automatically populate the “Create a Transfer” form with the correct recipient address. However, it is recommended to always verify the information provided by the system for accuracy.

For detailed instructions on creating a transfer, please refer to next section (**section 6.2**).

6. Vault Management and Transactions

In this section of the user guide, we will walk you through all aspects of transactions within the io.network and io.vault product. As a principal member there are seven key activities to take into consideration;

1. Creating a new vault;
2. Approving or rejecting a transaction request
3. Signing a request or a transaction
4. Resharing a vault.
5. Transferring Assets
6. API integration
7. Virtual Signer

6.1 Creating a new vault

To create a new vault:

Process Ref	**Process Step**
1	On the web dashboard, navigate to the "Vaults" section on the left-hand side, then select "+New Vault" located in the top right-hand corner

2	Specify a unique name for the vault and click "Next" **Please Note** - Once created the name cannot be changed
3	Specify the vault threshold ● The amount of signing power required to complete a transaction or reshare request **Please Note** - Threshold *can* be updated after creation, via a reshare
4	Select the users who will be a member of the vault signing party, and specify the signing power to be allocated to each user's signing device.. ● Signing power will determine the number of secret shares a user controls with their specified signer. **Please note** - If you wish to participate in the signing process, ensure that you are added as a signer. **Please note** - The user list will only show individuals who have registered a signer.
5	After selecting the signer(s), click on "review" to examine the details of the vault creation and the signing power allocated for this specific vault
6	Click "Submit for Approval" to send the vault creation request or if you need to amend / update the details, click "edit"
7	Once submitted, you can return to the dashboard by clicking on "dashboard" or track the progress of the vault creation by clicking on "track progress"
8	Each user specified as a member of the vault signing party must approve the request on their device and participate in the vault creation process ● A request must be approved and completed within **10 minutes**, after which the request will expire.
9	After successful completion, the vault will be viewable in the dashboard.
Please Note - You can review the vaults details, including the threshold and signing party, by selecting your desired vault from the dashboard	
Please Note - A request must be approved and completed within the **10 minutes** time-out limit	
Please note - All signing party users required to approve the request must be online and logged in with their registered devices simultaneously to complete the request	

Please note: As outlined in Section **2.6.b.,** you must share your vault address with the PM after it is created.

6.2 Approving / Rejecting a transaction request

Upon submission of a transaction request all members of the vault signing party will receive the request notification on their signing device to review. After reviewing the request details, a user may either decide to approve or reject the transaction.

Please Note - Any user with login credentials in the organisation can create a transaction request for any vault within the organisation, so it is important to review the information carefully each time before approving a request.

To approve a transaction:

Process Ref.	**Process Step**
1	Open the app on your registered signer
2	Select the pending transaction request you want to review
3	Review transaction details
4	Using the sliding bar, slide across the screen to approve the transaction
5	Successfully authenticate via FaceID
Please Note	The vault threshold must be reached by any combination of users with devices that have sufficient signing power to approve the transaction

To reject a transaction:

Process Ref.	**Process Step**
1	Open the app on your registered device
2	Select the pending transaction you want to review
3	Review transaction details
4	Select “reject request”
Please Note	If other members of the signing party are still able to reach the vault threshold, they may still complete the transaction.

6.3 Signing a request or a transaction

When signing any request or transaction, please ensure the following details are taken into consideration:

Please Note
There are two different time limits within the network; - A request (creating a vault or resharing a vault) must be approved and completed within the **10 minutes** expiration limit

- A transaction (sending assets to another client) must be approved and completed within the **24 hour** expiration limit
To complete any request, whether it's for a new vault, the management of users in a vault, a vault reshare, or a transaction, the required vault threshold of approvals must be met. All members who approve the request must be online and logged in with their registered devices simultaneously in order to sign the request (unless a user has enabled Background Signing on their device in which case it simply needs to remain powered on after approving the request).
Important: To streamline this process, we highly recommend using **Background Signing**, described below, for a more efficient signing experience.

6.3.a. Live Signing:

Please Note
If a transaction has reached the required threshold of approvals, the signing process will begin automatically between the signers that approved the request.
During Live Signing, each device must stay online and unlocked for the entire duration of the signing process (generally no longer than 10 seconds). If the device is locked or offline, the process will fail, requiring a new request to be created.

6.3.b. Recommended feature: Background signing

To avoid the limitations of Live Signing, you can enable **Background Signing**, which allows the signing process to continue even if your device is locked or running other applications. This feature ensures a smoother, more convenient signing experience without needing to actively keep your device unlocked or the application in the foreground.

To enable Background Signing users must activate location services:

Process Ref.	Process Step
1	When registering a signing device for the first time, you will be prompted to enable Background Signing (location access) on your device. You can choose to enable it by clicking "Enable" or decline by selecting "Not now" in the top-right corner of your screen.
2	Next, you will be asked to grant location access to "io.finnet." You can choose from the following options: ● Allow Once ● Allow While Using the App

	- Don't Allow **Please note:** If you select "Don't Allow," the Background Signing feature will not be activated. If you still have the background signing turned on within the app settings (top right button), you will receive a notification to either turn this off or allow background signing in your device settings.
3	Once completed, you can verify that the "Background Signing" option is enabled by going to the io.finnet app within your phone settings.
4	After completing these steps, go to your device settings and check the location access for the io.finnet app. Ensure that location access is set to at least "While Using the App" (minimum) or "Always" (recommended) for the best performance. **Please note** - if you choose "ask next time or when I share", you will be prompted next time you load the io.finnet app to choose the location access again.
Please Note:	If you force quit the io.vault app prior or during the signing of a request, the process will be interrupted, causing the transaction to fail. You will need to initiate a new request and approve it again to complete the transaction.

6.4 Resharing a vault

The reshare process enables you to modify specific vault thresholds, signing power allocation, or signing parties. Any modifications to these parameters require meeting the current approval threshold and participation by all signers of the resulting signing party.

A reshare request can be processed by following:

Process Ref.	Process Step
1	On the web dashboard, navigate to the "Vaults" section on the left-hand side, then select the relevant vault you want to edit
2	Click on the "gear icon" within the top-right (next to "new transfer" button)
3	Select "edit Threshold & Signers"
4	The following actions are then possible: ● Editing the vault threshold ● Adding a new user to a signing party ● Removing a user from a signing party ● Changing an existing user's signing power

5	Select "request reshare" in the bottom right ● all signing party members (existing or proposed) will be prompted to approve this reshare via their signing devices
6	Continue through the "Approving / Rejecting a transaction request" process as detailed in point **4.2**
7	Once approved, amendment will be updated within the vault setting
Please Note	Members of the existing signing party must meet the existing vault threshold to approve a reshare request
Please Note	Completing a reshare request requires ***all*** members of the ***resulting*** signing party to approve and participate in the reshare signing process

6.5 Depositing Assets into io.network

6.5.a. Cash Transfer

The network enables seamless 24/7 settlement. Before initiating any transfer on the network, please ensure you have sufficient assets in your vault. To achieve this, the process involves the following steps:

Cash Transfer	● Instructions are required prior to depositing funds with the Network's Principal Member. ● Transfer FIAT currency from your bank account to the Principal Member omnibus account previously provided ● Once received, the Principal Member will convert the FIAT into tokens and credit your vault address **Please Note**: This process may take up to one business day, depending on the timing of your transfer request. Token minting occurs several times throughout the day, so the tokens should typically be credited to your vault on the same day
Availability for Transactions	Once on your Vault, the tokens are then available to transact on the network with other users

6.5.b. Redeem Tokens

When you require to withdraw funds from the io.network, the following steps need to be completed:

Token(s) Transfer	● While withdrawing funds from the network, ensure you have notified the Principal Member of your intention. ● Transfer assets / tokens from your vault account to the Principal Member’s vault account found on the directory section of the dashboard. ● Once received, the Principal Member will convert the tokens into FIAT currency and credit your bank account. **Please Note**: This process may take up to one business day, depending on the timing of your transfer request. Token burning takes place at the 11:30am EST of each business day.

6.6 Transferring Assets

You have three options for initiating a transfer:

- Through the **Transfer page** (Option 1 – the quickest method),
- The **Vault page** (Option 2),
- Or the **Directory page** (Option 3 – a secure option to ensure assets reach the correct beneficiary). A transaction request is created on the dashboard by navigating to :the vault page:

Process Ref.	Process Step
1 a	**Option 1**: - Go to the "Transfer" section located on the left-hand side Select the vault from which you are creating the request Click the “sendnew transfer” button located either in the top right corner or next to your Assets
1b	**Option 2**: - Go to the “Vaults” section located on the left-hand side - Select the Vault from which you are creating the request - Click the “send” button located either in the top right corner or next to your Assets
1c	**Option 3**: **Recommended** - Go to the “Directory” section located on the left-hand side - Select the desired beneficiary from your contacts list

2	On the "Create Transfer"" page, complete the following fields: - Select the Asset using the dropdown menu - **Option 1 :** Enter or copy/paste the destination network address - **Option 2** : type the name of the recipient as displayed in the Directory (for more information, please refer to Section **5**) **Please note**: You can view your balance by clicking on the Asset icon box - Add a transaction memo, if desired (this memo is internal to your organization only)
3	At the bottom, click the "review" button to proceed with transferring the Asset, or "Cancel" to stop the transfer.
4	Now you can review the request, and if you wish to proceed with the transfer, click "Submit Request." At this stage, you can still go back to the previous page to edit or cancel the transfer.
5	Once submitted, you can return to the dashboard by clicking on "dashboard" or track the progress of vault creation by clicking on "track Progress".
6	Each user specified as a member of the vault signing party must approve the request on their device and participate in the signature process. A transfer request must be completed, signed, and approved within 24 hours, or it will expire.

6.7 API integration

The vault API enables programmatic access and usage of the product.

To generate API keys, an admin of your organization must access the "settings" page and select "API keys". After clicking "create new API key", specify a name and any IP addresses to be whitelisted (if desired) and click "create". Upon creation, be sure to copy both the API secret and public key as they will not be available again after initial generation.

To create a new API integration, you will need to follow the API documentation located here. You will find all relevant API development coding required in this location.

6.8 Virtual Signer

The Virtual Signer is a Multi-Party Computation (MPC) application that enables secure server side signing of transactions for your vaults with custom approval & rejection logic.

For more information on pricing and integration, please contact our customer support team via our help centre, accessible here, or through the support tab on the left-hand side of the dashboard.

7. Operational & Technical Support

In this section of the user guide, we will walk you through all aspects of operational and technical support within io.network. As an underlying client there are four key activities to take into consideration;

1. Raising an issue or query to your principal member;
2. Support FAQ's & Training Video Guides;
3. Disaster recovery process;
4. Best practices

7.1 Raising a query or issue to your Principle Member

Before raising a ticket, we strongly encourage you to check each valid section of this user guide and the FAQ's. If neither of these options addresses your question, please do not hesitate to contact the PM support desk by following the below process:

Process Ref.	Process Step
1	When you have an issue or query, please email client_service@britanniasecurities.com to gain support
2	client support will respond to you in the agreed SLA
Please Note	Please ensure you document the details of the issue / query, when in the process it took place, vault and transaction ID's (if applicable) and screenshot if available.

7.2 Support FAQ's

When you require further support against any process or procedure, you can find these in the below sections;

1. For all underlying clients vault FAQ's, this will be shared with you via PDF from your principal member.

7.3. Disaster Recovery Process

There are three possible scenarios involving some level of disaster recovery or business continuity procedures:

- If a user has lost a signing device, but utilizes the iCloud syncing feature and possesses the signer passphrase it is possible to simply restore the signer on a new device by downloading the app, logging in, selecting the "restore signer" option and inputting their signer passphrase to decrypt the data on the new device

- Alternatively, If a users' signing device is lost or misplaced and the user does not know the signer passphrase, so long as there are enough available shares to reach the vault threshold using other devices, then a reshare request can be created to issue new shares to a newly registered signing device

- Finally, If there are not enough shares available or the io.vault service becomes persistently unavailable for any reason, utilizing the offline disaster recovery process will be necessary

7.3.a. Responsibility

Each user is responsible for retaining, for each of their registered signer's: the signer passphrase, as well as downloading and storing an up-to-date encrypted device back-up file after participation in any vault creation or reshare and for the safe-keeping of their 24-word secret phrase in an offline and physically secure location.

7.3.b. Process to recover access

Process Ref.	Process Step
1	Members of the signing party with devices containing enough secret shares to reach the vault threshold must obtain their corresponding up-to-date encrypted back-up files and device specific 24-word secret phrases.
2	The organization should then decrypt and combine these files using the publicly available, open-source tool (published here on github) on a secure offline computer to generate, for the first time, a valid private key for the desired vault.
3	Follow the step by step guide from GitHub and our online guide.

Brief Overview	To use the recovery tool file, you need to launch it via the terminal. Follow the steps below: ● Download the recovery tool for your platform from here. ○ If you are using an Apple Silicon based Mac computer: **recovery-tool-mac** ○ If you are using a Linux based computer: **recovery-tool-linux** ○ If you are using a Windows based computer: **recovery-tool.exe** ○ For other platforms, we recommend building the tool yourself from source, which requires an installation of the latest Go language compiler from https://go.dev. ● Open Terminal or "Command Prompt": Navigate to the folder where your recovery tool file is located. For example, if it's in your Downloads folder: **cd ~/Downloads** ● Optional step: Use the sha256sum command to verify that the hash of the file you downloaded matches the hash shown on our GitHub releases page for the tool. e.g. **sha256sum recovery-tool*** ● Run the Recovery Tool: Run the recovery tool using one of the following commands in the terminal window. Be sure to replace **<Backup Files>** with a space-separated list of your backup file names taken from the io.finnet apps. ○ If you are using an Apple Silicon based Mac computer: **./recovery-tool-mac <Backup Files>** ○ If you are using a Linux based computer: ./recovery-tool-linux <Backup Files> ○ If you are using a Windows based computer: recovery-tool.exe <Backup Files> ○ If you are running from source, use go run ./ <Backup Files> in the git cloned repository directory. For more detailed instructions on using the Terminal, refer to the Apple Terminal Guide or Windows Command Prompt guide. The tool will recover a key that is usable for all existing supported coins in the following wallets: **MetaMask** (for Ethereum and EVM-based coins and tokens), **Electrum** wallet (for Bitcoin), and **TronLink** (for Tron). For detailed information on the process, please visit our online guide.

Please Note	**Troubleshooting Common Issues:** 1. Permission Denied Error**:** If you encounter a "permission denied" message when trying to run the recovery tool: ● Run the following command in the terminal to grant execution permissions: **chmod +x recovery-tool-mac** 2. Security Popup Issue**:** If you see a security popup message preventing you from running the tool: ● Go to your **System's Privacy & Security settings** ● Click on **Allow Anyway** for the recovery tool ● Try running the recovery tool again By following these steps, you should be able to successfully run and interact with the recovery tool file via the terminal
Please Note	This process must be used when funds cannot be withdrawn from a vault due to the inability to generate a signed transaction directly using the io.vault product. This can occur for example, by a critical software malfunction, a malicious DOS attack, a permanent service shutdown, or a critical loss of access to the io.finnet app by the user(s).
Please Note	The tool will recover a key that is usable for all existing supported coins in the following wallets: **MetaMask** (for Ethereum and EVM-based coins and tokens), **Electrum** wallet (for Bitcoin), and **TronLink** (for Tron). For newer supported chains and coins not listed here, please contact us for further information on which app to use for recovery.

7.4 Best practices

Below are some best practices we advise for all users and clients using the io.network and io.vault products;

Business Area	**Best Practise Detail**
Redundancy of users / devices	Create vaults with redundancy of users and their devices to avoid requiring implementation of the disaster recovery process for instances of a single user losing a signing device.
Backing up devices	Ensure all users are consistently and frequently backing up their device to the cloud

	● At a minimum, each user device should be backed up each time it participates in creation of a new vault or a vault re-share as these processes result in new shares being created locally on the devices