Developing a Recovery Plan for Cryptocurrency Holdings

Your company's recovery plan is the most important document you can create to ensure your business will survive disasters - whether natural or man-made. Coin recovery should be just one part of your overall strategic operations and recovery plan.

This process typically takes 3-4 meetings. Remember to encrypt internal communication about your recovery plan to protect its confidentiality.

Before your first meeting: review the questionnaire below and add questions you think may be relevant. Do not delete questions at this point. Then distribute the questionnaire to your team with instructions for them to review the document, make notes and be prepared to discuss at your first meeting.

First Meeting: Goals (1) assign sections to responsible person(s), (2) identify and clarify questions that are unclear, (3) add new questions to everyone's list, (4) discuss communication protocols, (5) set deadline for second meeting. Be sure to include developers and systems administrators in the conversation.

Subsequent Meetings: Review findings and begin drafting recovery plan.

Vital Records:

What vital records are required for recovery of coins?
What vital records are required for the continuation of the business? (for example what data do you need of employees, clients, vendors, investors; accounting and payroll records; insurance policies; tax returns; contracts, etc.)
Where are they backed up?
How will they be accessed in case of emergency?
Who has authorization to access them?
Are they encrypted?
Who has the encryption passwords?
Who is responsible for records management?
Who is responsible to update the backup copies of these records and how often?
Where are insurance contracts located, if any?
What, if anything, can you do to mitigate loss of one or more repositories of vital records?

Recovery Event Processes: (recovering funds from single addresses)

Who is responsible to initiate the recovery and under what circumstances?
Who must initially verify the request and what are the verification standards?
How is verification documented in an auditable way?
To what address will the recovery transaction sweep the funds?
Who created the address and how is customer/client control preserved?
Has the new address been tested?

Who will create the recovery transaction? (note, this should be different from the person to initiate the recovery)
How will the recovery transactions be verified, as properly authorized and going to the correct address?
What methods are in place to eliminate opportunities for collusion or bad actors?
How will the verified transactions be transmitted to the recovery company?
What is the process for the recovery company to verify the validity of the recovery request?
What if the recovery company cannot verify the recovery request or if the recovery request was unauthorized?
If the recovery company or authorized multisig key holder provides signed transactions, who is responsible to broadcast them and under what circumstances, if any, should they not be broadcast? (This is particularly relevant in an entire tree recovery)

Recovery Event Processes: (recovering funds from HD or HDM trees)

Review the Recovery Event Process in terms of recovering an entire tree or all trees.
What changes?
Are there additional safeguards in place to prevent errors?
Who, within the company, will be responsible to oversee the recovery of trees?
In the event the company is no longer operational, who will be responsible to facilitate recovery?

Payment for Recovery:

Who will pay transaction fees for the recovery transactions?
How will transaction fees be paid (company hot wallet, pre-divided UTXO, customer)?
Will the transaction fees be chained, affecting confirmation of other recovery transactions?
Who will pay the recovery company's fees?
If a fund has been set up to pay recovery fees, who manages/administers the fund?
If not, how will recovery companies be paid?

Communication:

Who is responsible to communicate to customers/clients/employees/public about the recovery?
Are there communication policies in place that govern crisis communications?
If so, where can employees find the policies during a crisis?

Changes to the Recovery Plan:

How often is the plan reviewed and by whom? (must be at least annually)
Who is authorized to make changes to the plan and by what process are changes made?
Where is the recovery plan stored?
Are redundant copies stored securely off-site?
How will they be accessed in case of emergency?
Who has authorization to access them?
Are they stored encrypted?
Who has the encryption passwords?
Who is responsible to update the redundant plans and ensure the most current versions are properly stored?

Building a Key Compromise Policy:

How many keys are currently in use within the company and to which assets/addresses/projects are they associated?
Who are the authorized signers for each address and where are the primary keys stored?
Where and how are backup keys stored?

What is a key compromise? (examples include: system hacked, vulnerability identified on key generation or storage device, physical compromise of key storage location, authorized signer leaves the organization, incomplete chain of custody logs)

How will the company learn that one or more keys may have been compromised?

Who should be notified of possible compromise?

What confidentiality policies, if any, are implemented during investigation of compromise?

What steps should be taken (in succession) during the investigation of a possible compromise?

How will a compromise be confirmed or disproved?

Who should be notified if compromise is confirmed?

How will they be notified?

What is the process for investigating possible compromise?

What is the process for migrating funds if the company's security is breached? If a relevant third party's security is breached?

What is the process for limiting damage to clients and the company itself in the event of key compromise?

Other Considerations:

Personnel: In the event of emergency, who will be responsible to coordinate company efforts and lead the Recovery Team? Who should be part of a Recovery Team?

Physical Locations: If you have a physical location, you should also consider physical evacuation procedures, employee communications, and business continuity plans for geographic natural disasters including fire, flood, etc.

Encrypted Communications: As a reminder, encrypting and signing communications whenever possible protects both confidentiality and authenticity (prevents man-in-the-middle and impersonation attacks).

Audited Standards: Companies should consider building systems compliant to industry best practices and standards, such as the CryptoCurrency Security Standard.

Hiring Third Key Solutions to Review Processes:

Policies and processes will be unique for each organization, project, and team. We do not build processes or policies for you; outsourcing these policies make them pointless as your team won't understand or follow them when the time comes. We may help guide your team through the process or we may simply review your policies and give feedback. We do not provide security advice or audits. Contact us for availability: info@thirdkey.solutions