SOP- The Handling of Authenticators that have been Compromised by Loss, Theft, Unauthorized Duplication or Unauthorized Usage

SOP #:	C.3
Version:	1.0
Author(s):	Al Tariq Sheik

1. PURPOSE

The security of a DID account is heavily reliant on the bound authenticator, which serves as a digital key to access the account. However, in situations where the authenticator is lost or stolen, the account's security is compromised as unauthorized individuals may gain access to sensitive information. Similarly, if the bound authenticator is duplicated or used without the consent of the subscriber or administrator, the DID account is considered compromised, and its confidentiality and integrity are put at risk.

To mitigate such security and trust-related risks, it is crucial for administrators to follow clear and comprehensive processes and procedures that are designed to handle the event of an authenticator breach. These protocols include immediate revocation of the compromised authenticator, as well as thorough investigations to determine the extent of the breach and any potential damage caused. By implementing proactive measures, administrators can minimize the likelihood and impact of future security breaches, thereby enhancing the security and trust of the DID system

2. SCOPE

This document outlines processes and procedures that must be followed by administrators in events that result in a compromised authenticator, including loss, theft, damage, or unauthorized duplication. To prevent or detect potential identity misuse, administrators are expected to implement a fraud detection system capable of promptly identifying any suspicious activity.

To ensure the security and integrity of digital identity accounts, the processes and procedures outlined in this document must be followed throughout the DID account's lifecycle. These measures include immediate revocation of the compromised authenticator, as well as prompt investigation and resolution of any suspected breaches. Adherence to these guidelines will allow administrators to maintain the trust and security of the digital identity system, preventing and mitigating any potential risks or breaches.

3. DEFINITIONS

Digital Identity (DID) – An online personal identity system.
Standard Operating Procedure (SOP) – The functions, processes and procedures that should be followed by Applicants, Subscribers, Claimants and Admin.
Subscriber – An Applicant who has passed validation and verification, and has been enrolled into the online Digital Identity system. Also, a Claimant who has passed authentication. The Digital Identity account holder.
Claimant – A person who claims to possess an identity and has not yet passed authentication.
Admin/Administration – The staff of the Digital Identity provider, who conducts Onboarding and Identity Lifecycle Management.

4. PROCESSES AND PROCEDURES

A. Subscriber loses their authenticator, or it is stolen:

i. The subscriber notifies the administrator of loss, theft, or damage of authenticator.
ii. The administrator expires the authenticator associated with the subscriber's account.
iii. The subscriber must repeat the identity proofing process for security reasons.
iv. The administrator confirms that the authentication claimant is the same person who was previously bound to the proofed evidence.
v. The administrator binds the replacement authenticator to the subscriber's account.
vi. If the subscriber has other remaining authenticators for multi-factor authentication, they may continue to use them for account access.

B. Authenticator is duplicated but it was not authorized:

i. The administrator activates fraud detection measures by incorporating intelligence.
ii. The administrator invalidates the current authenticator.
iii. The subscriber is required to undergo the identity proofing process again.
iv. The administrator verifies that the new claimant is the same as the one previously authenticated.
v. The administrator associates the replacement authenticator with the subscriber's digital identity.

5. SOP APPENDICES

Revision History:	Version	Effective Date	Description
blank	1.0	18-04-2023	First Approval