|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Changes Made** |
| 1.0 | 16/09/2024 |  |
|  |  |  |
|  |  |  |

*Prepared by the Trustworthy Digital Infrastructure for Identity Systems Team*

*This work was supported, in whole or in part, by the Gates Foundation [INV- 057591]. Under the grant conditions of the Foundation, a Creative Commons Attribution 4.0 Generic License has already been assigned to the Author’s Accepted Manuscript.*

Standard Operating Procedure TEMPORARY ACCOUNT SUSPENSION (FRAUD, INELIGIBILITY, GOVERNMENT ORDER)

LM.5.A - WITH RATIONALISATION

**Version Control**

**Guidelines for Maintaining the SOP Version Control Table:**

* **Version**: Assign a new version number for every update. Minor changes can be denoted by incremental changes in decimal (e.g., 1.1, 1.2), while major changes can increment the whole number (e.g., 1.0 to 2.0).
* **Date**: The date when the changes were finalised.
* **Changes Made**: A brief description of the changes or updates made.

Table of Contents

[1. Purpose 3](#_Toc177314689)

[2. Definitions and Abbreviations 3](#_Toc177314690)

[3. Application 3](#_Toc177314691)

[3.1 Ownership and Stakeholders 3](#_Toc177314692)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314693)

[3.1.2 IT and Security Teams 3](#_Toc177314694)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314695)

[3.2 Users and Beneficiaries 3](#_Toc177314696)

[3.2.1 General Public 3](#_Toc177314697)

[3.2.2 Government Agencies 4](#_Toc177314698)

[3.2.3 Private Sector Companies 4](#_Toc177314699)

[4. Prerequisites 4](#_Toc177314700)

[4.1 Assumptions 4](#_Toc177314701)

[4.2 Constraints 4](#_Toc177314702)

[5. Process Flow - Process and Procedures 4](#_Toc177314703)

[5.1. Initiate Fraud Report: 4](#_Toc177314704)

[5.2. Verify Suspicious Activity: 4](#_Toc177314705)

[5.3. Escalate to Local Authority: 4](#_Toc177314706)

[5.4. Government/Court Order Processing: 5](#_Toc177314707)

[5.5. Deactivate Account and Authenticator: 5](#_Toc177314708)

[5.6. Notify Stakeholders: 5](#_Toc177314709)

[5.7. Report Generation and Storage: 5](#_Toc177314710)

[5.8. Error and Exception Handling: 5](#_Toc177314711)

[5.9. Termination of Process: 6](#_Toc177314712)

[6. Visualisation 7](#_Toc177314713)

[7. Rationalisation 8](#_Toc177314714)

[8. References 9](#_Toc177314715)

# 1. Purpose

This SOP guides the suspension of accounts on a temporary basis for reasons such as fraud, ineligibility, or government order. It ensures secure and accurate processing through proper verification, documentation, and error handling.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**KR**: Key Revocation

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**AC**: Access Control

**HTTPS**: Hyper Text Transfer Protocol Secure

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership**: Oversee the suspension process.
* **Responsibilities**: Ensure secure and compliant suspension of accounts.

### 3.1.2 IT and Security Teams

* **Ownership**: Manage technical infrastructure and security protocols.
* **Responsibilities**: Maintain system security, data encryption, and infrastructure.

### 3.1.3 Compliance and Legal Departments

* **Ownership**: Ensure compliance with legal and regulatory standards.
* **Responsibilities**: Oversee compliance checks, documentation, and regulatory adherence.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users**: Individuals reporting fraud or ineligibility.
* **Usage**: Provide updated identity verification for secure account management.

### 3.2.2 Government Agencies

* **Users**: Agencies requiring verified and updated identities for services.
* **Usage**: Utilise verified identity information for secure service delivery.

### 3.2.3 Private Sector Companies

* **Users**: Businesses requiring updated identity verification.
* **Usage**: Use secured identities for compliance and verification purposes.

# 4. Prerequisites

## 4.1 Assumptions

* Subscribers have access to required documents and authentication methods.
* Administrators are trained to handle the suspension process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The suspension process may be affected by system downtimes or regulatory changes.
* Secure devices and internet access are required for administrators and users.

# 5. Process Flow - Process and Procedures

## **5.1. Initiate Fraud Report:**

* **Claimant/Subscriber Action:**
  + The process begins when a subscriber or claimant reports suspicious or fraudulent activity via phone, online, or through the DID portal.
* **Output:** Fraud report is initiated and logged.

## **5.2. Verify Suspicious Activity:**

* **Verifier/Administrator Action:**
  + The verifier or administrator receives details of the reported suspicious activity. They verify the subscriber's activity in the database to confirm any anomalies or unauthorised access.
* **Output:** Verification of suspicious activity status.

## **5.3. Escalate to Local Authority:**

* **Verifier/Administrator Action:**
  + If activity is found to be suspicious, the verifier escalates the report to the local authority for further review. The verifier also reviews all activities to gather comprehensive details.
* **Output:** Suspicious activities are reviewed and escalated to authorities.

## **5.4. Government/Court Order Processing:**

* **Verifier/Administrator Action:**
  + In cases requiring legal intervention, a government or court order is received to either revoke or terminate the account. This step includes validating the report's authenticity by alignment with government officials.
* **Output:** Court order for account action received and validated.

## **5.5. Deactivate Account and Authenticator:**

* **Private Network Systems (Server) Action:**
  + If fraud is confirmed, or a legal order is validated, the server deactivates the DID account and associated authenticators. The account status is updated to reflect the suspension.
* **Output:** Account and authenticators are deactivated, and the status is updated.

## **5.6. Notify Stakeholders:**

* **Public Network Systems (Client) Action:**
  + Notifications are generated and sent to relevant parties. This includes informing the subscriber of the account deactivation and providing the end date, or notifying them if a request for suspension is rejected, along with reasons.
* **Output:** Notifications are sent to subscribers, claimants, and reporting authorities.

## **5.7. Report Generation and Storage:**

* **Private Network Systems (Server) Action:**
  + A detailed report on the suspension process is generated. The report includes the reasons for suspension, the verification process, and the outcome. This report is stored securely in the DID account database for future reference.
* **Output:** Detailed report generated and stored.

## **5.8. Error and Exception Handling:**

* **Private Network Systems (Server) Action:**
  + The system includes mechanisms to handle errors and exceptions during the suspension process. These could involve discrepancies in verification data, unauthorised access attempts during the suspension, or notification delivery failures.
* **Output:** Errors are managed, logged, and resolved to ensure process integrity.

## **5.9. Termination of Process:**

* **Private Network Systems (Server) Action:**
  + If the request for account suspension is rejected or the process is completed, the system logs the final status. It either terminates the request or finalises the account suspension with the provided end date.
* **Output:** Process is terminated, and the final status is logged.

# 6. Visualisation

A screenshot of a computer screen

Description automatically generated

Please refer to the [GitHub](https://github.com/alan-turing-institute/Standard-Operating-Procedures-for-Digital-Identity-Systems) repository for further information.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LM.5.A TEMPORARY ACCOUNT SUSPENSION (FRAUD, INELIGIBILITY, GOVERNMENT ORDER)** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | Initiation of account suspension process | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Authenticate User | User logs in to report fraud | Authentication Server | Two-Factor Authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Report Fraud Activity | User reports suspicious activity | DID Portal | Data input validation | ISO 27001 Data Protection, GDPR Compliance for Data Handling |
| 4 | Verify Activity in Database | Verify reported activity against database records | Database Server | Data integrity checks | ISO 27001 Data Integrity, FATF Digital Identity Guidelines |
| 5 | Receive Government or Court Order | Official order to suspend account received | Administrative System | Compliance with legal requirements | ISO 27001 Legal Compliance, eIDAS Trust Services |
| 6 | Deactivate DID Account and Authenticators | Suspend all account activities | Account Management System | Immediate deactivation of access | ISO 27001 User Access Management, Aadhaar Secure Authentication Practices |
| 7 | Notify Reporting Party/Authority | Inform about the suspension and reason | Notification System | Secure notification delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 8 | Log the Process and Status | Record all actions and outcomes | Security Logs | Audit trails, logging | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 9 | End Process | Finalise the suspension process | System | Secure session termination | ISO 27001 Information Security Management |
| 10 | Exception and Error Handling | Manage errors and exceptions during the process | Security System | Error logging and response handling | ISO 27001 Event Management, NIST SP 800-61 Incident Response |
| 11 | Mask & Encrypt UIN and Subscriber Details | Secure personal details of the user | Database | Data encryption and masking | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 12 | Terminate Process if Needed | Lock user account if further fraud is detected | Authentication System | Account lockout policy | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |

# 8. References

1. NIST. Digital Identity Guidelines: Age Verification Guidance. Available at: [https://pages.nist.gov/800-63-3/].
2. eIDAS. Identity Proofing Requirements. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\_.2014.257.01.0073.01.ENG].
3. ISO. 27001, Secure System Access Control. Available at: [https://www.iso.org/standard/27001].
4. Aadhaar. Account Creation and Management. Available at: [https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar/aadhaar-enrolment.html].
5. SingPass. Account Creation and Management. Available at: [https://www.singpass.gov.sg/home/ui/assets/pdf/Singpass\_Registration\_Guide.pdf].
6. FATF. Digital Identity Guidance: Authentication Mechanisms. Available at: [https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html].
7. Estonia ID. Data Protection Practices. Available at: [https://toolbox.estonia.ee/asset-page/252494-e-estonia-guide-full-brochure].
8. Emirates ID. Available at: [https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id].