**SSC Offline**                                                          **Thursday 9 Sep**

**This WI is awaiting approval by Mark Wright and should not be used.**

| | |
|---|---|
| **WI Reference:** | WI3649S |
| **Title:** | Data Correction |
| **Author:** | Steve Parker |
| **Created:** | 08/09/2011 |
| **Last update:** | 11/02/2021 |
| **Last updated by:** | Adam Woodley |
| **Version:** | 18 |

**Details:**

GDPR regulations require that access to personal data remains within the European Union and PCI data security standards mandate physical security restrictions must be applied where update access is allowed to user data. Currently the only units which fulfil all these requirements for data access are the SSC and ISD Unix. The responsibility for data correction is vested with the SSC although ISD sometimes act under SSC authorisation (via the application of a tested script).

Corrections to live system data must be authorised via Account change control and auditable. Any correction requiring APPSUP role is to be witnessed by a second member of the SSC. Both names must be recorded on the change control for audit purposes.

# Data corrections

Support investigation may indicate the need for a data correction. In this context data correction is any support action that results in the modification or removal of Post Office data. If any correction is required then details must exist in the form of narrative on, or attachments to, a Peak incident to provide a clear audit trail. An approved Account change control entry (currently TfSNow) must also exist and be cross-referenced from the Peak. See below for details of change control.

# Financial data

Changes to financial data are rarely required. Where a requirement exists such changes must be made via contra journal entries to maintain audit trail and the change must be made using the two man rule. The "two man rule" (sometimes called the "four eyes rule" in security circles) specifies that there must be two individuals that must act in concert in order to perform some action. Further, each individual should have comparable knowledge and skill in order to detect attempts of subversion initiated by the other.

Within the SSC, one member of the SSC will perform the data correction while a second member of the SSC will witness the change being made. Both names must be recorded on the change control for audit purposes.

See the Host Branch Database Support Guide for details of the transaction correction tool used by SSC to correct transactions by inserting balancing records to transactional / accounting / stock tables in the BRDB system.

# Change Control

BM control for SSC data corrections will be raised by the MAC team. They will include the requirement for approvals from Post Office departments namely:

- POL Security
- POL Service
- POL Financial Service Centre

The Service team will be responsible for obtaining those authorisations (via the POA Duty Manager mailbox).

The SSC will supply the information the MAC team require to create a meaningful change. This will include:

1. A summary which describes the reason for the change
2. Impact of issue and ramifications of not completing the change
3. Technical detail showing how the change is being carried out.

# Other changes

Some changes that the SSC make are part of other Account processes. Where this is the case the team which manages the process will raise appropriate change control on the SSC's behalf. At the time of writing these are:

| Process | Team | Notes |
|---|---|---|
| Reconciliation | SecOps | |
| ARQ | SecOps | |

**References:**

| Reference Type | Value | Description |
|---|---|---|
| DOC | DESAPPSPG0001 | Host Branch Database Support Guide |

| DOC | DESAPPHLD0020 | Branch Database HLD |
| WI | WI3028L | Transaction Correction Tool / Appsup role |