POL00337652

POST OFFICE

Horizon Data Change Process

May 2021

INTERNAL

POL00337652

Overview

- Occasionally, at Post Office request, Fujitsu make changes to Horizon data to correct issues, for which they temporarily apply an elevated level of access to an engineer user account, e.g.
  - Assisted branch rollover
  - Change or delete branch data – e.g. remove a stuck user session or transaction
  - Change or delete a back end system file
- These changes must be approved in advance by all these Post Office teams, via email, as follows:
  - IT Service
  - IT Security
  - Business Operations (Branch Reconciliation Team or Data Governance, according to the change type)
  - Postmaster (only required for changes which impact a branch)
- The change details are recorded as an incident, and the approvals are attached to the incident ticket
- Once Fujitsu have made the change they provide evidence of what they did while the elevated access was in place, and attach the evidence to the incident ticket
- The Horizon IT Security team review the evidence to confirm the elevated access was used as agreed
- The Horizon IT Service team investigate why the change was required, with a view to preventing similar changes being required in future

POL00337652

Identification & Categorisation

- When a Horizon data change is required, Fujitsu will log an incident, and include "Elevated access" in the short description, so these changes can be easily identified
- IT DSD populate a template describing the change from information in the incident ticket as far as they can, seeking any missing information from appropriate contacts. The template is available via a knowledge article: KB0014710
  - If there are any issues, IT DSD escalate to Horizon IT Service team
- Once the template has been collected, IT DSD request approvals for the change according to the change type
  - The approvers for each team and change type are listed in the knowledge article.
  - The knowledge article is reviewed every 3 months, to check the approvers are correct

POL00337652

Requesting Approvals

- Once the required information for the request has been added to the template, IT DSD request approvals as follows:
  - Send approval request email to **all** the people listed as approvers, according to the change type
    - The approvers will agree within their teams who responds to the requests
  - Include the "Elevated access – …" wording from the short description in the email subject line
  - Attach a PDF extract of the incident, and the request template, to the email
  - Include the following wording at the end of the email ***Please let us know if any changes are required to the approvers for these changes for IT Service, IT Security, or Operations.***
  - Ask approvers to respond on the same day if possible, and follow up with any group which does not respond within the day
  - If the change is required to resolve a major incident, ask for immediate approval, and follow up with instant message or phone call as necessary
  - For changes which impact a branch, use the **Branch Information Lookup** tool to identify the Area Manager and Regional Manager for the branch, and include them on the email requesting approval

POL00337652

Postmaster Approval

- For changes which impact a branch, the Area Manager will contact the Postmaster, and discuss the change with them and confirm they are happy for the change to be made
  - Changes which require Postmaster approval include assisted rollovers, changes to or removal of stock units, and changes to or removal of user sessions
- The Postmaster will then provide approval via email
  - The Postmaster approval may be emailed directly to IT DSD, or the Area Manager may forward the approval email from the Postmaster to IT DSD
- For branches which are run by some multiple partners, the partner company is considered to be the Postmaster
  - For these branches the approval will be provided by the partner company head office
  - An example where this will be the case is Co-op branches
  - For these branches, the Area Manager will contact the appropriate relationship manager, who will liaise with the partner company to get approval

POL00337652

Responses to Approval Requests

- IT DSD attach the approval emails from each team to the incident ticket
- If all approvers have approved the request:
  - IT DSD send evidence of the approvals to Fujitsu, advising they can go ahead with the change
- If any approvers are not able to approve the request:
  - The approver should include the reasons why they cannot approve in their email response, and say what additional information they need, in order to be able to approve
  - IT DSD should then contact the Horizon IT Service team (Martin Godbold, Lorna Owens), with details of why approval has not been provided
  - Horizon IT Service will then follow up with the approver to try to resolve the issue
  - If it is decided the change will not go ahead, or if Fujitsu report that it was not possible to implement the change, IT DSD email all the approvers for this change type, informing them of the situation.

POL00337652

Implementation

- On receipt of approval to proceed, Fujitsu enable the elevated access required to make the change
- Fujitsu then make the change, and remove the elevated access
- Fujitsu then update the incident ticket to confirm the change has been made, and to attach evidence that the change made while elevated access was in place was agreed.
- Once Fujitsu confirm they have implemented the change, IT DSD email all the approvers (for this change type), advising them the change has been completed. This will act as a trigger for:
  - IT Security team to review the evidence provided by Fujitsu
  - IT Service team to investigate the root cause of the change being required, with a view to not having to make similar changes in future