## OPTUS DISENGAGEMENT PROTOCOL

***INTRODUCTION:*** *The following document details disengagement protocol. In all cases, TSA retains the right to the application, while Optus retains the rights to customer data and contractually agreed-upon assets (e.g. Business Area repository, etc.). Optus also owns the code in the “Optus repo.” In there, Optus will find a webserver IP code, and an application to map location ids from Optus system to TSA translation application.*

*Disengagement will result in the TSA application no longer supporting any previous functions, and Optus assuming control of all functions. TSA recommends execution take place between Monday, November 18th and Friday, December 6th. This allows 1 week of execution time per environment (SIT, PPT and PROD) before original service terms cease. Please note Optus also needs to consider their part in the transition, and what aspects need to be completed on the Optus side. TSA does not have access to Optus operations, and this document may not fully represent everything Optus needs to consider.*

***SCHEDULE of EVENTS:*** *Each week TSA and Optus would execute the following action, in the following order - TSA will work on items 1(b), 2(b), 3(b), 4(b) and 5(b). As a result, Optus will then need to do 1(c), 2(c), 3(c), 4(c) and (5)c. Once TSA has confirmed 6(b) Optus would need to execute 6(c). Week one (18/11 – 22/11) will be for SIT. Week two (25/11 – 29/11) will be for PPT. Week three (2/12 – 6/12) will be for PROD. Approaching disengagement in this manner will ensure each environment is appropriately addressed, and that any questions are addressed in pre-production environments before production is touched.*

**MAJOR ITEMS**

1. **SITE SERVICE: Optus has decided to discontinue use of Site Service.**
   1. Impact to merchants: If Optus wants to move to new desktop and mobile sites, all merchant sites will need to be deleted and updated. If Optus wants to retain current sites, Optus should know they will be viewable, but will not retain full functionality, nor will the merchant be able to modify or redeploy them.
   2. TSA Actions to Disengage:
      1. Stop Jboss server.
      2. Uninstall Optus ear file on odjaboss01 and odajboss02 servers in SIT, PPT and PROD.
      3. Delete the TSA property files and remove tsa\_messaging\_node1 directory.
   3. Optus Actions to Disengage and Delete Sites:
      1. Delete the site files in the end customer web servers.
      2. NOTE: If Optus does not delete the site files, Merchants may be able to still access partially functioning sites.

***NOTES:*** *TSA owns the code that controls the Apache configuration that controls a number of aspects about the site. If Optus opts to keep the sites, Optus will need to put in their own mobile detection utility on their webserver. They will need to re-configure the “go to full desktop site,” and the “contact us” functionality. They will assume update responsibility for social plugins and maps. Optus is already responsible for the rights to images used on merchant sites.*

1. **CAMPAIGN SERVICE & MCC: Optus has decided to discontinue use of Campaign Service. Disengagement will result in the TSA application no longer having access to the Optus AdWords MCC. TSA personnel will also no longer have access to the Optus MCC.** 
   1. Impact to Merchants:
      1. Optus will no longer be able to deploy or redeploy campaigns using the TSA application.
      2. Existing SEM campaigns for current merchants will need to be manually managed by Optus, or deleted, as budgets won’t be set or updated via TSA application.
   2. TSA Actions to Disengage:
      1. Stop Jboss server.
      2. Uninstall Optus ear file on odjaboss01 and odajboss02 servers in SIT, PPT and PROD.
      3. Delete the TSA property files and remove tsa\_messaging\_node1 directory.
      4. Stop AdMax listener in delete bidmgr build from bidding and bibu servers in SIT, PPT and PROD and delete the configuration files in /usr/local/tsa and /var/local/tsa.
      5. Delete AdMax listener in /etc/init.d.
      6. Stop cron jobs on bidding and bibu servers.
      7. Stop TSA replication on accounts and warehouse servers.
   3. Optus Actions to Disengage Campaigns:
      1. Unhook API access
      2. Delete Admin access for optus-booster account
      3. Delete all TSA personnel accounts
      4. Begin active management of current merchant accounts in MCC.
      5. Delete all test merchants in SIT and PPT. This can be done manually from the MCC after disengagement without impact to the system as the merchants will only exist in the MCC at this point.
      6. Optus to stop sending the calldata files to the bibu server in PROD for call-tracking information.

NOTE: If Optus does not manage SEM campaigns, the accounts will continue to spend unchecked.

1. **SSUI: Disengagement will result in Optus and Optus merchants no longer having access to the SSUI.**
   1. Impact to Merchants:
      1. Merchants will no longer have access to self-service UI to customize changes on their website.
   2. TSA Actions to Disengage:
      1. Delete SSUI build and configuration files.
   3. Optus Actions to Disengage:
      1. Inform Merchants that they can no longer modify their sites
      2. Work with NCS team to disengage OfficeApps from calling SSUI.
      3. NOTE: If Optus does not disengage office apps from calling SSUI, customers will be able to login to Office apps but they won’t be able to login to SSUI properly.

1. **DATA FEEDS: Disengagement will result in Optus no longer receiving data feeds for weekly reports. Optus retains data feed data.**
   1. Impact to Merchants:
      1. There is not impact to Merchants.
   2. TSA Actions to Disengage:
      1. Stop data feeds and report service running on odabackjboss server in SIT, PPT, and PROD.
      2. Delete kettle configuration files
   3. Optus Actions to Disengage:
      1. Determine mechanism used by Optus to pick up data feeds, and stop it.
      2. Every data feed file ever generated will remain in the odabackjboss server under /home/optus/data feeds. Optus needs to determine whether they would like to keep these files, or delete them. TSA will not have access to these files after disengagement.
      3. NOTE: If Optus does not stop picking up the datafeeds, the service Optus are using to pick up the datafeeds won’t be able to pick up any files, thus producing errors in Optus side.
2. **PIXEL SERVERS: Disengagement will result in the pixel server no longer logging pixel hits for paid or natural traffic.**
   1. Impact to Merchants:
      1. Site data will no longer be logged, nor fed into Merchant’s Dashboards.
   2. TSA Actions to Disengage:
      1. Delete the Apache configuration for pixel servers.
      2. Remove pixel server builds (TSAApp) that enable pixels to be logged.
      3. Disable TSA pixel round robin.
   3. Optus Actions to Disengage:
      1. Optus may or may not choose to keep the files for the pixel data logged. The data will remain logged on the pixel servers, and Optus can choose to keep these files, or delete them. TSA will not have access to these files after disengagement.
      2. NOTE: If Optus does not disengage, files will continue to reside on Optus servers.

***NOTES:*** *If Optus chooses to keep the sites, they may want to remove TSA’s pixel string from the sites.*

1. **DATABASES: Disengagement will result TSA no longer having access to the data in the databases, but the databases will not be wiped unless Optus decides to do so.**
   1. Impact to Merchants:
      1. Once the disengagement has taken place there won’t be an application running to get data from the databases, so at that time, there will be no known impact.
   2. TSA Actions to Disengage:
      1. TSA to inform Optus when the application has been disengaged.
   3. Optus Actions to Disengage:
      1. Stop replication on jboss1 and jboss2 servers on SIT, PTT and PROD.
      2. Stop regular DB maintenance; including Percona
      3. NOTE: If Optus does not disengage, the databases will continue to exist and monitoring scripts may produce errors due to the lack of maintenance.

**OTHER ITEMS**

**EMAILS**

TSA Actions: Return Optus the user name and password details for oda.issues@optusnet.com.au, optusbooster@gmail.com. Stop email notifications on all servers.

**TEST SITE**

TSA Actions: TSA to return UN and PW for mybizonlinetest.com.au to Optus.

**MONITORING**

TSA Actions: Uninstall nagios and disable all nagios plugins. Remove all TSA email addresses.

**EVENTUM (Customer Care Ticketing System – TSA side)**

TSA Actions: Delete Eventum instance, [optus-support@thesearchagency.com](mailto:optus-support@thesearchagency.com) and all associated data.

**TAXONOMY**

TSA Actions: Provide Optus with BA, BC, ads, keywords and mobile ad files and desktop and mobile templates, and delete copies from system.

**EDITORIAL & CARE DOCUMENTS**

TSA Actions: Delete Google docs.

**BRAND UI**

TSA Actions: Delete Brand UI build and configuration files.

**SERVER ACCESS**

TSA Actions: Disable access to Optus servers from Rhode Island office (site to site VPN).

Optus Actions: Delete all SSH keys for TSA crew so TSA can’t login into SIT, PPT and PROD.

\*NOTE: If Optus does not disengage, there are no known ramifications.

**LICENSES & ROYALTIES**

Optus Actions: Optus needs to follow up on Google Maps and Image royalty items.

\*NOTE: If Optus does not follow up on their Google Maps and Image royalties they may continue to incur undesirable costs.