

Incident Report - February 2, 2016

Incident #2016-130

IDM - Alias Removal

Summary

Following a testing exercise on Tuesday, February 2, 2016, the pre-production system of TridentHE (IDM) was left in a “confused” state where it partially thought it was still running as in the production system. This went unnoticed as only a small handful of accounts were originally affected. On Saturday, February 6, 2016, however, a large sync job increased the visibility to a larger number of accounts and the issue was identified.

Impact

In total 2,300 aliases were improperly removed from production accounts. This then caused email being sent to those addresses to be bounced. A non-delivery message was received by the sender.

Root Cause

Following a test exercise, the pre-production system was left with some connectivity to the production environment.

Resolution

Backups of the database were used to recover the deleted aliases. The aliases were then repopulated back onto the mailboxes.

Communications (Internal)

Once alerted to the issue by the IT Support Centre, the issue and resolution was communicated through Lync, phone, and face-to-face debriefings.

ITSP Communication (External)

Once the issue was confirmed, an ITS Notification was posted alerting the campus that ITS was investigating the issue. Upon resolution of the issue, the Notification was updated.

Lessons Learned

Upon returning a system to a non-production state following a test, carefully inspect activity to ensure the system is only communicating/updating the expected environments with the desired information.