

Policy on Change Controls Over the Universal Transaction Gateway

Introduction: The purpose of this paper is to describe Shift4's change control procedures for the Universal Transaction Gateway (UTG) after it has been deployed to the merchant environment. Merchants should use this information to update local change control policy and procedures in accordance with Requirement 6.4 of the PCI Data Security Standard (DSS).

UTG Change Control Types: At Shift4 Corporation we define three different types of changes to the UTG and corresponding events:

1. **Emergency Change.** Required immediately to prevent a cardholder data exposure or compromise.
2. **Break Fix.** Typically required as the result of UTG anomalous behavior not found in previous testing by the merchant, Shift4, or third party.
3. **Enhancement.** New feature and/or functionality requested by the merchant.

UTG Change Control Procedures:

Emergency Changes: Shift4's primary responsibility to the merchant is to secure cardholder data anywhere it is processed, transmitted, or stored by Shift4 payment applications. To that end Shift4 will immediately invoke an emergency change to a UTG in order to correct anomalous behavior that may cause leakage of cardholder data. Attempts will be made to notify the merchant before invoking an emergency change to the UTG, but if this is not possible, Shift4 will push the UTG change and notify the merchant after the fact. This procedure is necessary to eliminate the risk of a cardholder data exposure or compromise.

Break Fix and Enhancement: These types of changes to the UTG will be coordinated with the merchant on a case-by-case basis, as required by the individual merchant agreements. The merchant will be notified that a new UTG is available to download from the Web site. If required by local change control procedures, the merchant may download and fully test the new UTG before it is promoted to the production environment. In most cases Shift4 will assist with installation of the new UTG and depending on the relationship or established merchant agreement, the UTG update will be automatically pushed out.

Payment Application DSS Fundamentals:

All Shift4 products are developed in accordance with the Shift4 Software Development Lifecycle (SDLC) methodology, industry best practices, and the Payment Application (PA) DSS Requirement 5. Each version of the UTG undergoes rigorous, structured testing in a mockup of merchant environments in accordance with the Shift4 SDLC and the PA-DSS Requirement 7. This includes an independent code review to ensure Shift4 products are free of security vulnerabilities and gross abnormalities before they are released to merchants and partners. Shift4 cannot be held responsible for specific issues or UTG anomalous behavior relating to unknown changes in the merchant's environment.

The Shift4 Customer Support Center stands ready to assist with all issues pertaining to the UTG and may be contacted by calling (702) 597-2480, Option 2.