[Company Logo]

[Company Name]

PURPOSE:

The purpose of this procedure is to provide guidance for Information Systems Department personnel and other employees with regard to change management within the company. This procedure sets standards for how employees should go about putting a change into production.

This procedure will balance the concerns between security risks and operational risks. It has been determined that automated patching would not cover the full scope of issues, and thus this procedure has to be followed in regards to patching software. Making a change in hardware/software will be done and kept up to date to ensure integrity of data and applications. If a major service needs to be altered immediately, IT and the department responsible will coordinate for the update and communications should be sent out to those affected properly (Refer to procedure section below).

Definitions:

1. Downtime
   1. A period of time that a system is unavailable
2. Patch
   1. A set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bug fixes or bug fixes.
3. Software
   1. The programs and other operating information used by a computer
4. Vulnerability
   1. A weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system
5. Smoke-testing
   1. Known as “Build Verification Testing”, is a type of software testing that comprises a non-exhaustive set of tests that aim at ensuring that the most important functions work. The result of this testing is used to decide if a build is stable enough to proceed with further testing.
6. Non-production environment
   1. A software environment to be used exclusively for development or test activities, and not for business operations of users
7. Production environment
   1. An environment where functionality and availability must be ensured for the completion of day-to-day operations.
8. User
   1. An employee or consumer authorized to access the application/system

PROCEDURE:

1. Using the risk assessment guide, evaluate the change to determine the risk associated and identify its score.
   1. The score rankings are outlined within the Change Management Risk Assessment Document.
2. Submit a Change Request for any requests to be deployed which must be approved by IT and Business management.
   1. A change request will include basic information and a risk assessment guide which will include items such as; environment affected, number of employees affected, downtime required, ability to revert change, and ability to go into a non-production environment.
   2. If a non-production environment is not available for the application, ensure the change is monitored and done during hours outside business operations.
      1. An ability to revert changes is required when a patch is being deployed straight into the production environment.
      2. If there is no non-production environment for a third-party application, the vendor must be engaged during the patching event.
3. Deploy patches into a non-production environment to be smoke-tested by IT and monitored.
   1. If there are any issues, provide detailed documentation to the software development team so they can revise the patch and resubmit it for further testing.
4. Before production rollout, ensure backups have been synced.
5. If there will be downtime on a system, a communication should be sent to any affected teams/employees.
6. Deploy patches into the production environment during off-hours after 1 week of successful smoke-testing.
   1. Monitor for any issues; if something occurs, refer to 4a.
7. Document the patch management process, including any setbacks or issues that occurred.
8. Once devices have been patched, images must be updated to the recent patches.

Points of Contact:

1. The point of contact for this administrative guideline is \_\_\_\_\_\_\_\_\_. Contact for assistance or clarification of this procedure meant for software patching.
   1. Individual Roles/Positions