System Patching Policy

In this assignment, you will develop a patch management policy that adheres to corporate change management requirements. Understanding the set of changes conducted to a server or system to improve, update, shore up security vulnerabilities, and remove bugs is often referred to as patching. This action, usually put forward by the vendor, is often automatic in client operating systems.

Create a 500- to 750-word patch management policy that includes the following:

* **Overview:** Present a synopsis of the patching policy along with a stated goal.
* **Scope:** Identify to whom the policy applies.
* **Quality Assurance Plan:** Present a plan that certifies the veracity of the patch and verifies the success of the rollout. Be sure to identify change management requirements for pre- and post-implementation testing.
* **Frequency:** Include a defined schedule for all phases of the patching cycle. Be sure to address procedures for emergency patching and approval of exceptions to the patching schedule.
* **Rollback/Reversal Procedure:** Include a timeline, notifications, and supporting departments. Be sure to identify change management requirements for developing a rollback/reversal plan should a patch not function as desired.
* **Patching Exceptions:** Define the requirements and process for requesting a mitigating control in place of patching.
* **Authorizing Authority:** Identify at least two levels up and include organizational notification requirements for both patching and rollback.
* **Audit Controls and Management:** Document the process that evidences this policy is being followed in accordance with change management tracking requirements.