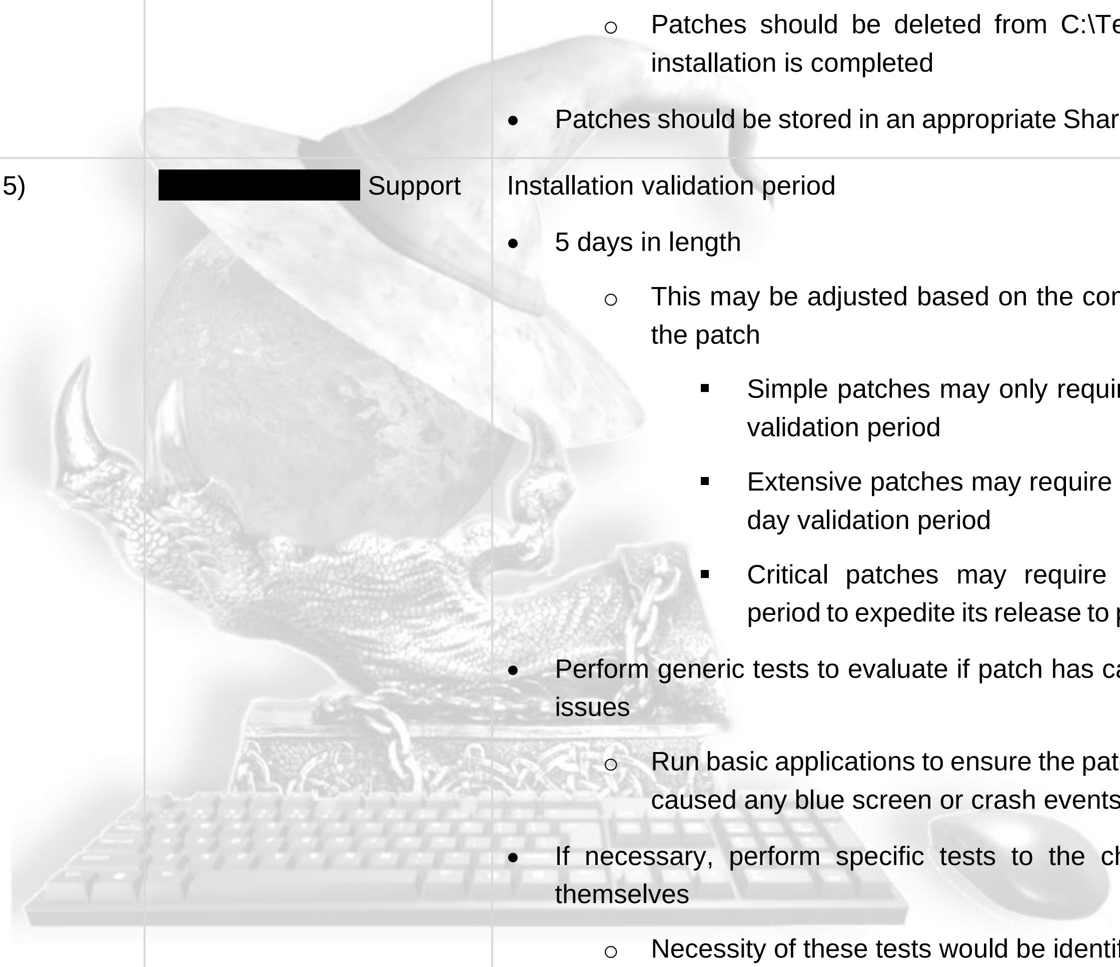
SAMPLE WINDOWS SERVER PATCH PROCEDURE

Sample of procedure to patch windows servers in appropriate order.

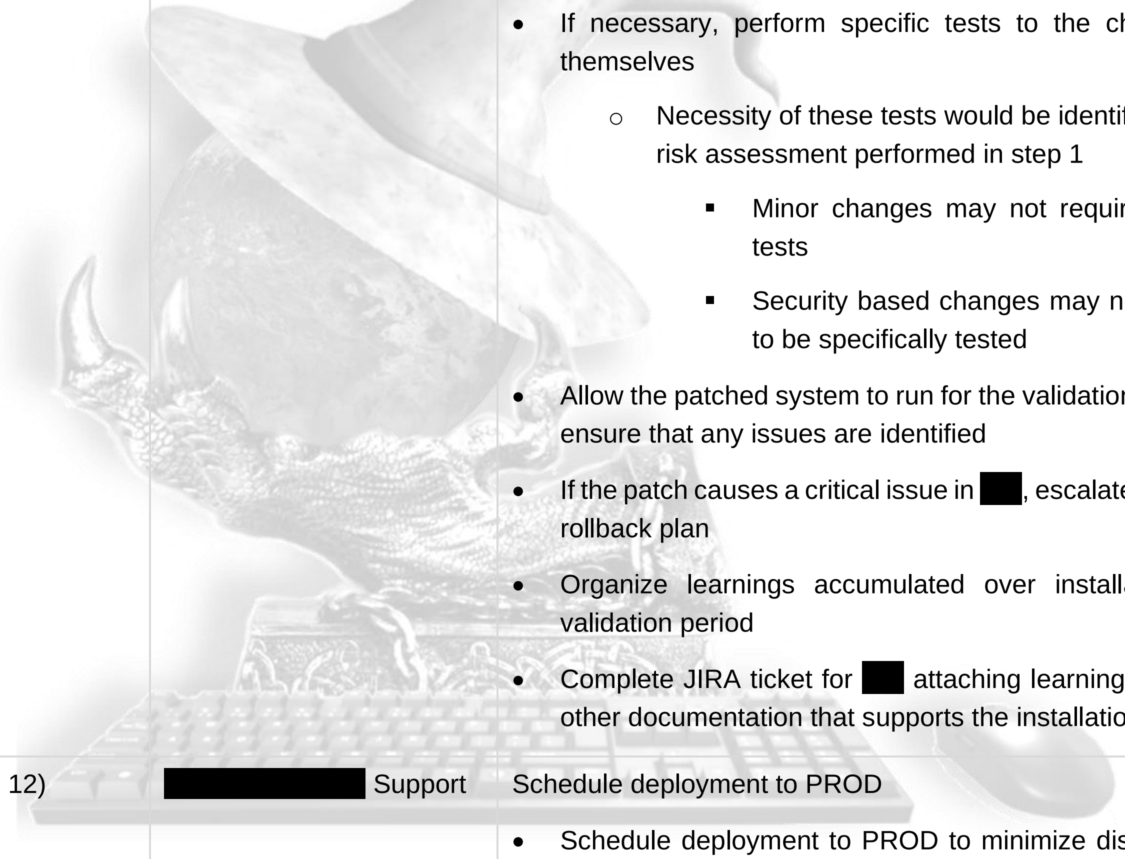
1.1 PROCEDURE STEPS

STEP	WHO IS RESPONSIBLE	WHAT TO DO
1)	[redacted] Support	Review KB article, conduct research on the patch and evaluate risks • On notification of a patch that is required for the [redacted] windows servers, seeks out the notes and performs any additional research of early adopters of the patch • Checks the patch against the [redacted] list of approved Windows Patches for [redacted] ○ If the patch is a critical security patch, then it may need to be installed even if it is not on this list. Ie: similar security issues to the Wannacry patching • Review notes ○ Evaluate the risks inherent in the patch ○ Asks for clarification on any issues or questions ○ On a case-by-case basis, evaluates the complexity of the release ○ Document which server roles are impacted by the patch
2)	[redacted] Support	Coordinates preparation for patch release • Sends out notification of the patch to all affected business areas • Schedules virtual server downtime • Takes a snapshot (image) of the designated [redacted] server being deployed to is taken prior to release ○ [redacted] servers must be kept in sync to avoid ADAM (Active Directory Access Management) issues • Snapshot serves as the rollback plan in case there are catastrophic issues with deployment of the patch



STEP	WHO IS RESPONSIBLE	WHAT TO DO
4)	[redacted] Support	Installs released patch • Performs primary installation • Troubleshoots any issues that arise during installation • Makes specific installation notes of any issues identified and what their resolution was • Patches are generally executed from C:\Temp unless the patch notes indicate otherwise ○ Patches should be deleted from C:\Temp when installation is completed • Patches should be stored in an appropriate Sharepoint site
5)	[redacted] Support	Installation validation period • 5 days in length ○ This may be adjusted based on the complexity of the patch ▪ Simple patches may only require a 3 day validation period ▪ Extensive patches may require up to a 30 day validation period ▪ Critical patches may require a shorter period to expedite its release to production • Perform generic tests to evaluate if patch has caused any issues ○ Run basic applications to ensure the patch has not caused any blue screen or crash events • If necessary, perform specific tests to the changes to themselves ○ Necessity of these tests would be identified by the risk assessment performed in step 1 ▪ Minor changes may not require specific tests ▪ Security based changes may not be able to be specifically tested

STEP	WHO IS RESPONSIBLE	WHAT TO DO
		• Allow the patched system to run for the validation period to ensure that any issues are identified • If the patch causes a critical issue, initiate rollback plan (apply snapshot to restore original configuration) • Organize learnings accumulated over installation and validation period
6)	Release Validation Manager	Approve the patch validation • Evaluates information accumulated over validation period • Approves patch for release • If patch is not approved, engage [redacted] if it is a required security patch and/or rollback server to previous configuration
7)	[redacted] Support	Deploys patch to other DEV servers • Deploy based on standard order of deployment to the various DEV servers
8)	[redacted] Support	Create JIRA tickets for deployment to [redacted] and PROD
9)	[redacted] Support	Triage patch for criticality • Use previous risk assessment performed during step 1 • If necessary call a meeting of the Change Advisory Board • Schedule deployment to [redacted] to minimize disruption to [redacted] activities, and based on scope of patch, risks associated with the patch and if patch is critical to operations
10)	[redacted] Support	Deploy patch to [redacted] servers • Use KB article, research and learnings from installation to DEV to streamline process • Deploy based on standard order of deployment to the various [redacted] servers
11)	[redacted] Support	[redacted] validation period • Variable length ○ This may be adjusted based on the complexity of the patch



STEP	WHO IS RESPONSIBLE	WHAT TO DO
		▪ Simple patches may only require a 3 day validation period ▪ Extensive patches may require up to a 30 day validation period ▪ Critical patches may require a shorter period to expedite its release to production • Perform generic tests to evaluate if patch has caused any issues ○ Run basic applications to ensure the patch has not caused any blue screen or crash events • If necessary, perform specific tests to the changes to themselves ○ Necessity of these tests would be identified by the risk assessment performed in step 1 ▪ Minor changes may not require specific tests ▪ Security based changes may not be able to be specifically tested • Allow the patched system to run for the validation period to ensure that any issues are identified • If the patch causes a critical issue in [redacted], escalate to initiate rollback plan • Organize learnings accumulated over installation and validation period • Complete JIRA ticket for [redacted] attaching learnings and any other documentation that supports the installation
12)	[redacted] Support	Schedule deployment to PROD • Schedule deployment to PROD to minimize disruption to PROD activities, and based on scope of patch, risks associated with the patch and if patch is critical to operations

STEP	WHO IS RESPONSIBLE	WHAT TO DO
12)	[redacted] Support	Deploy patch to PROD servers • Use KB article, research and learnings from installation to DEV and [redacted] to streamline process • Deploy based on standard order of deployment to the various PROD servers
13)	[redacted] Support	Complete testing and documentation • If possible, perform safe smoke test in PROD ○ This should not be necessary since after installation to DEV and [redacted] the patch should be thoroughly tested – however given the critical nature of the PROD environment, if there is a safe test that can be performed without impacting PROD • Complete JIRA ticket for PROD attaching learnings and any other documentation that supports the installation