Shreetron India Limited

Revision History

Version	Issue Date	Prepared By	Approved By	Changes
1.0	02.04.2021	Vaneet Soni	A P Panwar	Initial Draft

1. Purpose

The purpose of this policy is to ensure that all AUA owned devices and systems are proactively managed and patched with appropriate security updates.

2. Scope

The scope of the policy applies to all information systems and devices owned by AUA and are used in service delivery.

Shreetron India Limited

3. Patch Management

The Patch Management Lifecycle involves a number of key steps in an area of system management; like acquiring, testing, and installing multiple patches of software or existing application. The administered computer system determines which patch requires to be updated. The respective system admin ensures that patches are installed properly, and all associated procedures are documented as per specific configurations required. This makes the process simple and easy. Please find step by step patch management procedures for different systems below:

1. End-users computers

1. Scan for available patches
2. Download necessary patches from a trusted source (as made available)
3. Schedule deployment
4. Deploy patches

2. IT servers and network devices (or as applicable by SDC policies)

1. Scan for available patches
2. Download necessary patches from a trusted source (as made available)
3. Deploy patches
4. Verify services
5. Notify and report testing results

3. QA, Integration, Development

1. Scan for available patches
2. Download necessary patches from a trusted source (as made available)
3. Deploy patches
4. Verify services
5. Notify and report testing results

4. Pre-production, Demo and staging

1. Scan for available patches
2. Download necessary patches from a trusted source (as made available)
3. Deploy patches
4. Verify services
5. Notify and report testing results

5. Production

1. Patches are approved, deployed, and applied in staging
2. Create a change management request one week before the maintenance date
3. The project team shall communicate any down time to all users before hand
4. Deploy patches
5. Communicate extended out ages to all stakeholders
6. Verify services

6. Emergency security patching: (as applicable by SDC policies)

Note: The Security team will determine the risk and the relevance of the patch, as well as when the system should be patched.

1. Create a change management request before the maintenance date
2. Notify users
3. Deploy patches
4. Verify services
5. Notify and report testing results

-----End of the document-----