CHILLED WEB.COM

Committed to Excellence in Design & Development

Patching Policy

ChilledWeb Limited

Policy Name:	Patching Policy	Policy Ref:	CWPPAP
Date of Last Revision:	20 January 2021	Version No:	2.1

Contents

PATCHING POLICY **1**

ChilledWeb Limited 1

CONTENTS **1**

OVERVIEW **2**

PURPOSE **2**

SCOPE **2**

POLICY **2**

Priority 3

EXCEPTIONS **3**

NON-COMPLIANCE **3**

Overview

The process of patch management has been developed worldwide over many years to ensure the safe implementation of operating system enhancements, bug fixes and security updates.

This policy establishes a standard framework and procedures for the implementation of software patching as well as the identification of vulnerabilities and mitigation of such vulnerabilities.

Purpose

The ChilledWeb infrastructure must be properly maintained with the most up to date patches and updates. This is to minimise system vulnerability and to ensure the confidentiality, integrity and availability of systems and data (including third party data) stored on our systems. Without, strong, protected and robust IT Systems, ChilledWeb faces significant loss of revenue and damage to our reputation.

Scope

This policy applies to all software, servers, desktops, laptop computers, mobile phones and IT appliances owned and operated by ChilledWeb.

Policy

1. All End User devices, Server, Network and Appliance devices must be accurately listed in the Asset Database.
2. Vulnerability scanning will have a minimum frequency of being run monthly. Vulnerability reports will be available within 2 working days of the end of scanning. The Director is responsible for the efficient and effective running of scans to time and for the distribution of reports.
3. Threat analysis will be undertaken by the Director who also has responsibility for ensuring that threats are evaluated in a timely manner.
4. Threat Analysis (Discover and Assess) will determine whether the Patch or Vulnerability Mitigation is progressed to implementation.
5. Patches and Vulnerability Mitigation packages must be obtained from the relevant vendor or other trusted source. Each package must be authenticated, and its integrity verified using the method provided by the source. Credible sources will always provide such an authenticity method such as MD5Sum, Digital Signature, Encrypted Certificate and finally, internal testing. No package must be deployed unless its authenticity has been established.

6. All devices must run the latest supported and patched versions of software prior to being released as a live service.
7. Manual patches and updates will be tested prior to implementation into any live environment. Where this is not possible, the relevant authority to proceed must be obtained from the Director.
8. A back-out or recovery plan that allows safe restoration to pre-patch state must be devised prior to any patch or update.
9. An audit must be carried out to ensure that patches and updates have been applied as required or notified by vendors and are functioning as expected.

Priority

Where practically possible all patches should be implemented within 10 working days of being made aware of a security vulnerability. Further, ChilledWeb will employ the following sources of information to ascertain the priority for implementation of patches or rectification of vulnerabilities:

- Vendor Severity Rating
- CVSS Score

Exceptions

Any exception to the policy must be approved by the Directors in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.