totara

SUPPORT AND MAINTENANCE BEST PRACTICE

Software systems continually evolve. Change comes from the introduction of new features, bug fixes, addressing security issues, and different configurations to meet changing business requirements. To get the best results from your software investment requires good quality support and maintenance.

In this guidance paper we will answer the following common questions:

- *What do we mean by support and maintenance?*
- *What is software patching?*
- *What are the distinctions between Totara product support and the direct support services you receive from the Totara Partner you have selected?*

THE IMPORTANCE OF A TOTARA SUBSCRIPTION

MAINTENANCE RELEASES

Building networked software is one of the most complex tasks humans perform, so it's unsurprising that bugs slip through. It is simply not possible to build an application that is 100% free of bugs, now and into the future. Software developers deliver software products with defined functionality. However, our continual desire for more functionality and features means that the average number of lines of code in modern systems is increasing – and the more complex and multi-functional an application is, the more certain it is that it can be used in unintended ways.

In exchange for a low cost annual subscription, Totara provides monthly maintenance releases. A "patch" is a set of changes designed to update, fix, or improve the software. Maintenance releases include bug fixes and minor feature improvements designed to enhance the application's usability and performance

FEATURE PATCHES

Feature patching software is a little like car maintenance. While your car might still run without maintenance, the longer you go on without them, the more likely you will encounter problems, some with potentially very serious consequences.

SECURITY RELEASES

As Internet connectivity has become ubiquitous, our approaches to security have had to adapt to address data leakages or breaches. Your Learning Management System (LMS) is likely to be part of a broader information ecosystem - containing digital assets: documents, courses, discussions and more, but also a lot of personal information connected to the internet and within other integrated software. A modern Information Security strategy should include policies for rapid response updating of all the software installed on any system.

A security "exploit" is typically a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behaviour in the software application. It can mean anything from obtaining control of a system, extracting data, enabling an escalation in permissions, a data loss or a denial-of-service (DoS) attack that renders a website inoperable.

Security patching is like other forms of security. If you realise that the lock on your front door is broken, you would want to fix it urgently before someone uninvited misuses the opportunity. The same goes for patching – you must patch the exploit before anyone with ill-intent opens the door.

NEW RELEASES

As part of your annual subscription, Totara continually innovates and develops the core features and functionality of its products which are made available through regular product releases.

Customers also have direct access to learning resources, documentation and networking opportunities with other Totara users in the Totara Community.

SECURITY VERSUS FEATURE PATCHING

- **Software patching means applying available updates including both security and feature patches.**
- **Feature patching fixes and improves the software you use.**
- **Security patching fixes security vulnerabilities and is an essential part of regular cyber hygiene.**

WHY IS IT IMPORTANT TO HAVE A SUPPORT AND MAINTENANCE AGREEMENT WITH YOUR TOTARA PARTNER?

Your Totara Partner is responsible for designing, configuring, implementing and supporting your Totara solution. It is your Partner that will apply the patches, implement version upgrades, and ensure that your platform is secure. A Totara Partner will usually manage the physical environment where the IT infrastructure is located.

Patching, just like all things in security, concerns managing risk. All software is going to be vulnerable at certain times. However, your best chance of avoiding a major security crisis and preventing your systems from being severely compromised is to install new updates as soon as possible. Minimising the time between new Totara software releases and applying these to your LMS is crucial to reducing exposure to potential threats. You increase business risk unnecessarily by leaving your systems unpatched.

Without the efficient and effective delivery of support services from your Totara Partner, you are not receiving the full benefit of your Totara subscription. Routine patching is a critical part of every IT security plan.

RECOMMENDATIONS

1 *Check your Totara release version – you can find out how to do that **here**.*

2 *Join the **Totara Community** and subscribe to receive notifications of new releases and patches – it's free and contains comprehensive learning resources as well as the opportunity to connect with other Totara subscribers.*

3 *Contact your Totara Partner to discuss your software maintenance and security requirements.*

4 *Review your information security policies carefully and ensure they provide the right balance of protection and risk management for your business.*