# 7 MYTHS ABOUT SOFTWARE ESCROW DEBUNKED

IRON MOUNTAIN®

Software source code is the backbone of your business-critical applications. Yet we often encounter myths about software escrow — usually from people who are unclear about how it works.

A software escrow agreement protects the developer's intellectual property, while at the same time keeping a copy safe for the buyer, or licensee. An escrow agent, such as Iron Mountain, is a trusted, neutral third party that safely stores this source code until needed. If the developer ever goes bankrupt or can no longer support the software, the licensee requests a release of the source code from the escrow account which gives them options to keep their business up and running.

Here are seven myths about software escrow and why they are false:

MYTH # 1
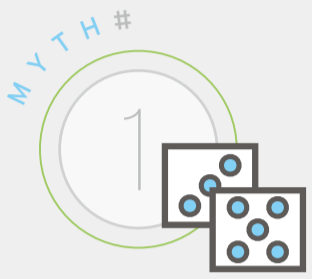
Escrowing my software isn't a good bet.

○ On the contrary, software escrow is like insurance and provides a backup file for your source code.

○ Source code needs protection in case of mergers or acquisitions, potential vendor bankruptcy, or insolvency. You'll be glad you have it when you need it.

MYTH # 2
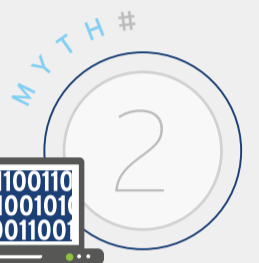
My escrowed source code is likely to be incomplete or out of date.

○ That's why we offer escrow verification services, to validate your software is complete and up to date.

○ With four levels of verification — from basic to a full usability test — we help ensure all the pieces of your escrow deposit will work together when needed.

MYTH # 3

If I get my source code out of escrow, I don't have the expertise to use it.

○ Craft your escrow agreement with the necessary legal use rights for the intellectual property and its intended use.

○ Access to source code and other proprietary information lets you maintain your business-critical application yourself or hire an outside programmer.

MYTH # 4

Delays and legal battles often accompany a release.

○ The vast majority of escrow releases happen smoothly, without the need for dispute processes or litigation.

○ Software escrow gives you the ability to *avoid* the cost and delays of litigating against trustees, other creditors, or anyone claiming the licensee doesn't have a right to the source code.

MYTH # 5

Escrow is too expensive.

○ In reality, *not* having a software escrow agreement is far more expensive; insurmountable costs could build up from lack of third-party protection.

○ Our customers tell us that "escrow is very cheap insurance" and that "the cost to protect these assets is trivial."

MYTH # 6
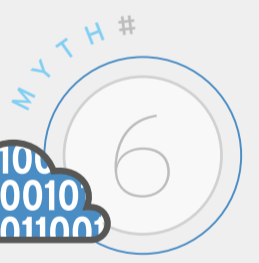
As companies rely on Software as a Service (SaaS), source code escrow is unnecessary.

○ With SaaS, both your software application *and* your data are in the cloud.

○ Iron Mountain has developed a disaster recovery and risk management solution for both SaaS providers and subscribers with its SaaSProtect® Solution for Business Continuity.

MYTH # 7
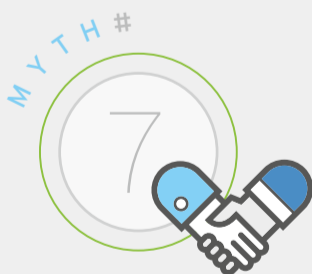
Your escrow vendor doesn't matter; it's a commodity business.

○ You need to trust the company that safeguards your valuable technology assets. Iron Mountain is the most experienced, most secure escrow agent in the business.

○ Get it right. Every time. With its global footprint and ultra-secure facilities, 90 percent of Fortune 500 companies trust Iron Mountain for software escrow protection.