ITGlue
A Kaseya COMPANY

Best Practices for **IT Asset Management**

Table of Contents

Introduction

Accounting for all the hardware assets in an organization is no easy task, especially when you add the complexity of keeping track of these assets' updates, maintenance and future deprecation into the mix. The task gets even more challenging when you realize that "assets" aren't just computers and servers. Everything that IT needs to know is an asset. This includes knowledge, passwords, user information and software assets, in addition to the more traditional view of IT assets consisting primarily of hardware.

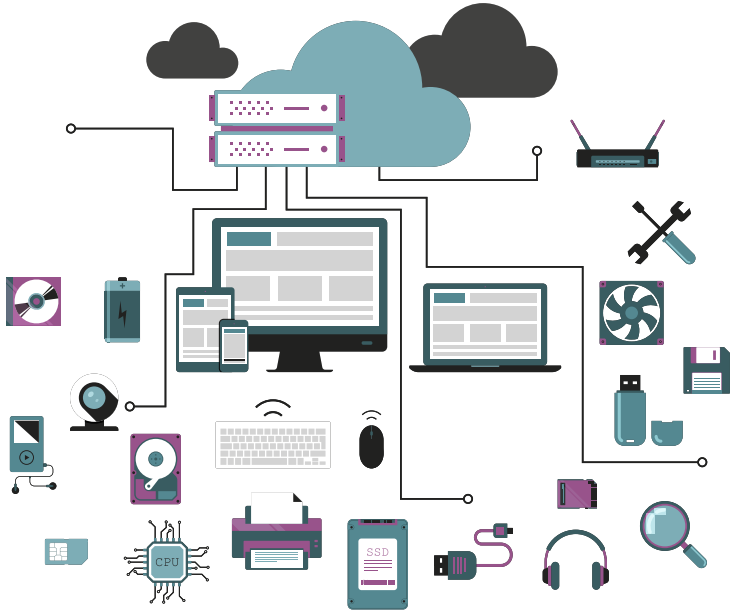
When you think about best practices for IT asset management, a vital filter to use is to think about the objectives that IT has as far as asset management is concerned. Your best practices will be guided by the specific outcomes you're looking to bring about. In that sense, IT Glue has been helping hundreds of thousands of IT pros manage their hardware and software assets. As a solution purpose-built to meet the needs of IT, our documentation platform helps you easily manage your IT assets.

If you're like most IT managers, your outcomes fall into one of these categories:

1. *Security*
2. *Asset lifecycle management*
3. *Audit and compliance*
4. *Helpdesk*

While some organizations might have other priorities, such as budget, operational efficiency, etc., for most organizations, these categories are among the most important priorities for the IT department.

Following these IT asset management best practices will move you toward your specific goals in each of these domains.



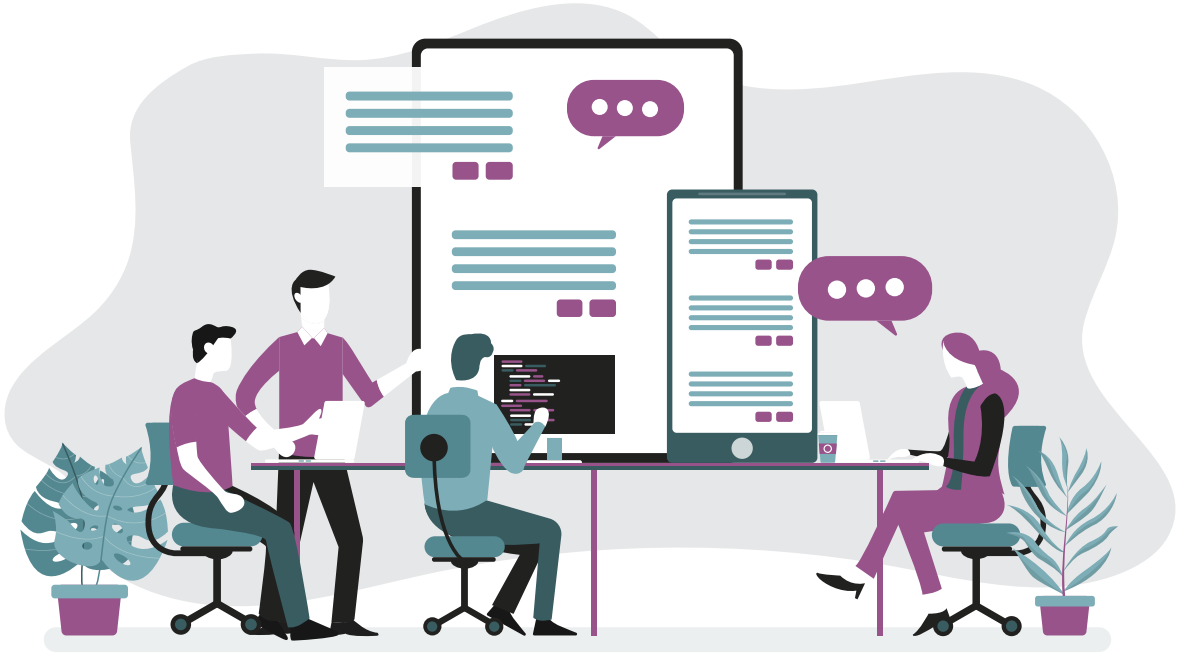
Document as Much as Possible

While documenting everything in your IT environment isn't a bad idea, sometimes you may spend too much energy on your documentation efforts compared to the value you receive from it. However, make no mistake, you are always better off documenting more.

The reason is simple: the knowledge you document is the knowledge you get to keep.

Anything that's not written down, or written down somewhere where you'll never find it, could be easily lost forever.

Log your hardware assets, such as workstations, servers, printers, tablets and laptops. Document their serial numbers, current and past users, operating systems, vendor info, SOPs for device-specific issues and anything else that can come in handy later. Ticket history for a machine is a big one for your helpdesk.



Document **Software Assets**

What software programs do you have on your hardware devices? Which users have software licenses? Are you paying for licenses that you aren't using?

With clear documentation on different software in your organization, you can avoid overpaying for licenses you don't need. Moreover, you get visibility into who uses a software program on a particular machine, which comes in handy when identifying vulnerabilities.

You can witness similar benefits with operating systems as well. Older versions of operating systems are vulnerable to attacks, but you can keep track of them easily with proper documentation.

Document **Vendor Risk Profiles**

Vendor management, as a whole, is not an IT function. It typically falls to a procurement or accounts payable team. However, no IT professional in their right mind would trust procurement or accounts payable to manage cybersecurity.

As such, IT teams need to undertake risk assessments for their companies' vendors. This includes risk level, business impact, key contacts, internal champion, etc.

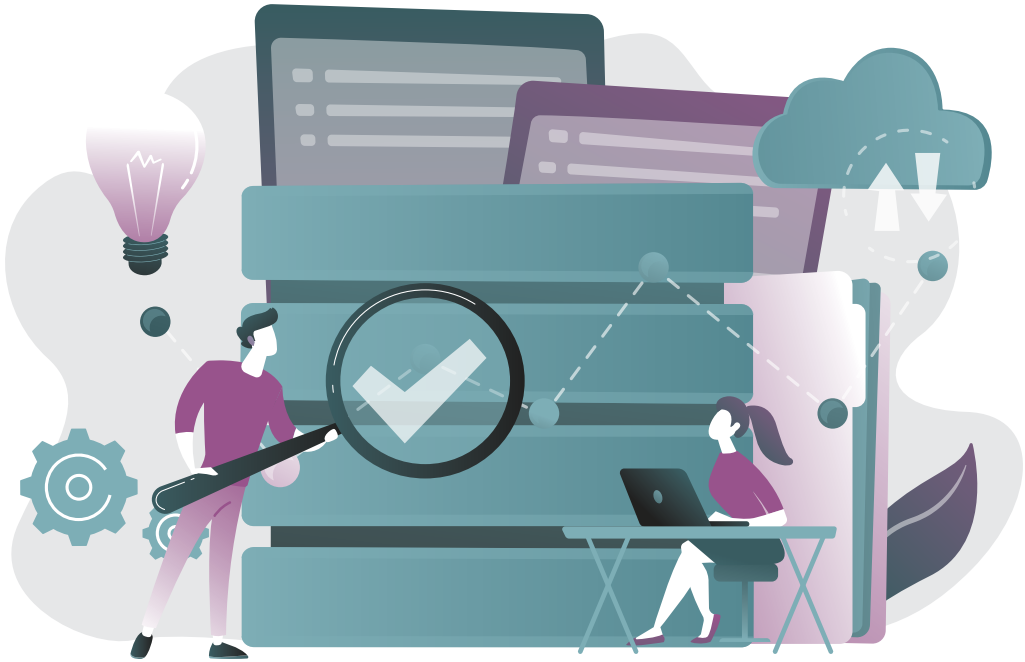
The information then needs to be documented where it can be located quickly and easily. You may not need this information until you witness a security breach. However, when you do, you need the documented information to bounce back from the breach.

Match Users with the Assets they Use

You can keep track of employees through user documentation, which has many benefits. Imagine a ticket coming through, and you have no record of that user existing, much less what equipment they use.

User documentation helps you match users and their hardware to recover devices when they leave the organization. Speaking of departures, user information is essential to create at-risk password reports that will help you eliminate vulnerabilities immediately when someone leaves your or your client's organization.

Pulling user information from Active Directory and Azure AD makes for easier onboarding, servicing and offboarding while keeping manual work to a minimum.



Don’t Forget about **BYOD**

Do you know what’s connected to your network? Or your clients’ networks?

It isn’t easy when everybody has a phone, a watch and, in some companies, a BYOD policy. However, as you can imagine, it’s hard to secure an environment where you have only limited visibility. IT may not have much responsibility for BYOD devices but security issues mean IT’s responsibility isn’t zero either.

Asset discovery, therefore, is a part of asset management, especially when combined with documentation. Add in a network diagram that updates daily or on demand, and you will have the sort of visibility that allows you to solve problems and eliminate vulnerabilities more easily.

Secure, Mature and Integrated Documentation

Make documentation easy

Create and store KB, checklists and SOP articles effortlessly, embed rich network diagrams or import Word documents so your team is empowered to train and help themselves.

Secure your critical information

Sleep better with next-level password management featuring access control, host-proof hosting, at-risk password report and audit trail.

See the complete picture

Link related items together, so that all the information you need is at your fingertips. Rapidly define and understand relationships between various elements of your documentation.

Build a documentation culture

Edit and collaborate directly within the platform. Automatically save and sync to ensure your documents are always up to date for all team members.

Trusted by More than 13,000 Partners in 70+ Countries

Safeguard Your IT Operations with Secure Documentation

Request a Demo

When it comes to data security, IT Glue is second to none. We have achieved a SOC 2 Type-2 attestation, a set of data security and service controls that can only be maintained through ongoing, company-wide commitment.