eBook

jumpcloud™

The IT Manager's Guide to Data Compliance Hygiene

Ace Your Audits with Less Stress

Introduction

Mindset — it's often the difference between a smooth journey (with a few bumps along the way) or a stressful sprint to the finish line (with many twists and turns).

This applies to everything from menial tasks to large-scale initiatives. Mindset shapes not only how you think about things, but how you go about accomplishing them.

As an IT manager, your mindset around why compliance matters informs your daily thoughts, feelings, and actions that will make or break future audits. Translation: you can view audit preparation in one of two ways:

1. A hassle to deal with before moving onto "what really matters" or
2. An incentive to practice strong security hygiene that keeps everyone safe.

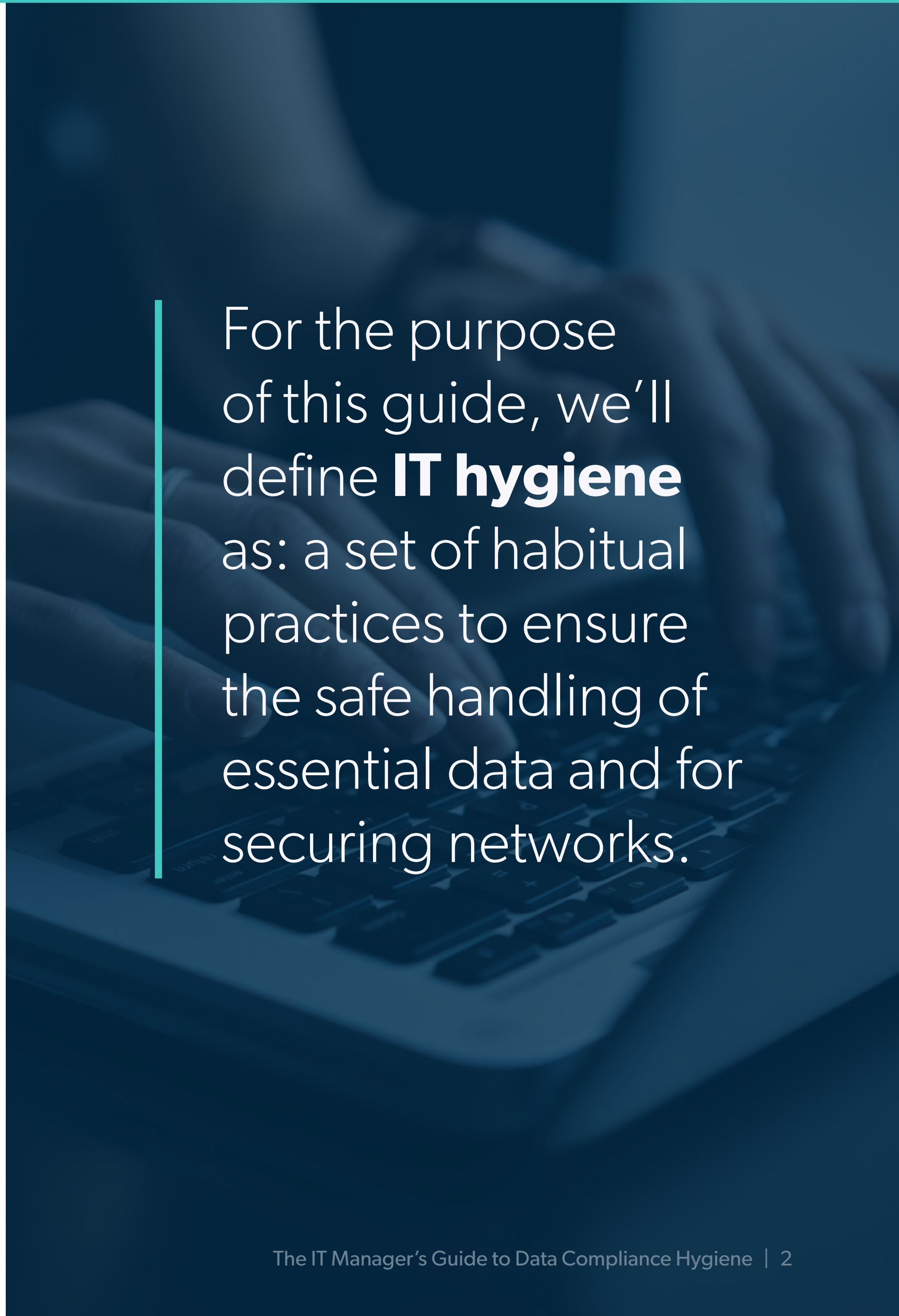
If you have downloaded this guide, you are probably spearheading the IT audit process for a startup or small-to-medium-sized enterprise (SME) for the first time. Or maybe you're an old pro looking to see what else you could be doing. Either way, we invite you to hit "pause," take a deep breath, and exhale.

You don't have to be perfect to pass your audit, and we can pretty much guarantee there is no such thing as 100% compliance at all times. This is why we recommend prioritizing the right actions throughout the year to ensure optimal results rather than just focusing on the operations of the audit itself. And that means increasing emphasis on the things you know matter, but may avoid prioritizing; in other words, **IT hygiene**.

We don't need to quote the latest cybersecurity breach statistics for agreement that security hygiene is about more than avoiding fines. But you may find it surprising that cyber attacks on SMEs have increased by approximately 400% over the past year. Consistent security hygiene is essential to reducing the likelihood of your brand name becoming the next newspaper headline.

This guide will review several IT hygiene practices worth automating year-round to facilitate smoother audit processes. It will also explore the relationship between faster prep times and consolidated toolkits/systems.

After reading, you can expect a better understanding of how (and why) to conduct internal audits, which preparatory action steps save time, and what to expect during official audits.



> For the purpose of this guide, we'll define **IT hygiene** as: a set of habitual practices to ensure the safe handling of essential data and for securing networks.

The Benefits of IT Hygiene

At first glance, it may not seem like IT hygiene is related to audit preparation. The latter involves gathering lists of data, securing an auditor, providing documentation, explaining control failures, and making remediation plans within a brief period of time.

The former refers to following through on best practices 24/7/365. But much like a runner shouldn't begin training a week before a marathon, an IT manager shouldn't start practicing IT hygiene right before their next audit! In addition to facilitating smoother compliance experiences, prioritizing IT hygiene provides the following benefits:

1 Identifies Inefficient Processes

Inefficient processes slow down operations, creating unnecessary bottlenecks. Data regulations mandate IT managers to discover opportunities for more efficient processes, procedures, and tools.

For example, imagine a pizza delivery firm that receives customer orders from one software, customer reviews from another, and order statistics from yet another.

An IT manager that prioritizes IT hygiene would seek opportunities to eliminate redundancies and unify data collection for more accurate reporting. Typically, this would involve switching to a software service that provides all these functions in its offerings.

This unified data collection makes it less likely that there will be a breach by reducing the overall attack surface and focusing security efforts, and makes data audits easier. It also makes the marketing department, which looks at the data for business reasons, more efficient because they have to do less copying and pasting from one application to the next when reviewing their marketing strategies.

Alternatively, managers who practice lackluster IT hygiene often find themselves switching between many misconfigured applications, which often increases vulnerabilities. In addition, purchasing multiple single-point solutions can be hard on the budget.

2 Reduces Security Vulnerabilities

Minimizing security vulnerabilities is the whole point of compliance, but it's worth emphasizing. Cybersecurity breach incidents scaled new heights in 2021.

According to the Identity Theft Resource Center (ITRC), data breaches increased more than 68 percent from 2020 to 2021. To make matters worse, an increasing amount of data incidents involve sensitive information, such as Social Security numbers.

The solution, of course, is data hygiene. According to the Microsoft Digital Defense Report, basic security hygiene still protects 98% of attacks. We'll call out the most crucial security hygiene practices you can take further down in the guide.

⚠ **68%**

Data breaches increased more than 68% from 2020-2021

The Benefits of IT Hygiene

3 Helps Avoid Penalties or Legal Trouble

Failing to follow through with mandatory IT hygiene regulations can cause serious trouble. According to The True Cost of Compliance with Data Protection Regulations study by the Ponemon Institute, non-compliance with leading cybersecurity standards costs more than twice as much as maintaining compliance.

Following data-compliant practices isn't always "easy peasy." But it's far more convenient and less expensive than paying legal fees, fines, or even worse penalties.

Of course, it isn't only cookie violations and personal information mishandling that can get a company into legal trouble. Failing to take adequate steps to prevent security breaches can result in millions in fines. British Airways knows a lot about that one.

> "...non-compliance with leading cybersecurity standards costs more than twice as much as maintaining compliance."

4 Minimizes Costs to Stay Compliant

Staying compliant is expensive; your organization may spend anywhere from a few thousand to hundreds of thousands of dollars on direct and indirect costs annually.

Totals vary based on the amount of employees, regulatory requirements, and data under your care. If your business processes credit card transactions, you're likely following the **Payment Card Industry Data Security Standard** (PCI DSS).

Gary Glover, vice president of assessments at SecurityMetrics, says annual compliance costs for PCI DSS range from $10K to $70K depending on the number of transactions processed. This includes expenses associated with updating policies, replacing old technologies, training employees, penetration testing, and on-site audits.

Alternatively, a typical SOC2 audit ranges from $25K to $39K. Failing to practice IT hygiene throughout the year means you're more likely to accrue additional expenses to "get it together" in time for your audit. Common costs accrued include exorbitant consultant fees, suspended business partnerships (due to failing grades), and astronomical regulatory fines.

5 Secures Business Partnerships

Have you ever heard the phrase "excellent practices breed excellent partnerships?" Probably not because we just made it up. But it's true — being IT-compliant silently communicates that your organization is up-to-date with the latest trends, technologies, and practices.

In other words, good cybersecurity habits forge a bond of trust between companies and prospective business partners. A higher level of trust translates to more referrals, improved vendor relationships, and more potential customers.

Highly regulated industries like healthcare, government, and banking are especially vulnerable to losing partnerships due to non-compliance. In addition, most enterprise-level companies require the minimum of a SOC2 and ISO27001 before they will even consider doing business with your organization. And, if that weren't enough, you will have a tough time securing cyber insurance which also impacts who will and won't work with you!

For the remainder of this guide, we'll connect the dots between the things you must do to satisfy data compliance audits and the IT hygiene best practices that support them.

Remember: audits may seem burdensome, but they provide an essential foundation for organizations to implement proven cybersecurity measures that keep precious data safe — standards that contain both proven and cutting-edge methods to ensure security.

7 IT Hygiene Best Practices to Follow

Whether you're a startup or an enterprise-level company, the best practices for achieving compliance are the same. The only difference is the amount of rigor required.

Audits happen regularly, and regulations change frequently. Translation: you must consistently carve out time to review and improve your existing security practices.

You can think of IT hygiene as your team's standard operating procedures that work harmoniously as part of your overall compliance strategy. A compliance strategy is a set of internal policies and procedures that will help your organization stay compliant.

Once your compliance strategy is complete, it's essential to assign team members responsible for implementing the various parts. Remember, IT compliance is a team effort that involves the contribution of many individuals outside of the IT department. Below are seven best practices worth following:

1 Monitor Your Unique Regulatory Requirements

Before setting out to improve your compliance posture, figure out which standards are mandatory and which ones aren't. Pay attention to obligatory and non-obligatory regulations, as both provide an organization with the benefits we discussed above.

For example, while HIPAA compliance is non-negotiable for health organizations, ISO 27001 implementation is voluntary. Nonetheless, according to the ISO Survey 2018, the demand for ISO certification grows by the year. In addition, you must also determine where the requirements of a specific regulation apply to your organization.

If you're uncertain about which audits you need to pass, consult with someone who has already "been there, done that" in your industry, trade, or supply chain. An experienced auditor will also know which standards and regulations your type of organization must follow.

Smaller SMEs won't have cybersecurity staff or even access to dedicated lawyers, at least not those practicing cyber. I'd suggest that you consult with your industry, trade, supply chain, and/or regional peers or simply ask your auditors on the regulations you might be subject to.

You can also analyze the data your organization handles to figure out which requirements it's subject to. *Usually*, IT compliance focuses on three types of data:

- **Personally identifiable information:** Any information that relates to an identifiable person: name, home address, date and place of birth, biometric records.
- **Financial data:** Credit card numbers, data on income and expenses, financial reports of an individual, organization, or any other entity.
- **Protected health information:** Results of medical examinations, information about health care plans, and any medical records linkable to a specific person.

In addition, pay attention to the privacy standards and remember that laws such as the GDPR and the 2019 Online Privacy Act contain web/cookie data regulations. Hence, if your business handles customer cookies, you'll be better off obtaining permission before retrieving necessary cookies and letting your clients' have full disclosure on how their data is used.

7 IT Hygiene Best Practices to Follow

2 Appoint a Data Protection Leader

Large enterprises often hire internal data protection officers (DPOs) to oversee data protection measures and ensure the department is responsible for meeting them. If you're a startup or SME, you probably don't have the budget or bandwidth for a full-time DPO yet.

But that doesn't mean you can't recruit an internal data protection leader to drive your compliance efforts on the side. Both the GDPR and PCI DSS require an organization to designate an employee who is responsible for compliance. Your compliance champion should make an effort to:

- **Increase knowledge of cybersecurity legislation.** Having an expert on the team translates into being able to develop data-compliant policies and procedures for data handling. It also means that staff can be better and continuously trained on data protection best practices. In addition, the project driver can act as a resource for employees who have questions about the organization's data protection practices.
- **Regularly monitor IT compliance statuses.** While other staff focus on their roles between audits, your data protection leader can perform data protection impact assessments (DPIA), track changes in regulations, and check whether current security controls are in tune with current data-protectionist standards.
- **Quickly respond to breaches.** In the event of a security breach, the data protection leader should have a plan in place for doing damage control, notifying affected parties, and reporting the breach to authorities and clients. Fast response times mitigate consequences and reduce fines.

It's worth mentioning that the conflict of interest requirement doesn't mean a DPO can't hold other roles within the company. Still, such a role must not be one that can involve making decisions that might mean data protection taking the back seat while business considerations ride shotgun.

However useful a DPO or data protection leader may be, it's important to remember that a single person can't make an organization compliant. This person will require support from company management and the authority to improve existing security controls and policies, reconfigure existing software, and deploy new software.

> It's important to remember that a single person can't make an organization compliant.

3 Conduct a Risk Assessment and a Self Audit

A risk assessment identifies and analyzes security risks your organization might face.

During a risk assessment, it's important to identify:

- cybersecurity risks and threats to your organization
- assets that are critical to your organization and are subject to compliance regulations
- your current level of protection, as well as the weak and strong points of your defenses

A self-audit has a lot in common with a risk assessment: it's an evaluation of implemented security controls. But unlike a risk assessment, a self-audit helps you evaluate your current compliance level and identify gaps in data protection. It also prepares your employees for a real IT audit.

Most startups begin conducting quarterly self-audits no sooner than their board of directors tell them to "get on the ball." No matter the size of the organization, most internal audits include the same basic steps as shown below.

The one drawback to self-audits is their high cost, both in terms of money and time. However, discovering gaps in cybersecurity during an actual audit has an even higher cost: failing the audit and starting over!

Below are the three basic steps of conducting an audit:

- **Gather lists of assets:** Assets refers to all relevant IT-related stuff (i.e., devices, devices with full-disk encryption, users etc.). This typically comes from a master IT asset management platform. Pro Tip: Prioritize maintaining a central source of truth.
- **Identify the gaps:** Upon comparing your lists, you may be surprised to find several assets listed within the master database are unaccounted for in the lists coming from your IT tools. Answer questions like: *Where are these items? Why aren't they following protocol? Do we have devices out for repair?*
- **Fix the outliers:** Once you have identified non-compliant assets, you're ready to make a remediation plan. Auditors are real people who understand reasonable exceptions. Taking action to demonstrate reduced risk however you can and explaining the reasons behind any outliers with screenshots is satisfactory.

Unfortunately, you're never going to have everything you need in one place for compliance. There are simply too many factors you must take into account. But you can still save time and energy by consolidating tooling wherever possible.

7 IT Hygiene Best Practices to Follow

4 Fix Missing Controls

OK, you have finished conducting your risk assessment and self-audit. You now know what policies, practices, and technical controls to implement for a passing grade. At this point, it's time to take action and fix any oversights you found.

The good news? Requirements of common regulations, standards, and laws overlap in many areas. It's likely that some of the elements you fix today will make things easier for your team in the future. For example, most data mandates require using tools for identity management, access control, user activity monitoring, and breach notification.

While it's beyond the scope of this guide to delve into comprehensive controls, below are **nine of them** worth following year-round. You will find these general protocols as requirements in many different types of regulations.

There are many other aspects of data compliance hygiene that we can't cover in the scope of this guide. But by following best practices in online security, physical security, and incident response, you've got no need to be jittery about that upcoming compliance audit.

Unifying your stack with the JumpCloud Directory platform can also relieve the stress that comes with tool sprawl. JumpCloud combines Linux, Windows, Mac, and iOS devices behind one pane of glass for convenient heterogeneous device management. In addition, JumpCloud also handles identity and access management (IAM), and Zero Trust security elements like single sign-on (SSO) or multi-factor authentication (MFA).

Here are some of the controls we recommend prioritizing always:

Full-Disk Encryption:

Full-disk encryption (FDE) is a simple way to ensure data remains inaccessible without an authentication key should a device become lost or stolen. Every organization should prioritize FDE regardless of regulatory requirements.

Anti-Virus Software:

Like the battle between good and evil, cybersecurity is a classic depiction of infinite warfare. New security threats always emerge, and so must the measures to combat them. This means admins should run the latest versions of antivirus software on company endpoints at all times.

Breach Notification:

Notifying affected individuals and regulators of a data breach helps mitigate damages caused by unauthorized access or disclosure of personal information. In addition, breach notification gives individuals the opportunity to beef up protection from future identity theft and scams.

Identity Access Management:

Use Identity and access management (IAM) solutions to control who can access, view or modify sensitive information. IAM measures aid in compliance with data privacy regulations, such as the General Data Protection Regulation (GDPR). Platforms like JumpCloud also automate audit trails so admins can easily prove policy adherence.

MDM Patch Management:

The global shift toward remote work and the adoption of Bring Your Own Device (BYOD) policies necessitate continual patch updates. Manual patching reduces IT worker productivity and increases the likelihood of overlooking outlier devices. Automated patch management saves time and increases accuracy.

Multi-Factor Authentication (MFA):

MFA is one of the easiest controls to implement that can yield extremely high dividends. Enforcement can range from requiring biometric data in addition to a password, to asking for the user's maiden name and considering what role the user holds in the organization.

Naming Conventions:

Savvy admins adopt naming conventions because it helps them find requested data lightyears faster. It also facilitates carrying over information when installing other management solutions. Establishing distinguishable names for device classes and individual devices is simply good hygiene. Don't name every device "Company XYZ's Macbook!"

Password Security:

Strong password security requires the implementation of several policies. Password complexity, anti-keylogging measures, and anti-phishing measures are all essential components of good data hygiene.

Data Backups:

Backing up data is like stashing cash for a rainy day. No one wants a system failure or data breach, but it's essential to prepare for the unexpected. Store encrypted data backups in a secure location unaccessible to unauthorized individuals.

7 IT Hygiene Best Practices to Follow

5 Setup IT Audit Trails

Maintaining a clear audit trail is essential to acing any audit. An IT audit trail is a set of records that depict any activities with sensitive data, databases, applications, or parts of your infrastructure. It allows IT compliance auditors to examine how your employees handle sensitive resources and assess that you have been doing what you said you would.

Audit trails can be manual or electronic so long as they act as documentation and proof of compliance. Security policies and processes (like data retention and document control) significantly manage audit trails.

Digital audit trails offer a number of advantages over their analog counterparts. For one, they are much harder to manipulate or tamper with. This can be valuable in situations where fraud or misuse is suspected. Additionally, digital audit trails are usually more accurate and up-to-date than analog records. This can save time and money that would otherwise be wasted on trying to track down missing or outdated information.

Finally, digital audit trails provide a more complete picture of your compliance posture at any given moment. This is because they are more readily accessible in real time. Logging an audit trail is also useful for security monitoring and incident investigation. You can track any action inside your protected environment using generated logs, identify security incidents, and assess threat sources.

> Maintaining a clear audit trail is essential to acing any audit.

6 Automate Compliance-Related Activities

For now, there isn't a workaround for the manual effort necessary for some compliance audit activities. Reviewing policies, investigating security incidents, and cooperating with certification bodies takes time.

But thankfully, the vast majority of activities that go into making an organization data compliant can (and should) be automated. Automation tools help reduce compliance overhead, save time preparing for the audit, minimize the risk of human errors, and improve the overall efficiency of your IT operations.

Automation is especially helpful for large organizations that have to pass several IT compliance audits annually. It ensures your team performs tasks in the same manner each time.

While it's not possible to automate everything, prioritize automating what you can. The time it takes to do the upfront work is nothing compared to the long-term dividends of finding exactly what you need when you need it later. And, of course, you will sleep better at night knowing your organization's data is safe and sound.

> JumpCloud's Directory Platform provides a suite of tools that can help you automate many of the tasks associated with data compliance. With JumpCloud, you can manage passwords, users, events, automate security patches, and lots more all from one dashboard.

Several different ways to automate compliance-related activities exist, including:

Password Management: Password management tools can help to create and enforce complex passwords and keep them up-to-date. This can help to prevent hackers from gaining access to your systems and data.

User Management: Use automation tools to carry out employee onboarding and offboarding processes for any company. Not only do they help to ensure compliance with data regulations, but they also protect both the employee and the company's data. User management technologies can be used during onboarding to automatically identify an employee and grant them the necessary level of access to specific information. In the event that the employee's appointment gets terminated or their user profile becomes vulnerable, the system can easily revoke or suspend their access pending a review.

Event Reporting: Event reporting is the process of documenting and analyzing events that occur within a company's network. This can include everything from malware detections to user logins. Event reporting helps to identify trends and potential issues, and can be used to isolate and investigate incidents. Automated event reporting tools can help streamline the process by collecting data from multiple sources and generating reports automatically. This saves time and resources, and can also help to ensure that reports are accurate and up-to-date. In addition, automated event reporting can help to identify patterns that might otherwise be missed.

7 Raise Security Awareness

One of the most important steps in maintaining data compliance is ensuring that all employees who work with sensitive data understand their responsibilities and use safe practices. This includes not just IT staff but also employees in other departments who may have access to sensitive information.

Education is key to ensuring employees understand the importance of data security and compliance, no matter how it may be inconvenient. They must be aware of the risks associated with mishandling data and the consequences of violating any regulations.

In addition, employees need to know how to protect themselves and the company from potential security threats. This includes knowing how to create strong passwords, how to identify phishing emails, and how to respond to a data breach.

Regular reminders and updates are essential in helping employees stay safe and compliant. It's also important to keep up with regulations and best practices changes so that employees are always up-to-date on the latest security threats.

Ace Your Next Audit with JumpCloud

Any IT admin that wants a smooth audit experience must lay a proper foundation with proven security hygiene measures. Solid foundations yield strong security postures that inspire trust.

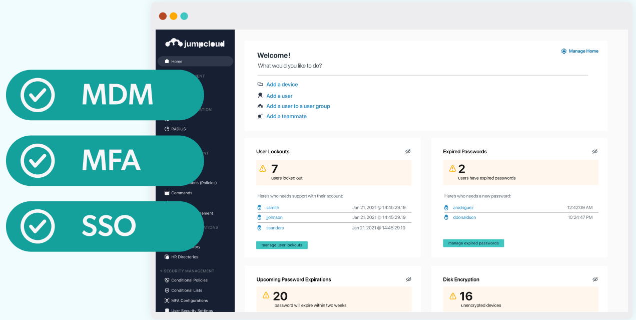
Data compliance hygiene is a valuable asset for any organization when done correctly. A big help in achieving data-compliant status is to employ solutions like the JumpCloud Directory Platform that support data hygienic practices with tool consolidation.

The JumpCloud Directory Platform provides:

- Advanced reporting that gives insight into data access and compliance-related activities
- MFA protocols for logging in to an organization's IT resources
- Effective password policies that comply with best practices
- Device management of all devices authorized to access company resources
- Automation of user onboarding and offboarding

Are you feeling uncertain about how to implement the compliance controls you need? Are you feeling overwhelmed with tool sprawl? If so, the JumpCloud Directory Platform can streamline your security stack and provide real-time audit trails.

Our Professional Services Team can help implement many of the cybersecurity best practices you need to feel prepared come audit time. Hand-off a chunk of your workload to world-class engineers with high-caliber project management skills for a small fee.



Welcome!
What would you like to do?

Add a device
Add a user
Add a user to a user group
Add a teammate

User Lockouts
7 users locked out
Here's who needs support with their account:

ssmith	Jan 21, 2021 @ 14:45:29.19
jjohnson	Jan 21, 2021 @ 14:45:29.19
ssanders	Jan 21, 2021 @ 14:45:29.19

manage user lockouts

Expired Passwords
2 users have expired passwords
Here's who needs a new password:

arodriguez	12:42:09 AM
ddonaldson	10:24:47 PM

manage expired passwords

Upcoming Password Expirations
20 password will expire within two weeks

Disk Encryption
16 unencrypted devices

JumpCloud® helps IT teams **Make Work Happen**® by centralizing management of user identities and devices, enabling small and medium-sized enterprises to adopt Zero Trust security models. JumpCloud has a global user base of more than 180,000 organizations, with more than 5,000 paying customers including Cars.com, GoFundMe, Grab, ClassPass, Uplight, Beyond Finance, and Foursquare. JumpCloud has raised over $400M from world-class investors including Sapphire Ventures, General Atlantic, Sands Capital, Atlassian, and CrowdStrike.

For more information on JumpCloud and how organizations everywhere are providing Secure, Frictionless Access™ to all their IT resources, visit jumpcloud.com/why.

jumpcloud™

Try JumpCloud Free →