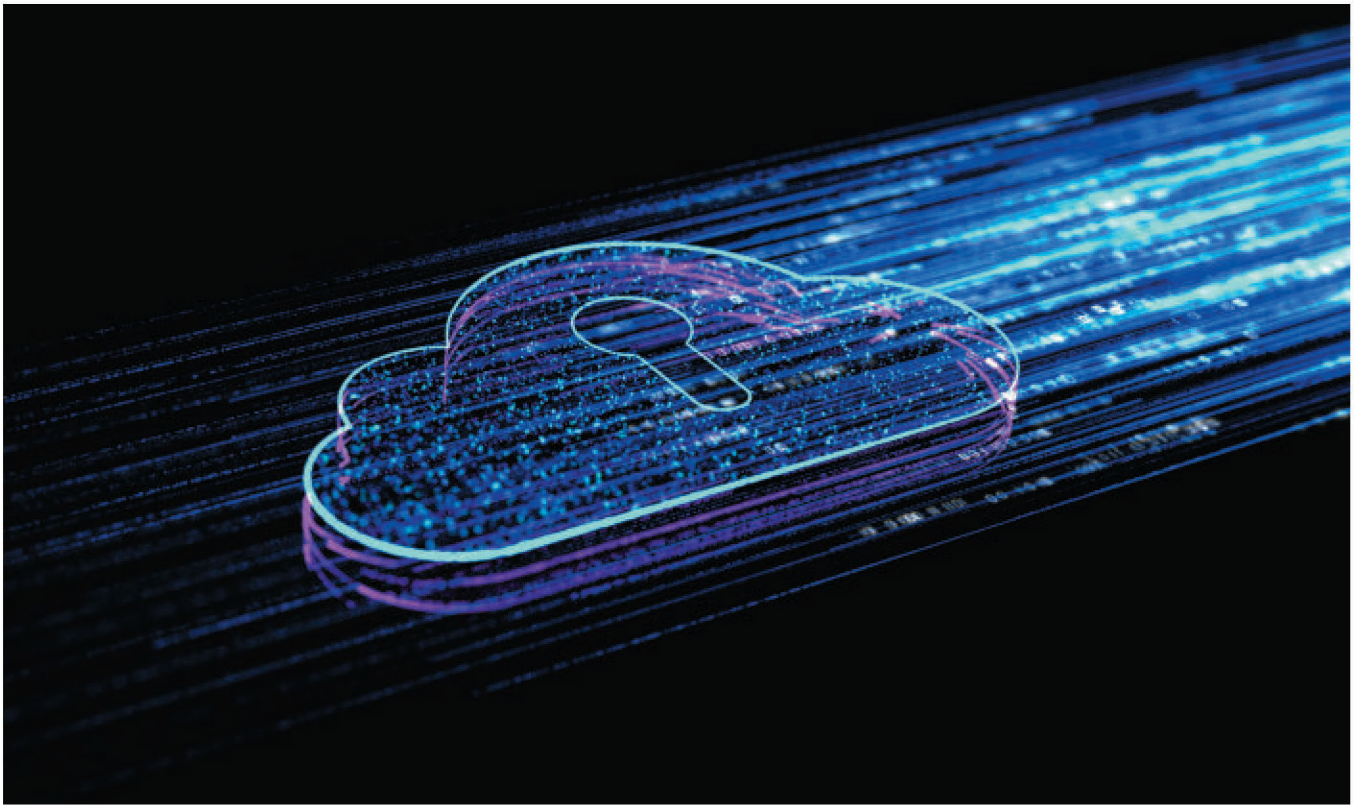
Strengthen Your Cyber-Resilience with an Acceptable Use Policy

Michele Vayle | RENOVODATA



ISTOCK.COM/KANAWATTH

HALF OF ALL U.S. organizations plan to continue allowing employees to work outside the office full-time for the foreseeable future. The data landscape has changed forever, and companies—especially 3PL's requiring 24/7 uptime—are scouting for tools to bolster their data recovery capabilities and resilience. The availability of shipping, tracking, and parcel data is more critical than ever before. If a 3PL falls victim to data corruption, hardware failure, ransomware, or even a natural disaster, the fallout could have operational implications with irreparable damage.

Unfortunately, our trusted employees are often responsible for exposures leading to cyberattacks and data outages. All it takes is a carrier rep clicking on the wrong link in their email, or a remote agent whose infected personal computer has been connected to the company network, and an entire organization's infrastructure could come crumbling down. Work from home has also accelerated the adoption of cloud-based applications, and without recovery tools and policies in place, an outage could leave critical data inaccessible. Network breaches, data theft, destructive malware, and phishing attacks are more common than ever—and more effective due to a disparate, remote workforce. A tactical, approachable first step towards resiliency from these threats is an Acceptable Use Policy.

Our employees may be responsible for exposures, but they are also an organization's first line of defense. If you equip your workers with the appropriate training and tools, such as an Acceptable Use Policy, you will become more resilient. Acceptable Use Policies are standards set by the company management that plainly state how an employee is permitted to use and access the organization's data and network. An Acceptable Use Policy is an effective model for employee mindfulness when interacting with company resources.

Comprehendible Security

The Acceptable Use Policy will be utilized by staff at each level of employment, and by individuals with varying levels of IT knowledge. Management should consider this when crafting the policy, and it should lead to a concise document with a table of contents for ease of navigation.

Guidelines & Protections

Acceptable Use Policies provide rules and regulations for all of the company-owned technology an employee has access to. Here are a few examples of guidelines and protections that a policy could provide:

- Specifics regarding which employees have access to interact with the trucking management software.
- Guidelines stating if an employee is allowed to connect their personal device to a company network and what protections their machine should have before it does.
- Implement precautions such as auto-locking PC's that have been left unattended.
- Restrictions that clearly forbid the installation of applications for personal use on company PC's where booking and loading data presides.

OUR EMPLOYEES MAY BE RESPONSIBLE FOR EXPOSURES, BUT THEY ARE ALSO AN ORGANIZATION'S FIRST LINE OF DEFENSE.

Newly Exposed Threat Vectors: Work from Home Endpoints

- **Unprotected PC's:** Work from home has provided employees plenty of good reasons to use their personal devices as opposed to those distributed by their employer. The issue is that their home computer doesn't have the same antivirus, ad-block, or email filtering that is standard for your organization. An Acceptable Use Policy would guide employees to the most effective tools to protect their home PC, or alternatively, disavow the use of their company-issued PC for personal activities.
- **Internet of Things Concerns:** Working with your team to give them the comfort of being able to work on their home computer with the company's security standards is an effective strategy to keep workers at home happy. The truth is, it will be much more than their computer that makes your network vulnerable. For example, due to the growing Internet of Things, a rogue actor could hack a printer that had has documents stored locally about loading or shipping. An Acceptable Use Policy may direct employees to connect work-related devices in their home to a virtual private network offered by the company, which would add a layer of protection between a compromised personal network of an employee and access to the company network.
- **Browsing Leads to Phishing:** Websites that would normally be frowned upon in offices (social media) are now at the employee's disposal from the comfort of their home. Social-engineered phishing attacks are commonplace on these sites and could become the burden of your organization. With an Acceptable Use Policy, you can clearly spell out that some sites are entirely forbidden to access on company machines, but you can also guide your employees on safe browsing. This is a great opportunity to implement cybersecurity training on phishing into your Acceptable Use Policy. Employees can learn about avoiding unsecure websites, identifying threatening links, and ultimately, they'll be equipped to browse safely and responsibly.

The Big Picture: Continuity Planning

The past few years have brought multiple disruptions to the traditional organizational data landscape. These changes encourage broadening component policies such as Internet Use, to include activity on machines with company data. Acceptable Use Policies and Internet Use Policies are two comparably small, core aspects of a much larger, comprehensive Business Continuity Plan. In total, these plans house a breakdown of core processes and people needed to stay operational in the event of a disaster—but many of these details have changed with the landscape. Strengthen your IT resiliency by updating your plans to reflect the changes brought about by remote work. Here are a few examples of quality tools that protect remote workplaces and can help bolster your updated plans.

- Organizations with remote workers largely rely on web applications, such as cloud-based email and other tools to transmit, interact, and create

ISTOCK.COM/MIKKELWILLIAM

company data. Now that they serve a critical function, offsite backups for suites such as Google Workplace or Microsoft Office 365 are a best practice. Cloud apps unfortunately have less than 100% uptime, and your employees are going to need to access the data saved on these apps when the provider is down or if the data is corrupted. The criticality of cloud suites and the data that lives within them has become a threat vector for a single point of failure for many organizations. Once a single point of failure is identified, it's crucial that recovery and continuity tools are implemented.

- Although more data is being stored in these web apps than ever before, there are still plenty of resources that employees have saved locally. Instead of saving locally, there are file-share tools available that store revisions of documents. These continuous backups allow the application to restore to a point in time moments before a data loss or corruption event. Additional benefits some of these tools offer are real-time syncing, strong encryption, and the ability to create shares at the individual, group and company level for seamless file permission access.
- Policies and Plans should not be treated as a substitute for (at the very least) annual cybersecurity training at each level of employment. Even basic, less effective training programs about topics like "identifying and responding to phishing attacks" have shown a 7-fold return on investment. Many training programs include short videos and quizzes that make it easy for employees to absorb information that could save your organization. Both the Acceptable and Internet Use Policies should refer to the subjects that employees will be educated about, and how often employees should engage in that training.

Plan of Attack: Protect

Work-from-home has created a host of responsibilities and has spread many 3PL technical support departments thin. This presents a unique struggle; the push and pull of technical resources have never been more strained. That's part of the reason why organizations of all sizes are seeking out certified business continuity professionals and managed service providers to help shoulder the responsibility of creating and updating policies and plans. A sizable cyber-attack or data loss event could cause customers to seek out competitors—so there's a need to have policies to support your people, and external support to help mitigate loss.

Business Continuity (BC) Plans are created simply to understand your environment and protect it. Supplemental documents like Acceptable Use Policies and resiliency tools such as backups for cloud applications, file sync & share, and cybersecurity training bolster the strength of a BC plan by empowering employees with knowledge and equipment. Be prepared for the inevitable in a new data landscape—and make your organization more resilient with disaster recovery and business continuity planning.

RenovoData is a leading cloud backup and disaster recovery planning company, and DR/BC planning service provider helping companies protect critical data worldwide. For more information and guidance, please call toll-free at 877-834-3684 or email us at info@renovodata.com