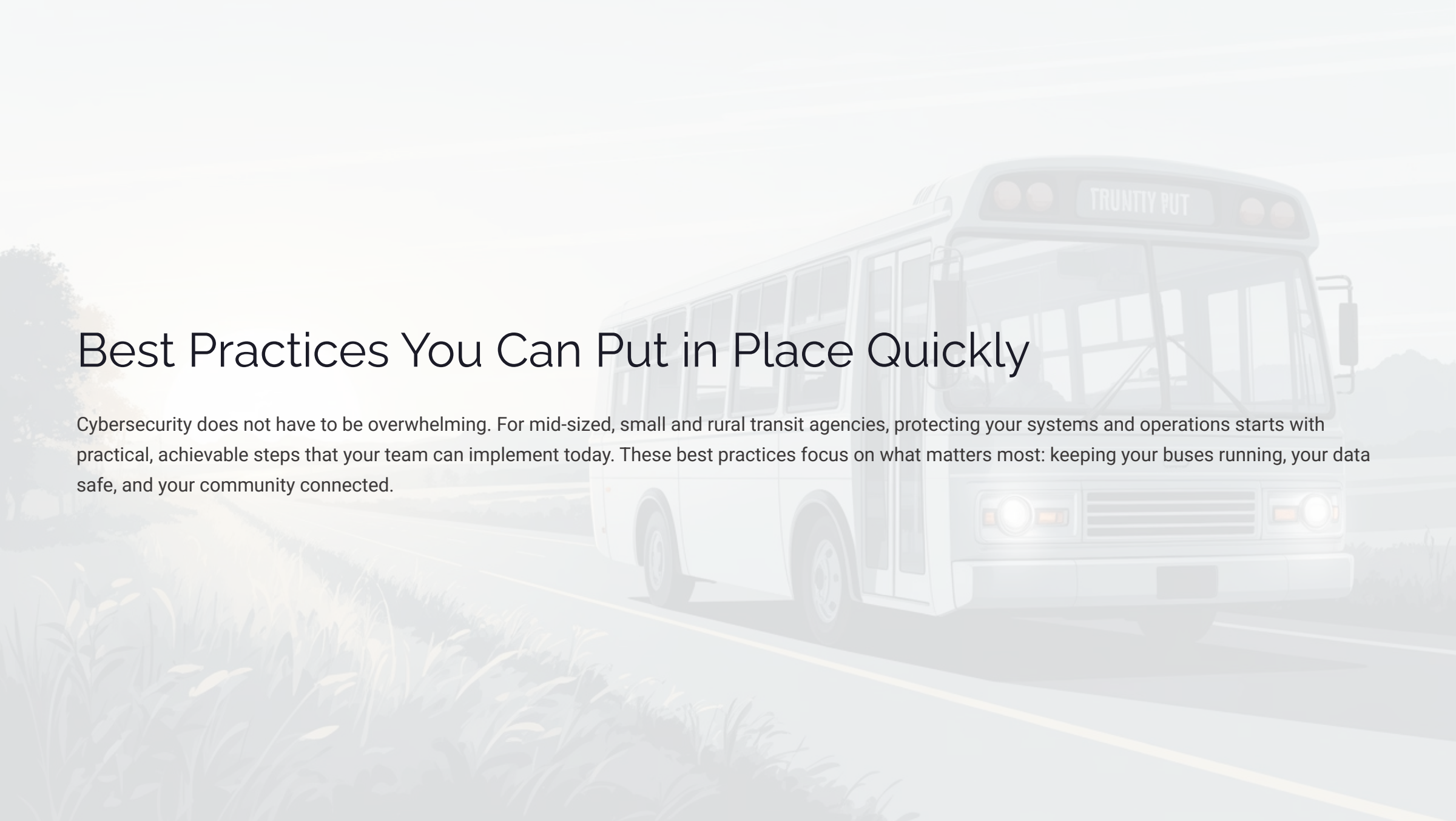


Best Practices You Can Put in Place Quickly

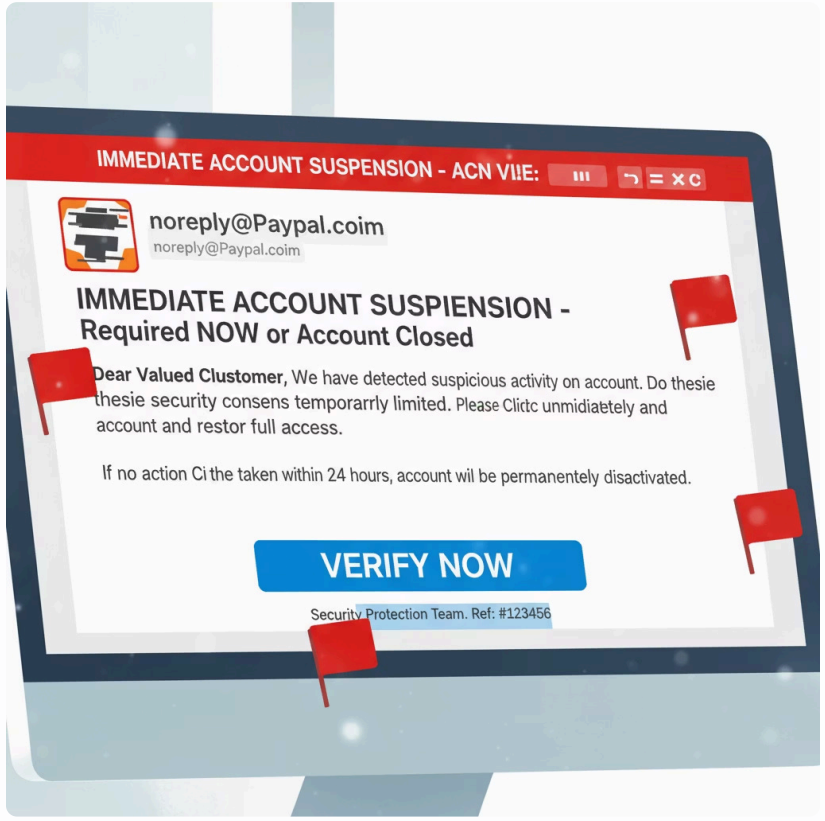
Cybersecurity does not have to be overwhelming. For mid-sized, small and rural transit agencies, protecting your systems and operations starts with practical, achievable steps that your team can implement today. These best practices focus on what matters most: keeping your buses running, your data safe, and your community connected.

Train Your Team to Recognize Phishing Attacks

Phishing remains the number one method attackers use to compromise transit systems. These deceptive emails trick employees into clicking malicious links or sharing sensitive information. The good news? A simple two-minute reminder at your next staff meeting can prevent a devastating outage.

Share real examples of suspicious emails with your team. Teach them to watch for urgent requests, unexpected attachments, and sender addresses that don't quite match legitimate sources. Encourage a culture where reporting suspicious messages is praised, not punished. When everyone becomes a first line of defense, your entire agency becomes more resilient.

Consider posting quick-reference guides near workstations showing common phishing red flags. Regular, brief touchpoints are far more effective than annual training sessions that staff quickly forget.



Prepare for System Downtime

01

Identify Critical Functions

List what you absolutely must do to dispatch buses and communicate with drivers when systems are offline.

02

Create Simple Fallbacks

Paper schedules, printed route maps, and analog communication methods can keep operations running during outages.

03

Document and Train

Make sure every team member knows where backup procedures are stored and how to access them quickly.

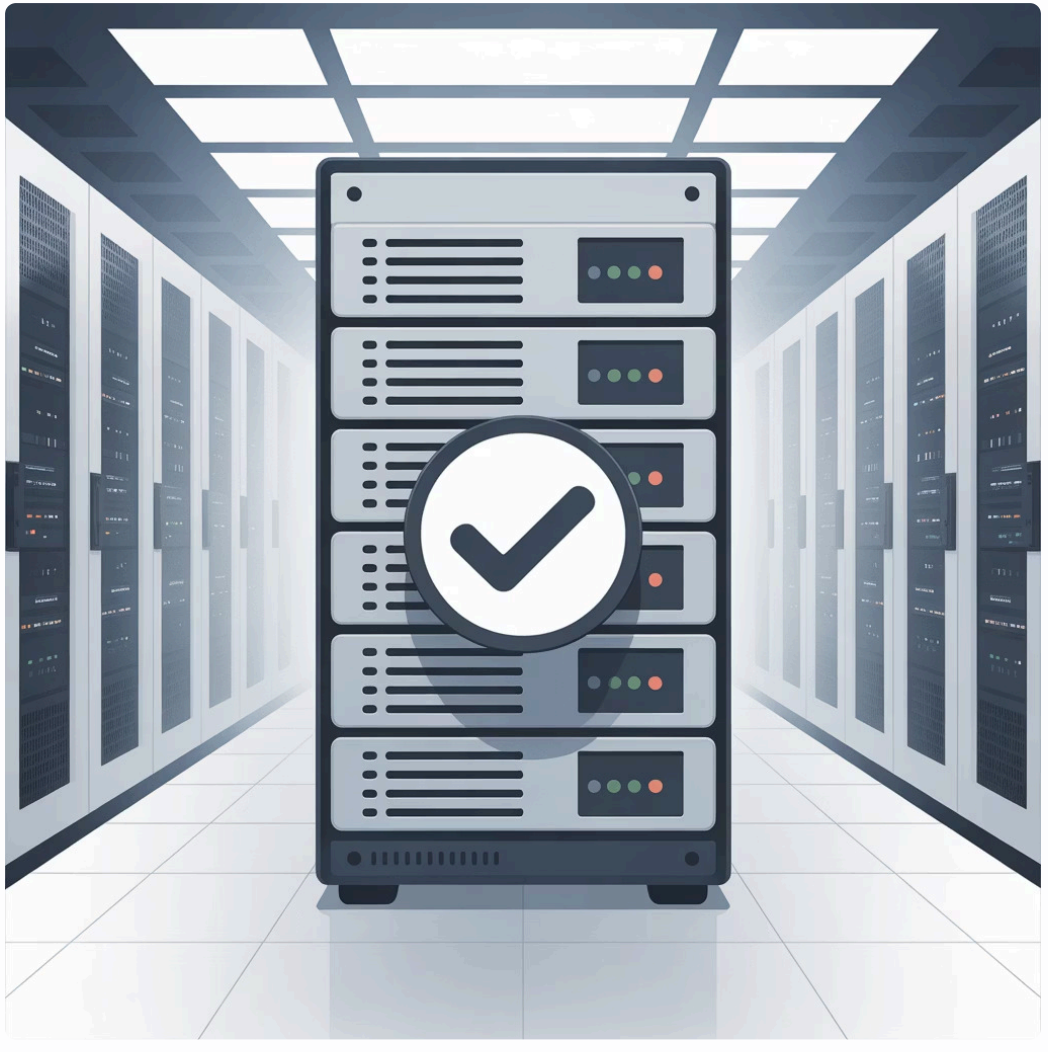
04

Test Your Plan

Walk through your fallback procedures once or twice a year to identify gaps and build staff confidence.

Could you still dispatch buses or access schedules if your network went offline tomorrow? Having a simple fallback plan, even if it relies on paper, can be the difference between continuing service and complete disruption. The key is ensuring everyone knows where these backup resources are located and how to use them effectively.

Back Up Your Data. And Prove You Can Restore It



A backup is only valuable if it actually works when you need it. Too many organizations discover their backups are corrupted or incomplete only during an emergency, when it is far too late to fix the problem.

Know exactly where your backups are stored, whether they are local, cloud-based, or both. Identify who is responsible for monitoring backup success and addressing failures. Most importantly, test your ability to restore data at least once per quarter.

This does not need to be complicated. Start by restoring a single file or small dataset. Document the process, time how long it takes, and note any issues. This simple exercise builds confidence and reveals problems while they're still manageable.

Document Everything and Share Knowledge

Critical Processes

Step-by-step procedures for essential tasks like dispatching, scheduling changes, and system restarts.

Password Management

Secure storage of credentials with clear protocols for password resets and account recovery procedures.

Vendor Contacts

Complete list of technology vendors, support numbers, account numbers, and escalation contacts for emergencies.

If one person knows everything and they are out sick or leave the agency, that is a critical vulnerability. Single-person dependency creates enormous operational risk that many small agencies do not recognize until it is too late.

Create simple documentation for your most important processes. This does not require fancy software, a well-organized binder or shared drive folder works perfectly. The goal is ensuring that someone else can step in and keep things running. Update documentation whenever processes change, and review it quarterly to ensure it remains current and accessible.

Limit Access and Maintain Emergency Contacts

Grant Minimum Necessary Access

Fewer administrators means fewer potential mistakes and security risks. Grant staff only the system access they actually need to perform their jobs effectively. This principle of "least privilege" (POLP) is one of the most fundamental security practices.

Regular access reviews help ensure permissions stay appropriate as roles change. When someone moves to a different position or leaves the agency, promptly remove their old access rights. This simple practice prevents unauthorized access and reduces your attack surface significantly.

Keep a Printed Contact List

In an emergency, you do not want to waste precious time hunting for contact information while systems are down. Create a printed "Who to Call" list and post it near dispatch or in a physical binder that everyone knows about.

Include your IT support contacts, key vendors, internet service provider, software companies, and relevant government agencies. Update this list whenever contact information changes and distribute copies to multiple locations for redundancy.

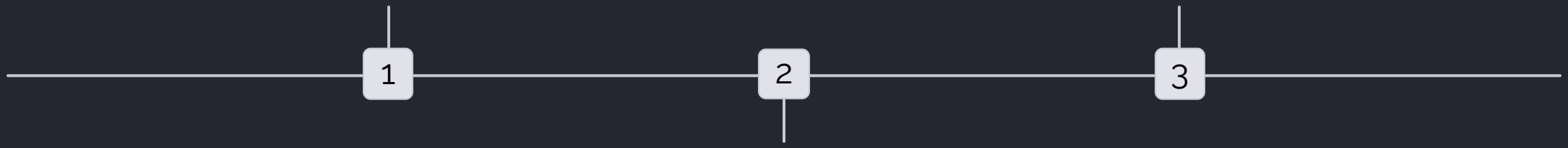
Review Your Readiness Regularly

Quarterly Reviews

Quick 30-minute check-ins to verify backups, test key processes, and update documentation as needed.

Annual Assessment

Comprehensive review using self-assessment tools to identify gaps and plan improvements for the coming year.



Semi-Annual Training

Brief refresher sessions on phishing awareness, security policies, and incident reporting procedures.

You do not need a full 200-page policy manual or complex compliance framework. What matters is repeating small, practical steps regularly. Consistency beats complexity every time, especially for resource-constrained rural transit agencies.

A quick self-review using simple assessment tools helps you spot small gaps before they become operational problems. This proactive approach is far less stressful and expensive than responding to incidents after they occur. Set calendar reminders to ensure these reviews actually happen rather than getting pushed aside by daily operations.

Essential Policies for Transit Agencies

Most small and rural transit agencies do not need eighteen different policy documents gathering dust on a shelf. Focus on the policies that actually move the needle and protect your operations. These four core policies establish clear expectations and provide practical guidance your team can actually follow.

1

Acceptable Use Policy

Sets clear expectations for how staff use computers, email, internet access, and agency systems. Defines appropriate and inappropriate uses to protect both the organization and employees.

2

Password & Access Control Policy

Defines password requirements, multi-factor authentication use, user account approval processes, and who receives administrative rights. Establishes the foundation for secure system access.

3

Data Backup & Recovery Policy

States what data gets backed up, where backups are stored, who owns the backup process, how often backups run, and how frequently restore tests occur.

4

Email & Phishing Awareness Policy

Provides plain-language expectations for email use and clear instructions on how to recognize and report suspicious messages. Empowers staff to be your first line of defense.

Critical Operational Plans

Incident Response Plan

Step-by-step guidance for what to do when something looks wrong and who to call for help. This should be one page, not forty, focused on immediate action steps that anyone can follow during a stressful situation.

Business Continuity/Disaster Recovery Plan

Defines how you keep buses moving and maintain essential services if systems go offline. Paper-based procedures are perfectly acceptable, the critical factor is usability under pressure, not sophistication.

Annual Cyber Program Plan

Establishes a quarterly rhythm for your cybersecurity activities: policy reviews, backup testing, brief training touchpoints, and simple tabletop exercises. Creates sustainable momentum without overwhelming your team.

These three plans transform cybersecurity from an abstract concept into concrete, actionable steps. They do not require technical expertise to create or follow, just practical thinking about your agency's specific operations and risks.

Why These Seven Documents Matter

With just these four policies and three plans, your transit agency gains powerful capabilities that dramatically improve security and operational resilience. This is the "minimum viable program" for cybersecurity in small transit - achievable, repeatable, and genuinely high-impact.

These documents enable your agency to control system access, maintain operations during outages, know exactly who to call when problems arise, and brief leadership with confidence. You will eliminate dangerous single-person dependency risks and establish a foundation for continuous improvement.

7	4	3
Core Documents	Essential Policies	Critical Plans
Everything you need to build a solid cybersecurity foundation	Clear expectations that guide daily operations and secure systems	Actionable procedures that keep your transit service running during disruptions

Start with these seven documents and refine them over time based on your actual experiences and needs. Perfection is not the goal, practical protection is. Your community depends on reliable transit service, and these straightforward tools help ensure you can deliver it consistently, even when technology challenges arise.