WATER SYSTEM

Security Self-Audit

A practical workbook for small and mid-size water systems

What this is. A guided walkthrough that helps you find the security problems that cause real incidents at water systems: the way people log in from outside, the passwords on your equipment, and what protects your unmanned sites. You do it yourself, at your own pace, with no special tools.

Who it is for. Operators, superintendents and managers at community water systems. You do not need an IT background. If you know your plant, you can do this.

How long it takes. Roughly six to ten hours of work, and you should spread it across several days. Each part stands on its own, so you can stop and pick it back up.

BEFORE YOU START — PLEASE READ THE SAFETY PAGE

This workbook is designed so that nothing in it can disrupt your plant. That only holds if you follow the safety rules on page 3. They are short. Read them first.

Prepared by:

D6 Labs
Engineered IoT Solutions

1-844-365-8647

info@d6labs.com

Free to use, copy and share within your utility and with other water systems.

Contents

How to Use This Workbook

Work through the parts in order. Part 1 builds the list of equipment and people that the rest of the workbook depends on, so do not skip it, even if it feels obvious.

Part	What you do	Roughly
1 · What Do You Have?	Write down your equipment, your sites, and who has access	1–2 hours
2 · Ways In From Outside	Find every path into your system from off-site	1–2 hours
3 · Passwords and Accounts	Check credentials on equipment and software	2–3 hours
4 · Walk Your Sites	Physically inspect your plant and remote sites	2–3 hours
5 · Quick Recovery Check	Could you get back up after losing everything?	30 minutes
6 · Score and Plan	Turn findings into a prioritised list with names and dates	1 hour
7 · What This Did Not Cover	Know the limits, and where to get more help	15 minutes
Appendix A · Fixing It	Practical guidance on the repairs, in the order to do them	Read as needed

YOU DO NOT HAVE TO SOLVE ANY OF THIS TODAY

This will turn up more than you expected. That is normal — almost every system finds the same things. Appendix A sorts the findings into what you can fix this week for nothing, what needs planning, and what belongs in a budget.

A few practical notes

- **Work with a partner where you can.** One of you writes while the other looks.
- **Write down what you do not know.** "Nobody here knows" is a finding, and often an important one.
- **Take photographs** inside panels and at remote sites. It saves a second trip.
- **Do not fix things as you go.** Write it down, finish the section, then plan the repair using Appendix A.
- **Keep the finished workbook somewhere safe.** It describes every weak point in your system.

What you need

- This workbook, printed, and something to write with
- A camera or phone, and keys to your panels and remote sites
- Any documentation you have: diagrams, manuals, integrator contact details
- A computer with internet access for one step in Part 2 — not one on your control network

Revision 1.0 *© 2026 Digital Six Laboratories Inc, All Rights Reserved*

Safety — Read This First

Your control system runs a plant that people depend on. Some of the equipment in it is older than the security tools people normally use to test networks, and it can be knocked offline by things that would not bother an office computer.

This workbook is built to be safe. Everything in it is *looking, reading, asking and writing down* — never testing, probing or changing. If you stay inside that boundary, nothing here can take your plant down.

DO NOT DO ANY OF THESE THINGS DURING THIS AUDIT

Each of these has caused real outages at real utilities. None of them are needed for anything in this workbook.

- Do not run scanning software of any kind against your control network. Network scanners and vulnerability scanners have crashed PLCs that were working fine.
- Do not try a default password on live equipment "just to see" if it works. You can lock the account, trip a fault, or lose your own access. Part 3 shows you a safe way to answer this question instead.
- Do not unplug network or serial cables to find out what they do.
- Do not reboot, reset or power-cycle anything as part of this audit.
- Do not change a PLC keyswitch position while the site is running, unless you have coordinated it and you know what the process will do.
- Do not install software of any kind on the SCADA computer.
- Do not connect your own laptop, phone or USB drive to the control network.

When to do this work

- During normal operating hours, when the people who know the system are available
- Not during a storm, a high-demand period, a chemical delivery, or any maintenance activity
- Not when you are the only person on duty
- Not on a Friday afternoon, if you can help it

If something goes wrong anyway

Stop the audit. Return to normal operations and follow your emergency response plan. Nothing in this workbook is more important than your plant running properly. You can come back to it tomorrow.

If you find something alarming

It happens — some utilities find an open remote-access tool or an unknown account on the first afternoon. Do not panic and do not start pulling cables. Finish documenting what you found, then contact your supervisor and your IT support. If you believe an intrusion is actually in progress, contact CISA at report@cisa.gov or 1-844-SAY-CISA, and your state drinking water program.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

What This Will and Will Not Find

What it will find

This workbook targets the problems that caused the actual attacks on water systems — not theoretical risks. In the incidents that made national news, attackers did not break sophisticated protections. They logged in using remote-access software, or found equipment sitting on the internet with the password it shipped with.

- Remote access paths you had forgotten about, or that more people can reach than you realised
- Equipment still using default or shared passwords
- Accounts belonging to people who no longer work for you
- Equipment reachable from the public internet
- Unmanned sites where the only protection is a padlock
- Missing records — nobody knowing who has access, or when a password last changed

What it will not find

Be clear-eyed about this. A self-audit has real limits, and knowing them is part of doing it properly.

- Whether someone is already inside your system. This workbook looks at doors, not intruders.
- Weaknesses that only show up in network traffic analysis
- Detailed firewall, switch and server configuration problems
- Software vulnerabilities in your PLCs, HMI or SCADA software
- Anything requiring active testing — which this workbook deliberately avoids

Part 7 covers where to go for the things this workbook cannot reach, including several excellent services that cost nothing.

How this relates to your AWIA risk assessment

If your system serves 3,300 people or more, federal law requires you to complete a Risk and Resilience Assessment and an Emergency Response Plan, and to recertify them to EPA every five years. Cybersecurity is not an optional part of that. The Safe Drinking Water Act requires the assessment to cover your "electronic, computer, or other automated systems (including the security of such systems)."

That requirement has been in the law since 2018. What has changed is that EPA is now actively inspecting and enforcing against systems that fall short, and the current recertification round is under way.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

THIS WORKBOOK IS NOT YOUR AWIA SUBMISSION

It does not replace a Risk and Resilience Assessment and it does not satisfy any regulatory requirement. What it will do is give you organised, written evidence about the cybersecurity part — an equipment list, an access list, findings and a dated remediation plan — which is exactly the material that part of the assessment needs and which most utilities have to assemble from scratch.

- Recertification deadlines are staggered by system size and by when you last certified. Confirm your own date — do not assume.
- Your state drinking water program can tell you your deadline and what they expect.
- If you are not sure whether you have ever done one, that is worth finding out this week.

WHEN YOU FINISH, PROTECT THIS DOCUMENT

A completed copy of this workbook is a list of every weak point in your water system. Treat it the way you would treat a master key.

- Keep the completed copy locked up, and limit who has it.
- Do not email it around, and do not leave it on a shared drive everybody can read.
- If your utility is subject to open-records law, talk to your attorney before this becomes a public document. Most states have a security exemption, but you need to ask before someone requests it — not after.
- When you replace it with a newer audit, shred the old one.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Part 1 · What Do You Have?

Everything else depends on this. You cannot protect equipment you have not written down, and most utilities have never made a complete list. Expect to find at least one thing nobody remembered was there.

1.1 Your sites

List every location with equipment that talks to your SCADA system — the plant, wells, towers, booster stations, lift stations, and anything else.

Site name	What's there	How does it communicate?	Manned?

Revision 1.0 *© 2026 Digital Six Laboratories Inc, All Rights Reserved*

1.2 Your control equipment

Walk through your sites list and write down the control equipment at each one. If you do not know a make or model, write down what is printed on the front of the box and move on.

Site	Equipment (PLC, HMI, radio, modem…)	Make / model	Age

1.3 Your computers

Every computer that touches the control system in any way.

Computer	Where is it?	Operating system	Used for anything else?

© 2026 Digital Six Laboratories Inc, All Rights Reserved

A QUESTION WORTH ASKING NOW

Is your SCADA computer also used for email, web browsing or paperwork? Write down the honest answer. It matters more than almost anything else in this workbook — it is the most common way trouble reaches a control system.

1.4 Who has access

List everyone who can get into the SCADA system or the control equipment — including contractors, your integrator, and anybody who used to work here whose access you are not certain was removed.

Name	Role	What can they access?	Still employed / current?

Now answer these

- ☐ Is there anyone on that list who no longer works here?
- ☐ Is there anyone on that list you were not certain about until you wrote it down?
- ☐ Does your integrator or vendor have access? Do you know when they last used it?
- ☐ Is there a written list like this anywhere else in your utility — or is this the first one?

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Notes, questions, and things to come back to

Revision 1.0 *© 2026 Digital Six Laboratories Inc, All Rights Reserved*

Part 2 · Ways In From Outside

This is the part that matters most. In the water system attacks that have made the news, this is how the attackers got in — not by defeating security, but by using a way in that was already open.

2.1 Remote access software

Remote access software lets you see and control the SCADA computer from somewhere else. Common names are TeamViewer, AnyDesk, LogMeIn, ScreenConnect, Splashtop, and Windows Remote Desktop. Look on the SCADA computer for any of these — check the taskbar, the system tray by the clock, and the list of installed programs.

Software	Who can use it?	Shared login?	Two-step login?	Last reviewed

For each one, answer honestly

- ☐ Does everybody use the same username and password to log in?
- ☐ Is there a second step after the password — a code from a phone, an app, or a key?
- ☐ Would you know if someone else logged in last night?
- ☐ Is it running all the time, or only turned on when needed?
- ☐ Does anyone outside your utility have access to it?
- ☐ Has anyone left the utility since this was set up?

WHY THIS SECTION MATTERS MOST

In 2021 an attacker used shared remote-access credentials at a Florida water plant and raised the sodium hydroxide setting to more than a hundred times its normal level. It was caught only because an operator happened to be watching the screen at that moment. The same category of software appears by name in the federal advisory for the July 2026 attacks. This is not a hypothetical risk.

2.2 Other ways in

Remote access software is the obvious one. These are the ones people forget.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Way in	Do you have it?	Who set it up, and when?
A VPN into the utility network		
Port forwarding on your internet router		
A cellular modem at any site		
A vendor or integrator connection		
Wi-Fi that reaches control equipment		
A dial-up or phone line to any equipment		
Anything else you can think of		

2.3 What the internet can see

There are search engines that continuously scan the internet and catalogue every device that answers — including industrial equipment. Attackers use them to find targets. You can use the same thing to see what they would see.

THIS STEP IS SAFE

Looking your own address up in a search engine does not touch your equipment at all. You are searching a database that was built elsewhere. This is one of the few outside-looking-in checks you can do with no risk whatsoever.

How to do it

Use a computer that is NOT on your control network — a home computer or an office machine that has nothing to do with SCADA.

- **Find your utility's public internet address.** On that computer, search for "what is my IP address." If your SCADA system uses a different internet connection, you need that one — ask whoever manages it.
- **Go to shodan.io** and search for that address. A free account is enough.
- **Write down anything that comes back.** Especially anything naming a control system brand, or any login page.
- **Also search your utility's name and your town's name.** Sometimes equipment is listed that way.

What came back	What is it?	Should it be there?

© 2026 Digital Six Laboratories Inc, All Rights Reserved

- ☐ Nothing came back at all (good — but see the note below)
- ☐ Something came back that I recognise and expect to be there
- ☐ Something came back that I did not know about
- ☐ I could not work out our public address, so I could not complete this step

If nothing came back, that is a good sign but not a guarantee — these search engines do not see everything, and your address may have changed recently. Write down the date you checked and check again in six months.

Notes, questions, and things to come back to

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Part 3 · Passwords and Accounts

Every publicly documented attack on a US water system in recent years involved a password problem — a default one, a shared one, or one belonging to somebody who had left.

THE SAFE WAY TO CHECK FOR DEFAULT PASSWORDS

Do not try the default password on live equipment to see whether it works. You can lock the account, trigger a fault, or lose your own access. Instead, find out what is known:

- Ask who set the equipment up, and whether they changed the password from the factory setting.
- Look for a record — a commissioning document, a password list, an email from the integrator.
- Check whether the device shows a last-changed date in its own settings, if you can view that without changing anything.
- If nobody can tell you when it was changed, write it down as UNKNOWN and treat it as though it was never changed. That is the safe assumption, and it is usually correct.

3.1 Equipment passwords

Work through the equipment list from Part 1. Include PLCs, HMIs, radios, cellular modems, network switches, cameras, and the SCADA software itself.

Equipment	Site	Password changed from factory?	When / who knows?

Mark each one Yes, No, or UNKNOWN. Count your UNKNOWNs — for planning purposes, treat every one of them as a No.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

3.2 Shared accounts

A shared login is one that several people use with the same username and password. They are convenient, and they are a problem for two reasons: when somebody leaves, the password walks out with them; and your records cannot tell you whether it was an operator or a stranger.

System	One login for everybody?	How many people know it?	Last changed
SCADA software			
Remote access software			
The SCADA computer itself			
PLC / HMI programming			
Cameras			

3.3 People who have left

Go back to the access list in Part 1.4 and check each departed person against every system.

- ☐ SCADA software login removed
- ☐ Remote access software login removed
- ☐ Windows or computer login removed
- ☐ VPN access removed
- ☐ Shared passwords they knew have been changed
- ☐ Keys and badges returned
- ☐ Their phone number removed from alarm call-out lists

If you cannot confirm all of these for everyone who has left in the past few years, that is a finding. In 2019 a former employee at a Kansas water district logged in with access nobody had removed and shut down the disinfection process.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

3.4 Two-step login

Two-step login — also called two-factor or MFA — means a password alone is not enough. There is a second step, usually a code from a phone app. It is the single most effective protection against a stolen password, and it is usually free.

Access path	Two-step login in place?	If not, is it available?
Remote access software		
VPN		
SCADA software login		
Cloud or vendor portals		
Email accounts		

Notes, questions, and things to come back to

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Part 4 · Walk Your Sites

Physical security is part of cybersecurity. The programming port inside a control panel bypasses every password you have. A fence and a padlock stop casual trespassers — they do not stop anyone who came deliberately.

Do this at your plant and at every remote site. If you have many similar sites, do all of them anyway — the weakest one is the one that matters, and it is usually the one furthest away that nobody has looked at in a year.

Per-site inspection

Copy this page for each site. Take photographs of anything you mark as a concern.

Site name: _____ **Date:** _____ **Inspected by:** _____

Getting to the equipment

Question	Yes	No	Notes
Is the site fenced?			
Is the gate locked, and is the lock in good condition?			
Is the building or enclosure locked separately from the gate?			
Is the control panel itself locked?			
Could someone reach the equipment without breaking anything?			
Is the site visible from a road or a neighbour?			
Is there lighting?			

Would you know if somebody had been there?

Question	Yes	No	Notes
Is there a camera?			
Does it alert someone, or only record?			
Is there a door or panel alarm wired into SCADA?			
Would an intrusion show up in an alarm log?			
When did you last check that any of this works?			

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Inside the panel

Open the control panel and look. Do not unplug anything, and do not change any switch positions.

Question	Yes	No	Notes
Is there a PLC programming port that is easy to reach?			
Is the PLC keyswitch set to RUN?			
Are there any network ports not being used?			
Is there a cellular modem or radio in the panel?			
Are there any devices you cannot identify?			
Is there a written password taped anywhere?			
Are there signs somebody has been in here — dust disturbed, new cables?			

ABOUT THE KEYSWITCH

Many PLCs have a physical switch with positions such as RUN, REMOTE and PROGRAM. Leaving it in REMOTE or PROGRAM allows the logic to be changed over the network. Setting it to RUN blocks that. Federal guidance after the July 2026 attacks recommends setting it to RUN — it costs nothing.

Do not change it during this audit. Note the position, and plan the change with whoever maintains your programming, because some systems legitimately need REMOTE for normal operation.

Radio and communications

Question	Answer
What kind of link does this site use? (radio, cellular, wired)	
If radio: is the traffic encrypted?	
If you do not know, who could tell you?	
Is the antenna or radio physically reachable from outside the fence?	

If nobody at your utility can tell you whether your radio traffic is encrypted, write that down as UNKNOWN and ask your integrator. It is one short question, and many radios have encryption built in that was simply never switched on.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Part 5 · Quick Recovery Check

This is a short section, but do not skip it. The most likely serious incident at a water utility is not a targeted attack — it is ransomware that arrives by email and spreads. What saves you then is not prevention. It is being able to recover.

Backups

Question	Answer
Do you have a backup of your SCADA configuration and screens?	
Where is it kept?	
Could ransomware on your network reach that backup?	
Do you have a copy of the program in each PLC?	
Are those copies current, or from the last time somebody changed something?	
When did anyone last actually RESTORE from a backup to check it works?	

That last question is the one that matters. An untested backup is a hope, not a plan — and a surprising number of backups turn out to be empty, corrupted, or years old.

Running without SCADA

- ☐ We could run the plant manually if we lost SCADA entirely
- ☐ Somebody currently on staff has actually done it
- ☐ There are written instructions for doing it
- ☐ We have practised it in the last year

Who do you call?

Situation	Who, and what number?
Something looks wrong with SCADA	
We think we have been attacked	
Our integrator / SCADA vendor	
State drinking water program	
CISA (report@cisa.gov · 1-844-SAY-CISA)	

© 2026 Digital Six Laboratories Inc, All Rights Reserved

If any of those are blank, filling them in is the cheapest thing you will do all week.

Notes, questions, and things to come back to

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Part 6 · Score and Plan

Now turn what you found into something you can act on and hand to your board.

6.1 Where you stand

For each area, tick the description that best matches what you found. This is not a grade — it is a starting position.

Area	Not started	Beginning	Managed	Strong
Knowing what you have				
Ways in from outside				
Passwords and accounts				
Physical site security				
Recovery readiness				

Rough guide:

- **Not started —** no records, nobody responsible, unknowns everywhere
- **Beginning —** you know roughly where you stand, but little is documented or verified
- **Managed —** written records, someone owns it, reviewed at least yearly
- **Strong —** all of that, plus you have tested it and it worked

6.2 Your plan

List what you found, worst first. Be honest about which column each item belongs in — the point of the three columns is that the first one contains things you can do without asking anybody for money.

Do this month — free or nearly free

What needs doing	Who	By when	Done

Revision 1.0 *© 2026 Digital Six Laboratories Inc, All Rights Reserved*

This budget year

What needs doing	Rough cost	Who	By when

Capital planning

What needs doing	Rough cost	Notes

IF YOU ONLY DO THREE THINGS

Across every water system attack that has been made public, these three would have prevented most of them — and none of them require a budget request.

- Get the SCADA computer off the internet, and off email and web browsing.
- Change every default password you found, and give each person their own login.
- Turn on two-step login for every way into your system from outside.

6.3 Tell somebody

A finished audit that stays in a drawer changes nothing. Take the plan from 6.2 to your superintendent, manager, board or council. You do not need to hand over this whole workbook — in fact you should not. A one-page summary of the three lists is enough, and it is more likely to be read.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

If you need to justify the spending, the news coverage from 2026 is the strongest argument you will ever have available, and this workbook is evidence that you looked.

Notes, questions, and things to come back to

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Part 7 · What This Did Not Cover

You have done the part that finds most real-world problems. Here is what is still outside the fence, so you know what you do not know.

Not covered in this version

- **Network segmentation and firewall configuration.** Whether your control network is properly separated from your office network, and whether the rules on that boundary are right.
- **Software vulnerabilities.** Whether the specific versions of software and firmware you run have known flaws.
- **Network traffic analysis.** What is actually talking to what, and whether anything unexpected is on your network.
- **Detecting an intrusion already in progress.** This workbook looks at doors. It does not look for footprints.
- **Deep configuration review** of servers, switches and the SCADA application itself.
- **Anything requiring active testing.** Deliberately excluded, for the safety reasons on page 3.

Free help — use it

These cost nothing. Do them.

Who	What they offer
EPA	Free cybersecurity assessments and technical assistance for water systems, through the Water Sector Cybersecurity Evaluation Program.
CISA	Free vulnerability scanning for water utilities — they scan from outside weekly and email you what is exposed. Also regional advisors who will visit your plant.
WaterISAC	Water-sector threat alerts and cybersecurity fundamentals for utilities.
Your state drinking water program	Many run cybersecurity assessment programs and can point you at grant funding.
Rural water association	Circuit riders and technical assistance, often at no cost to members.

When to bring in a professional

Consider paid help when any of these are true:

- You found things in this workbook you do not know how to fix
- You need an independent assessment for a regulator, an insurer, or your board

© 2026 Digital Six Laboratories Inc, All Rights Reserved

- You are planning a major SCADA upgrade and want the design reviewed before you buy
- You want the things in the 'not covered' list above properly examined

Questions to ask anyone you hire

These apply to every vendor, including the ones who wrote this workbook.

- What certifications do your assessors hold, and have any of them ever run a water plant?
- Will you run any active scans against our live control equipment? (If the answer is anything but a clear no, ask a great deal more.)
- What exactly will we receive at the end, and can we see a redacted example?
- Will the report be suitable for our board and for our regulator?
- Do you also sell equipment or remediation services? If so, how do you handle that conflict?
- How will you protect our data, and how long will you keep it?

Do this again

Set a reminder for twelve months from today and work through this workbook again. It is much faster the second time, and the point is to catch what has drifted — the new contractor account, the port forward somebody opened for a project, the site where the lock was replaced with a cheaper one.

Audit completed on: _____ **Next audit due: _____**

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Appendix A · Where to Start: Fixing What You Found

If you have just finished the workbook, you are probably looking at a longer list than you expected. Every utility that does this finds the same things, and none of it means anyone has been doing a bad job. Most of these problems were built in over years, by people making reasonable decisions with the budget and the tools they had.

You are not going to fix all of it, and you do not need to. A small number of these repairs prevent most of what actually happens to water systems. This appendix sorts them by what they cost and how hard they are, so you can start with the ones that are free and finish this week.

FIXING IS RISKIER THAN LOOKING — READ THIS BEFORE YOU CHANGE ANYTHING

The audit was safe because you only looked. Repairs are different: they change a working system, and a careless change can do more damage than the weakness you were fixing.

- Change one thing at a time, and write down what you changed and when.
- Before changing any password on control equipment, make sure the new one is recorded somewhere safe first. Some controllers cannot be recovered without a factory reset, which means losing the program.
- Radio encryption has to match at both ends. Turn it on at one site only and you lose that site.
- Before removing a port forward or a remote-access tool, find out who was using it. It may be how your integrator supports you, or how your after-hours callout works.
- Taking the SCADA computer off the internet can break licence checks, historian syncing or vendor support tools. Find out before you unplug it, not after.
- Do repairs in a planned window, not on a Friday, and have a way to put it back.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

The order to work in

Work down this table. It is arranged so that the cheapest, safest and highest-value repairs come first — and so that you get several wins before you have to ask anyone for money.

Fix	Cost	Risk of doing it	When
Remove access for people who have left	None	Low	This week
Fill in your who-to-call list	None	None	This week
Stop using the SCADA computer for email and web	None	Low	This week
Turn on two-step login where it already exists	None	Low	This week
Set PLC keyswitches to RUN	None	Medium — coordinate first	This month
Give every person their own login	None	Low	This month
Change default passwords	None	Medium — record them first	This month
Remove port forwards you do not need	None	Medium — check who uses them	This month
Lock the control panel, not just the gate	Low	None	This month
Password manager for the utility	Low	Low	This month
Cameras with person alerts at remote sites	Medium	None	This year
Panel tamper switches wired into SCADA	Low	Low	This year
VPN with two-step login for remote access	Medium	Medium	This year
Turn on radio encryption, or replace radios	Low to high	High — plan carefully	This year
Offline backups you have actually tested	Low	Low	This year
Separate the control network from the office	Medium to high	High	Capital
Replace unsupported operating systems	High	High	Capital

A1 · This week — free, and almost no risk

Remove access for anyone who has left

Work through the list from Part 3.3. Every departed person, every system. If a shared password was known to someone who has left, change it — that is the one case where changing a password is genuinely urgent.

Stop using the SCADA computer for anything else

No email, no web browsing, no paperwork. This is free, it takes a conversation rather than a purchase, and it removes the most common path by which trouble reaches a control system. If people need a computer for those things, they need a different computer.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

If something on the SCADA machine genuinely needs internet access — licence checks, remote support, a cloud historian — write down what and why. That becomes a real question for your vendor rather than a reason to leave everything open.

Turn on two-step login wherever it is already available

Most remote-access tools, VPNs and cloud portals support it and it is usually free. It takes a few minutes per account, and it is the single most effective protection against a stolen password. Start with any way in from outside.

Fill in the who-to-call list

From Part 5. Print it and put it where the night operator will find it.

Post the warning signs

Setpoints that moved on their own, logins at odd hours, the mouse moving by itself, PLCs dropping offline, your own account locked out. Put that list on the control room wall. Every operator becomes someone who might notice.

A2 · This month — free or cheap, but plan it first

Give every person their own login

Shared logins are the most common finding in this whole workbook, and they cause two problems: the password leaves with anyone who leaves, and your records cannot tell an operator apart from an intruder.

- Create an account for each person who genuinely needs one.
- Give people the level of access their job needs, not the maximum available.
- Once everyone has their own, retire the shared account rather than leaving it enabled.
- If your SCADA software cannot do per-person logins, write that down — it is a real limitation and it belongs in your next upgrade conversation.

Change default and unknown passwords

Everything you marked No or UNKNOWN in Part 3.1. Do this carefully — this is the repair most likely to go wrong.

- **Record the new password before you set it,** in your password manager or a sealed envelope in a safe. Not on a sticky note in the panel.
- **Do one device at a time,** and confirm you can still get in afterwards before moving to the next.
- **Check who else needs it** — your integrator may lose access, and you may need them at 2 a.m. next week.
- **Some equipment cannot be recovered** if you lose the password. For those, involve whoever maintains the programming.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

A word about rotating passwords

Older advice said change every password every 90 days. Current guidance has moved away from that, because forced rotation mostly produces Summer2026 followed by Autumn2026 — which is worse, not better.

Rotate on events, not on the calendar. Change a password when someone with access leaves, when a vendor engagement ends, when you suspect it has been exposed, or when it was shared and you are moving to individual accounts. Otherwise, use longer passphrases and leave them alone.

The exception is any password that still has to be shared — a piece of equipment that only supports one login. Those should be changed whenever the group of people who know it changes, and they should be first in line for replacement.

Set PLC keyswitches to RUN

This blocks changes to the control logic over the network, and it costs nothing. Federal guidance issued after the 2026 attacks recommends it.

Coordinate first. Some systems legitimately need REMOTE for normal operation or for how your integrator supports you. Ask before you turn the key.

Remove port forwards and unused remote access

Every path from Part 2 that nobody can justify. Before removing one, find out who set it up and who uses it — the answer is sometimes "our integrator, every month."

Lock the panel, not just the gate

The gate is a suggestion. The panel is the target. A decent lock on the enclosure is one of the cheapest improvements available, and while you are there, take the taped-up password off the inside of the door.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

A3 · This budget year — the things that cost money

Cameras that tell you somebody is there

Cameras that only record are useful after the fact. Cameras with person detection send an alert to a phone when a human — not a deer, not a branch — enters the site. That turns an unmanned site into one you find out about the same night.

- Look for person detection specifically, not just motion, or you will turn the alerts off within a week.
- Check what it needs: power, and either cellular or a network connection.
- Decide who receives the alerts and what they are expected to do about them.
- Cheaper than one emergency callout, at most sites.

Tamper switches into SCADA

A switch on the enclosure door, wired back as an alarm point. Now an opened panel is an alarm on the screen at 2 a.m. rather than something you discover next month. If you have spare digital inputs, this is among the cheapest options in this appendix.

Secure the radio links

Start by asking one question: is our radio traffic encrypted? Many radios have AES encryption built in and shipped with it switched off, in which case this is a configuration change rather than a purchase.

- **If encryption is available:** plan the change carefully. Both ends must match, so the sites have to be done together, and you want a way to put it back if something does not come up.
- **If it is not available:** put AES-capable radios in the capital plan, and until then treat everything on that link as public.
- **Either way:** alarm on values that do not make physical sense, so a spoofed reading has a chance of being caught.

Proper remote access

If people need to reach the system from outside — and they usually do — the answer is not to forbid it. It is a VPN with two-step login, instead of a consumer remote-desktop tool sitting there listening all day.

The principle worth remembering: your system should reach out to connect. It should not sit waiting for someone to connect in.

Backups you have actually restored

Backups of the SCADA configuration and of every PLC program, kept somewhere that ransomware on your network cannot reach — which usually means offline or on separate credentials. Then restore one, on purpose, and see whether it works. An untested backup is a hope.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

A4 · Capital planning — the ones you cannot fix with an afternoon

Some findings do not have a cheap repair, and pretending otherwise wastes your time. These belong in a capital conversation.

Separating the control network from the office network

If a ransomware infection on an office computer can reach the SCADA system, that is a network design problem, not a settings problem. Doing it properly usually needs help and planning, but it removes the most likely serious incident at a water utility.

Unsupported operating systems

A SCADA computer running an operating system that no longer receives security updates cannot be made safe by configuration. Newer SCADA versions increasingly require newer Windows, which in turn often requires newer hardware — so "upgrade the software" quietly means a new computer as well. Plan for the whole chain rather than being surprised by it.

When the architecture is the problem

There is a point at which you are adding locks to a building that was designed without doors in mind. If you find yourself maintaining a long list of compensating fixes, it may be time to ask what a modern replacement would look like rather than continuing to patch.

Whatever you look at, and whoever you talk to, these four questions separate systems that were designed to be secure from systems that had security added afterwards:

- ☐ Does the equipment connect outbound only, or is something sitting there listening for inbound connections?
- ☐ Is communication between sites encrypted?
- ☐ Are credentials certificates you can revoke, or passwords that can be stolen and shared?
- ☐ What can somebody do with physical access to the device?

Ask them of every vendor, including whoever gave you this workbook.

Paying for it

Most of A1 and A2 costs nothing but time. For the rest, there is usually more money available than utilities realise:

- State cybersecurity grant programs — several states now fund assessments and upgrades specifically for water utilities. Ask your state drinking water program what exists.
- Drinking Water State Revolving Fund
- Hazard mitigation and resilience funding, where security counts as resilience
- Your rate case — security is a defensible operating cost, and a completed audit is evidence

A finished copy of this workbook, with the plan from Part 6 attached, is a stronger funding request than a general appeal for cybersecurity money. It shows the board you looked, what you found, and exactly what the money would buy.

© 2026 Digital Six Laboratories Inc, All Rights Reserved

Write down what you changed

Keep a record as you go. It matters for your next audit, for your AWIA documentation, and for the next person who has this job.

Date	What we changed	Who did it	Verified working

© 2026 Digital Six Laboratories Inc, All Rights Reserved

About This Workbook

This workbook was produced by D6 Labs and is free to use, copy and share within your utility and with other water systems. We wrote it because the attacks on water systems in 2026 exploited problems that most utilities could find and fix themselves, without hiring anybody — if somebody handed them a structured way to look.

We build SCADA equipment. We have deliberately kept our products out of this workbook, and the questions in Part 7 are the ones we would want you to ask us as much as anyone else. If this document is useful to you and you never speak to us again, it has done its job.

Disclaimer

This workbook is provided for educational purposes only, without warranty of any kind, express or implied. It is not professional security advice and is not a substitute for a professional security assessment. It does not claim to be complete, and completing it does not guarantee the security of any system.

Completing this workbook does not by itself satisfy any regulatory requirement, including the risk and resilience assessment requirements of America's Water Infrastructure Act §2013. It may help you prepare for those requirements. Confirm your obligations with your state drinking water program.

You are responsible for the security of your own systems and for any action you take or do not take as a result of this workbook. D6 Labs accepts no liability for any loss, damage or disruption arising from its use. Follow the safety guidance on page 3.

Version

Version 1.0 — August 2026

This is the first edition, and it deliberately covers a narrow set of topics — the ones that account for most real incidents. Later editions will add network segmentation, backup and recovery in depth, and incident response planning.

Tell us what was wrong with it

If something in here was unclear, took far longer than we said, or did not apply to your system, we would genuinely like to know. That feedback is what makes the next edition better.

1-844-365-8647
info@d6labs.com

© 2026 Digital Six Laboratories Inc, All Rights Reserved