Cybersecurity Plan Template

(Compliant with Missouri Water Safety & Security Act, § 640.142, RSMo)

Replace bracketed text with utility‑specific information. Review at least annually or whenever major changes occur.

# 1. Cover Page

Utility Name: [City / District]

Public Water System ID (PWSID): [MO--‑‑‑‑‑‑]

Plan Version & Date: [v1.0 – 15 Aug 2025]

Prepared by / Contact: [Title, phone, email]

# 2. Purpose and Scope

This plan fulfills § 640.142, RSMo, by identifying cyber‑related risks to both information‑technology (IT) and operational‑technology (OT) assets that support the drinking‑water system, and by defining the controls, schedule, and responsibilities needed to manage those risks.

# 3. Regulatory & Policy References

• Missouri Water Safety & Security Act (§§ 640.141 – 640.145, RSMo)

• America’s Water Infrastructure Act (AWIA) Risk & Resilience Assessment / ERP (if applicable)

• [Utility] Acceptable‑Use Policy, Backup Policy, Incident‑Response Plan (IRP), etc.

# 4. System Overview

4.1 Physical & Organizational Context – service area, population served, staffing.

4.2 Critical Processes – treatment, distribution, SCADA, billing, laboratory data, etc.

4.3 Network Architecture Summary – plain‑language narrative; attach a diagram in Appendix B.

# 5. Asset Inventory (Statutory cornerstone)

Provide (or reference) a table listing every IT and OT asset that is network‑connected or critical to operations:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Asset Name | Type (IT/OT) | Location | Connectivity | Software/Firmware | Owner | Criticality |
|  |  |  |  |  |  |  |  |

Insert the complete inventory in Appendix A; keep a master spreadsheet for updates.

# 6. Risk Assessment

6.1 Methodology – e.g., NIST CSF, CIS Controls, or simplified “likelihood × impact” matrix.

6.2 Threat & Vulnerability Identification – summarize findings (malware, unauthenticated remote access, outdated firmware, shared passwords, etc.).

6.3 Risk Register – map each significant risk to its existing controls, residual risk score, and mitigation action (see Section 7).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Description | Existing Controls | Residual Risk Score | Reference to Section 7 |
|  |  |  |  |  |

# 7. Risk Mitigation Plan

For each Medium or High risk, document one or more controls, responsible party, and target date.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk ID | Control(s) / Action | Type (Technical / Administrative / Physical) | Responsible | Target Date | Status |
|  |  |  |  |  |  |

Typical control categories to consider: network segmentation/firewalls, multi‑factor authentication, secure remote access, offline backups, patch management, logging & alerting, employee cyber‑awareness training.

# 8. Implementation Schedule & Resources (Statutory requirement)

Provide a schedule showing who will perform what by when, along with estimated labor hours, capital purchases, or grant funding (e.g., WSSA Project Grant).

# 9. Incident‑Response & Recovery Integration

9.1 IRP Reference – cite where the full incident‑response plan is stored.

9.2 Escalation Contacts – internal chain of command, CISA reporting e‑mail/phone, FBI field office.

9.3 Backup & Restore Procedures – location of offline copies, restoration time objective (RTO).

# 10. Training & Awareness Program

• Annual cybersecurity refresher for all staff with network or SCADA access

• Role‑based training for administrators and operators

• Tabletop exercise frequency (e.g., once per calendar year)

# 11. Plan Maintenance and Review

• Scheduled Review: every 12 months (due each January)

• Triggered Review: after any cyber incident, major asset change, or SCADA upgrade

• Revision Log: maintain version history with date, editor, and summary of changes

|  |  |  |
| --- | --- | --- |
| Date | Editor | Summary of Changes |
|  |  |  |

# 12. Approval & Certification

|  |  |  |
| --- | --- | --- |
| Name / Title | Signature | Date |
|  |  |  |
|  |  |  |

# Appendices

A. Detailed Asset Inventory Spreadsheet

B. Network / Data‑flow Diagram

C. Risk Assessment Worksheets

D. Policies & SOPs Referenced

E. Revision History

# Quick‑Use Checklist

* ☐ Asset inventory updated < 1 year old
* ☐ Risks scored and documented
* ☐ Mitigation actions assigned with deadlines
* ☐ Offline backups tested within last 90 days
* ☐ Cyber‑incident contacts verified
* ☐ Staff cyber training completed this year
* ☐ Management signed latest version