



A Middlesex Water Company Affiliate

August 29, 2022

Electronic Delivery via DelaFile

Samantha Hemphill
Ombudsman
Delaware Public Service Commission
861 Silver Lake Boulevard
Cannon Building, Suite 100
Dover, DE 19904

Re: Docket 16-0659
2022 Annual Cybersecurity Filing – Tidewater Utilities, Inc.

Dear Ms. Hemphill:

In compliance with Delaware Public Service Commission (PSC) Order No. 8955 in the above referenced docket, Tidewater Utilities, Inc. (Tidewater) respectfully submits that it has reviewed the list of questions pertaining to cybersecurity posted on the PSC's website and finds that no revisions at this time are recommended. Furthermore, Tidewater's responses to the questions previously provided questions to the PSC are attached.

If you have any questions regarding the changes to this application, please contact me at (302) 747-1308.

Sincerely,

A handwritten signature in black ink, appearing to read "J.C. Cuccinello".

Joseph C. Cuccinello
CPCN Coordinator

Enclosures

cc: Georgia Simpson, Tidewater Utilities, Inc.
Kirsten Higgins, Tidewater Utilities, Inc.

PSC Docket No. 16-0659

Tidewater Utilities Inc. Cybersecurity Responses

Planning/Risk Management:

- Is your cybersecurity plan regularly reviewed and audited? Internally or externally?
Yes, Both, internally and externally.
- Has your plan been reviewed recently? If not how often is it reviewed?
Yes, Annually
- Do you assess vulnerabilities to your system and assets?
Yes
- Do you assess threats to your system and assets?

Yes
- Do you prioritize risks? And what processes do you use?

Yes, Risks are prioritized by our external contractor based on severity and potential impact to the asset and the company.

Personnel and Policies:

- Are background checks being conducted upon hire?

Yes
- Do you provide internal cyber security training for all employees?
Yes
- Do you provide enhanced internal cyber security training for those that are actually in the utilities operating network?

No.
- Are there structural and/or organizational policies and procedures in place that allows the utility to able to address or think through these things (cybersecurity issues)?

Yes

- Are there managerial and operational controls in place?

Yes

- How quickly is access to those personnel who quit/fired eliminated?

Less than 24 hours

- Do you have certain employees that are assigned as cybersecurity personnel?
Or outsourced?

Both

- Do you have specific practices and policies in place about how your private customer data should be handled? Contingency plans for breach of data?

Yes

- Are recovery activities communicated to internal stakeholders and executive and management teams?

Yes

- Do you screen vendors and third parties that have access to cyber control systems?

Yes

Standards and Guidelines for Reporting

- Do you have a disaster recovery plan? (The plan itself should not be made public.)

Yes

- Do you have separate plans for separate business units in the company?

No.

- Are you reporting to the necessary agencies in regards to your plan?

Yes

- Are response and recovery plans regularly tested?

Yes.

- Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?

Yes

- Do you have a list of contacts for cybersecurity information sharing? (i.e. Federal and state emergency management, law enforcement, National Security, or Any others?)

Yes

- Should the commission create guidelines or regulations to ensure utilities are properly managing cyber security issues?

No

- Does your utility use multi-factor identification for system sign-on purposes?

Yes

- Do you keep audit logs for all remote connection protocols?

Yes

- Do you have the capability to identify and suspend access of users exhibiting unusual computer activity?

Yes