City of Elkins

Sanitary Board

July 15, 2024
10:00 AM
401 Davis Avenue
Council Chamber, 2nd Floor

Meets every 3rd Monday of the month

AGENDA

1. **Call to order and roll call**
2. **Public comment**
3. **Minutes**
    a. Proposed minutes for the meeting of June 17, 2024
4. **Presentation**
5. **Reports**
    a. Wastewater Superintendent/Chief Operator
    b. Wastewater Collection Supervisor
    c. Financial Statements as of June 30, 2024
6. **Unfinished business**
7. **New business**
    a. Approval of Sewer Invoices
    b. Consideration of BIDS for the Vacuum Truck Dumping Station
    c. Cybersecurity Policy for Sanitary Department
8. **Announcements**
9. **Adjournment**

CITY OF ELKINS
AGENDA ITEM REPORT

Meeting Date:	July 15, 2024
Section:	Minutes
Category:	Action Item
Agenda Item Name:	Proposed minutes for the meeting of June 17, 2024
Recommended By:	Whitney Hymes-Wastewater Superintendent/Chief Operator
Summary:	Approval of minutes for the June 17, 2024 Sanitary Board Meeting
Fiscal Impact:	N/A
Recommendation:	Consider for Approval
Attachments:	1. Sanitary Board - 2024_06_17 - minutes

SANITARY BOARD
REGULAR MEETING
MINUTES

401 Davis Avenue
City Hall, Council Chambers
June 17, 2024
10:00 a.m.

Present were Committee Members: Jerry Marco, Richard Carr

Also attending: Whitney Hymes (Wastewater Chief Operator), Tracy Judy (Treasurer), and Liz Roberts (Executive Secretary) were also present.

Randall Biller and Mark Hartley were absent.

MINUTES

Richard Carr, **MOVED APPROVAL OF THE MINUTES OF THE MAY 30, 2024, MEETING.** The motion carried.

REPORTS

Whitney Hymes, Wastewater Superintendent/Chief Operator, provided a report for the month of May 2024.

Tracy Judy (City Treasurer) provided financial reports for the month of May 2024.

NEW BUSINESS

Jerry Marco **MOVED APPROVAL OF SEWER INVOICES.** The motion carried.

Sewer Issues at 1210 S. Davis Street- resident provided no information. Therefore, item was removed.

Jerry Marco, **MOVED APPROVAL OF ENTERING INTO EXECUTIVE SESSION FOR THE PURPOSE OF SEWER ISSUES AT 312 S. RANDOLPH AVE.** The motion carried. The Board entered executive session at 10:09 a.m. and returned at 10:11 a.m. The chair announced that no action was taken.

The meeting adjourned at 10:12 a.m.

The foregoing minutes were approved at the meeting of ___________, 2024 Sanitary Board meeting.

Name & Title	Signature

CITY OF ELKINS-SANITARY BOARD

WASTEWATER SUPERINTENDENT/CHIEF OPERATOR REPORT

Date:	July 15, 2024
Time:	10:00AM
Report Presented By:	Whitney Hymes-Wastewater Superintendent/Chief Operator

11TH STREET LINE RELOCATION

- Advertisement for BIDS were published on June 5th and June 12th
- BID Opening was on July 10, 2024 @ 2:00PM at Elkins City Hall 2nd Floor Council Chambers.
- BID tabulation is as follows:
  - Hulls's Contracting Inc. ***Total BID= $134,800.00***
  - Green River Group, LLC ***Total BID=$138,435.00***
  - Doss Enterprises LC ***Total BID=$170,000.00***
  - Polino Contracting, Inc ***Total BID=$189,603.00***
- All work summarized shall be substantially complete within sixty (60) calendar days after the date when the contract times commence to run.
- This will be presented to council at the August 1, 2024 Council Meeting

DUMP STATION CONSTRUCTION

- Advertisement for BIDS were published on June 7th and June 14th
- BID opening was on July 10, 2024 @ 3:00PM at Elkins City Hall 2nd Floor Council Chambers
- BID tabulation is as follows:
  - Hulls' Contracting Inc.
    Total BID: $268,500.00
    Deductive Alternative #1: $5,000
    Deductive Alternative #2: $60,000
  - Green River Group, LLC
    Total BID: $392,000
    Deductive Alternative #1: $15,000
    Deductive Alternative #2: $62,000
  - Polino Contracting, Inc
    Total BID: $396,921.00
    Deductive Alternative #1: $12,517.00
    Deductive Alternative #2: $58,240.00

- All work summarized shall be substantially complete within sixty (60) calendar days after the date when the contract times commence to run.
- This has been added to the July 15, 2024 Sanitary Board Agenda for consideration

GEORGETOWN SEWER LINE EXTENSION

- Procurement for Engineering Services was sent on June 5, 2024.
- Deadline to submit requested information is June 26, 2024 @ 3:00PM
- Committee selected for review of firms-Whitney Hymes, Randall Biller, Rich Carr, and Jasmine Mallow

WASTEATER COLLECTION STORAGE BUILDING

- 1st Reading occurred on 1/18/2024 Council Meeting
- 2nd Reading occurred on 2/15/2024 Council Meeting
- 3rd Reading occurred on 3/21/2024 Council Meeting
- Notice to Proceed was given on 5/3/2024
- Notice of Award and Agreement was signed by Lee Reger Builds, Inc on 5/13/2024
- Meeting with Lee Reger Builds, LLC on 5/20/2024
- Start date of construction is 6/17/2024
- Materials delivered to 31 Jones Ave-waiting approval from Fire Marshall to proceed with construction.
- All work summarized shall be substantially complete within sixty (90) calendar days after the date when the contract times commence to run.

CONSENT DECREE/LTCP UPDATES

- No updates from EPA concerning the LTCP updates or the Consent Decree
- Flow Meters were calibrated on June 19-20 and (2) rain gauges installed at Barron Ave Lift Station and Old Elkins Plant Lift Station.

HIRING OF ADMINISTRATIVE ASSISTANT

- Jasmine Mallow was hired as the part-time Administrative Assistant. Her first day was July 1, 2024.

FISCAL YEAR 2025 RAISES

- The FY2025 wastewater raises that were approved at the May 30, 2024 Sanitary Board Meeting were implemented on July 1, 2024. Overtime has been limited in the department to help with budget restraints at this time.

FY 2024 BUDGET CONTROL REPORT

Revenues	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Revenues Over Expenses	Total
	$216,491.85	$207,080.31	$217,303.75	$243,124.25	$248,104.41	$215,658.94	$206,231.45	$275,589.81	$294,490.38	$229,240.03	$251,484.99	$252,264.77	-$46,969.75	$2,857,064.94
Expenses	**July**	**Aug**	**Sept**	**Oct**	**Nov**	**Dec**	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**		
	$244,836.96	$222,640.35	$241,235.73	$232,602.45	$312,911.69	$255,922.02	$248,473.42	$215,323.88	$245,346.95	$256,968.52	$268,683.05	$159,089.67		$2,904,034.69

Bank Balance as of 6/30/2024: $93,964.21

401-SEWER FUND
FINANCIAL SUMMARY

% OF YEAR COMPLETED: 100.00

	CURRENT BUDGET	CURRENT PERIOD	PRIOR YEAR PO ADJUST.	Y-T-D BALANCE	TOTAL ENCUMBERED	BUDGET BALANCE	% OF BUDGET
REVENUE SUMMARY							
TAXES	15,000	1,048.70	0.00	24,861.52	0.00	(9,861.52)	165.74
CHARGES FOR SERVICES	2,775,000	215,838.82	0.00	2,588,644.48	0.00	186,355.52	93.28
MISCELLANEOUS REVENUE	170,000	35,377.25	0.00	243,558.94	0.00	(73,558.94)	143.27
TOTAL REVENUE	2,960,000	252,264.77	0.00	2,857,064.94	0.00	102,935.06	96.52
EXPENDITURE SUMMARY							
CSO	50,459	2,269.41	0.00	35,814.11	0.00	14,644.39	70.98
CSO-OTHER	145,576	9,188.98	0.00	131,979.69	0.00	13,596.31	90.66
SEWER COLLECTION	1,001,170	52,417.84	0.00	928,806.80	0.00	72,362.70	92.77
SEWER TREATMENT	1,345,974	83,809.01	0.00	1,262,636.45	0.00	83,337.55	93.81
UTILITY BILLING	28,610	1,404.12	0.00	26,707.31	0.00	1,902.69	93.35
ADMIN & GENERAL	388,212	10,000.31	0.00	442,427.58	0.00	(54,215.58)	113.97
CAPITAL OUTLAY	0	0.00	0.00	75,662.75	0.00	(75,662.75)	0.00
TOTAL EXPENDITURES	2,960,000	159,089.67	0.00	2,904,034.69	0.00	55,965.31	98.11
REVENUE OVER/(UNDER) EXPENDITURES	0	93,175.10	0.00	(46,969.75)	0.00	46,969.75	0.00

401-SEWER FUND

% OF YEAR COMPLETED: 100.00

REVENUES	CURRENT BUDGET	CURRENT PERIOD	PRIOR YEAR PO ADJUST.	Y-T-D BALANCE	TOTAL ENCUMBERED	BUDGET BALANCE	% OF BUDGET
TAXES							
401-000-302-0000 Penalty Income	15,000	1,048.70	0.00	24,861.52	0.00	(9,861.52)	165.74
TOTAL TAXES	15,000	1,048.70	0.00	24,861.52	0.00	(9,861.52)	165.74
CHARGES FOR SERVICES							
401-000-361-0000 Metered Sales to Res Cu	1,290,900	103,398.07	0.00	1,188,004.94	0.00	102,895.06	92.03
401-000-361-0001 Metered Sales to Comm C	1,050,000	72,976.68	0.00	957,601.38	0.00	92,398.62	91.20
401-000-361-0002 Unmetered Sales to Res	19,100	1,198.09	0.00	16,118.39	0.00	2,981.61	84.39
401-000-361-0003 Taps & Connections	10,000	750.00	0.00	12,329.48	0.00	(2,329.48)	123.29
401-000-361-0004 Services to Other Syste	405,000	37,515.98	0.00	414,590.29	0.00	(9,590.29)	102.37
TOTAL CHARGES FOR SERVICES	2,775,000	215,838.82	0.00	2,588,644.48	0.00	186,355.52	93.28
MISCELLANEOUS REVENUE							
401-000-380-0000 Interest Earned	13,000	322.65	0.00	5,761.60	0.00	7,238.40	44.32
401-000-381-0000 Reimbursements	2,000	0.00	0.00	2,908.10	0.00	(908.10)	145.41
401-000-382-0000 Refunds & Rebates	4,000	0.00	0.00	4,234.78	0.00	(234.78)	105.87
401-000-383-0000 Sale Of Fixed Asset	0	0.00	0.00	14,647.00	0.00	(14,647.00)	0.00
401-000-386-0000 Insurance Claims	0	0.00	0.00	0.00	0.00	0.00	0.00
401-000-399-0000 Miscellaneous	1,000	2,059.08	0.00	16,278.43	0.00	(15,278.43)	1,627.84
401-000-399-0001 Lab Analysis Services	150,000	32,995.52	0.00	199,729.03	0.00	(49,729.03)	133.15
TOTAL MISCELLANEOUS REVENUE	170,000	35,377.25	0.00	243,558.94	0.00	(73,558.94)	143.27
TOTAL REVENUE	2,960,000	252,264.77	0.00	2,857,064.94	0.00	102,935.06	96.52

401-SEWER FUND
CSO

% OF YEAR COMPLETED: 100.00

EXPENDITURES	CURRENT BUDGET	CURRENT PERIOD	PRIOR YEAR PO ADJUST.	Y-T-D BALANCE	TOTAL ENCUMBERED	BUDGET BALANCE	% OF BUDGET
PERSONAL SERVICES							
401-509-103-0000 Salaries & Wages	19,095	1,464.00	0.00	19,468.33	0.00	(373.33)	101.96
401-509-104-0000 FICA Tax	1,590	107.70	0.00	1,499.08	0.00	90.92	94.28
401-509-105-0000 Group Health Insurance	7,560	565.95	0.00	6,791.39	0.00	768.61	89.83
401-509-106-0000 Retirement	2,047	131.76	0.00	1,827.83	0.00	219.17	89.29
401-509-108-0000 Overtime/Extra Help	1,667	0.00	0.00	840.67	0.00	825.83	50.45
TOTAL PERSONAL SERVICES	31,959	2,269.41	0.00	30,427.30	0.00	1,531.20	95.21
CONTRACTUAL SERVICES							
401-509-216-0000 Maint of CSO Equipment	10,000	0.00	0.00	1,685.00	0.00	8,315.00	16.85
401-509-217-0000 Maint Repair Autos & Tr	1,000	0.00	0.00	0.00	0.00	1,000.00	0.00
TOTAL CONTRACTUAL SERVICES	11,000	0.00	0.00	1,685.00	0.00	9,315.00	15.32
COMMODITIES							
401-509-341-0000 Supplies & Materials	6,000	0.00	0.00	3,701.81	0.00	2,298.19	61.70
401-509-343-0000 Automobile Supplies	1,500	0.00	0.00	0.00	0.00	1,500.00	0.00
TOTAL COMMODITIES	7,500	0.00	0.00	3,701.81	0.00	3,798.19	49.36
TOTAL CSO	50,459	2,269.41	0.00	35,814.11	0.00	14,644.39	70.98

401-SEWER FUND
CSO-OTHER

% OF YEAR COMPLETED: 100.00

EXPENDITURES	CURRENT BUDGET	CURRENT PERIOD	PRIOR YEAR PO ADJUST.	Y-T-D BALANCE	TOTAL ENCUMBERED	BUDGET BALANCE	% OF BUDGET
PERSONAL SERVICES							
401-510-103-0000 Salaries & Wages	100,960	6,432.64	0.00	95,211.45	0.00	5,748.55	94.31
401-510-104-0000 FICA Tax	8,430	517.72	0.00	7,649.00	0.00	781.00	90.74
401-510-105-0000 Group Health Insurance	17,866	1,131.37	0.00	14,017.79	0.00	3,848.21	78.46
401-510-106-0000 Retirement	9,070	621.26	0.00	8,424.85	0.00	645.15	92.89
401-510-108-0000 Overtime/Extra Help	9,250	485.99	0.00	6,676.60	0.00	2,573.40	72.18
TOTAL PERSONAL SERVICES	145,576	9,188.98	0.00	131,979.69	0.00	13,596.31	90.66
TOTAL CSO-OTHER	145,576	9,188.98	0.00	131,979.69	0.00	13,596.31	90.66

401-SEWER FUND
SEWER COLLECTION

% OF YEAR COMPLETED: 100.00

EXPENDITURES	CURRENT BUDGET	CURRENT PERIOD	PRIOR YEAR PO ADJUST.	Y-T-D BALANCE	TOTAL ENCUMBERED	BUDGET BALANCE	% OF BUDGET
PERSONAL SERVICES							
401-511-103-0000 Salaries & Wages	100,960	6,432.70	0.00	95,212.50	0.00	5,747.50	94.31
401-511-104-0000 FICA Tax	8,430	517.68	0.00	7,648.78	0.00	781.22	90.73
401-511-105-0000 Group Health Insurance	17,866	1,459.49	0.00	17,004.43	0.00	861.57	95.18
401-511-106-0000 Retirement	9,070	621.26	0.00	8,424.93	0.00	645.07	92.89
401-511-108-0000 Overtime/Extra Help	9,250	486.04	0.00	6,677.01	0.00	2,572.99	72.18
TOTAL PERSONAL SERVICES	145,576	9,517.17	0.00	134,967.65	0.00	10,608.35	92.71
CONTRACTUAL SERVICES							
401-511-211-0000 Telephone	3,000	224.04	0.00	2,617.26	0.00	382.74	87.24
401-511-213-0000 Utilities/Purchased Pow	100,000	240.02	0.00	95,811.13	0.00	4,188.87	95.81
401-511-214-0000 Travel	1,000	0.00	0.00	0.00	0.00	1,000.00	0.00
401-511-215-0002 Stormwater Supplies	10,000	0.00	0.00	1,206.36	0.00	8,793.64	12.06
401-511-216-0000 Maint Pumping Equipment	15,000	0.00	0.00	20,653.37	0.00	(5,653.37)	137.69
401-511-216-0001 Maint Structures/Improv	32,670	0.00	0.00	10,033.09	0.00	22,636.41	30.71
401-511-217-0000 Maint Repair Autos & T	15,000	0.00	0.00	23,953.11	0.00	(8,953.11)	159.69
401-511-221-0000 Training & Education	1,500	0.00	0.00	0.00	0.00	1,500.00	0.00
401-511-222-0000 Dues & Subscriptions	0	0.00	0.00	2,600.58	0.00	(2,600.58)	0.00
401-511-230-0000 Contracted Services	2,000	0.00	0.00	20,341.27	0.00	(18,341.27)	1,017.06
401-511-240-0000 Refunds & Reimbursement	2,000	0.00	0.00	3,493.65	0.00	(1,493.65)	174.68
TOTAL CONTRACTUAL SERVICES	182,170	464.06	0.00	180,709.82	0.00	1,459.68	99.20
COMMODITIES							
401-511-341-0000 Supplies & Materials	50,000	0.00	0.00	33,990.28	0.00	16,009.72	67.98
401-511-343-0000 Automobile Supplies	20,000	0.00	0.00	16,910.20	0.00	3,089.80	84.55
401-511-345-0000 Uniforms	5,200	0.00	0.00	4,291.12	0.00	908.88	82.52
401-511-399-0000 Miscellaneous	16,500	0.00	0.00	7,345.48	0.00	9,154.52	44.52
TOTAL COMMODITIES	91,700	0.00	0.00	62,537.08	0.00	29,162.92	68.20
CAPITAL OUTLAY							
401-511-458-0000 Bond Payable S-1-09-A-R	33,965	2,830.41	0.00	33,964.92	0.00	0.08	100.00
401-511-458-0001 Bond Payable S-1-15-A-R	87,233	7,269.39	0.00	87,232.68	0.00	0.32	100.00
401-511-458-0003 Bond Payable S-1-20-A-R	320,771	26,784.32	0.00	321,411.84	0.00	(640.84)	100.20
401-511-458-0004 Bond Payable S-2-20-A-R	31,442	2,620.15	0.00	31,441.80	0.00	0.20	100.00
401-511-459-0000 2018 Van & Sewera Camer	26,520	2,271.56	0.00	26,862.57	0.00	(342.57)	101.29
401-511-459-0001 2021 Ford F-150	6,758	563.16	0.00	6,757.92	0.00	0.08	100.00
401-511-459-0002 Capital Outlay	12,000	0.00	0.00	0.00	0.00	12,000.00	0.00
401-511-459-0003 900 ECO Cleaner	59,815	0.00	0.00	41,352.93	0.00	18,462.07	69.13
401-511-459-0004 Wastewater Garage	0	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL CAPITAL OUTLAY	578,504	42,338.99	0.00	549,024.66	0.00	29,479.34	94.90
OTHER EXPENDITURES							
401-511-670-0000 Interest & Penalties	3,220	97.62	0.00	1,567.59	0.00	1,652.41	48.68
TOTAL OTHER EXPENDITURES	3,220	97.62	0.00	1,567.59	0.00	1,652.41	48.68
TOTAL SEWER COLLECTION	1,001,170	52,417.84	0.00	928,806.80	0.00	72,362.70	92.77

401-SEWER FUND
SEWER TREATMENT

% OF YEAR COMPLETED: 100.00

EXPENDITURES	CURRENT BUDGET	CURRENT PERIOD	PRIOR YEAR PO ADJUST.	Y-T-D BALANCE	TOTAL ENCUMBERED	BUDGET BALANCE	% OF BUDGET
PERSONAL SERVICES							
401-512-103-0000 Salaries & Wages	278,380	18,141.49	0.00	241,331.16	0.00	37,048.84	86.69
401-512-104-0000 FICA Tax	22,445	1,446.26	0.00	18,887.67	0.00	3,557.33	84.15
401-512-105-0000 Group Health Insurance	54,580	3,427.11	0.00	42,538.88	0.00	12,041.12	77.94
401-512-106-0000 Retirement	23,850	1,622.03	0.00	21,361.52	0.00	2,488.48	89.57
401-512-108-0000 Overtime/Extra Help	15,000	1,141.06	0.00	10,468.26	0.00	4,531.74	69.79
TOTAL PERSONAL SERVICES	394,255	25,777.95	0.00	334,587.49	0.00	59,667.51	84.87
CONTRACTUAL SERVICES							
401-512-211-0000 Telephone	3,000	215.65	0.00	2,351.23	0.00	648.77	78.37
401-512-213-0000 Utilities/Purchased Pow	160,000	0.00	0.00	163,518.14	0.00	(3,518.14)	102.20
401-512-214-0000 Travel	3,000	0.00	0.00	1,643.85	0.00	1,356.15	54.80
401-512-215-0000 Maint of Bldgs & Ground	1,000	0.00	0.00	49.29	0.00	950.71	4.93
401-512-216-0000 Maint Treat/Disp System	60,000	2,409.00	0.00	12,007.88	0.00	47,992.12	20.01
401-512-216-0001 Maint Structures/Improv	26,000	0.00	0.00	12,874.47	0.00	13,125.53	49.52
401-512-217-0000 Maint Repair Autos & Tr	9,000	0.00	0.00	3,097.12	0.00	5,902.88	34.41
401-512-218-0000 Postage	80	0.00	0.00	85.26	0.00	(5.26)	106.58
401-512-220-0000 Advertising	0	0.00	0.00	521.62	0.00	(521.62)	0.00
401-512-221-0000 Training & Education	3,000	0.00	0.00	2,899.00	0.00	101.00	96.63
401-512-222-0000 Dues & Subscriptions	200	0.00	0.00	3,005.90	0.00	(2,805.90)	1,502.95
401-512-230-0000 Contracted Services	32,000	5,955.10	0.00	46,473.47	0.00	(14,473.47)	145.23
TOTAL CONTRACTUAL SERVICES	297,280	8,579.75	0.00	248,527.23	0.00	48,752.77	83.60
COMMODITIES							
401-512-341-0000 Supplies & Materials	12,000	304.23	0.00	25,814.21	0.00	(13,814.21)	215.12
401-512-341-0001 Supplies & Matls Chemic	28,000	0.00	0.00	29,457.80	0.00	(1,457.80)	105.21
401-512-341-0002 Purification Supplies	10,000	0.00	0.00	62.97	0.00	9,937.03	0.63
401-512-343-0000 Automobile Supplies	9,500	399.69	0.00	11,057.78	0.00	(1,557.78)	116.40
401-512-345-0000 Uniforms	5,200	0.00	0.00	4,350.00	0.00	850.00	83.65
401-512-399-0000 Miscellaneous	0	175.00	0.00	648.75	0.00	(648.75)	0.00
TOTAL COMMODITIES	64,700	878.92	0.00	71,391.51	0.00	(6,691.51)	110.34
CAPITAL OUTLAY							
401-512-459-0000 Bond Payable S-1-06-A-R	563,268	46,939.02	0.00	563,268.24	0.00	(0.24)	100.00
401-512-459-0001 Bond Payable S-1-86-B-R	12,962	1,080.16	0.00	12,961.92	0.00	0.08	100.00
401-512-459-0002 Ford F-350	6,639	553.21	0.00	6,638.52	0.00	0.48	99.99
401-512-459-0003 Sewer Areation Equipmen	6,770	0.00	0.00	6,744.51	0.00	25.49	99.62
401-512-459-0005 Capital Outlay	0	0.00	0.00	0.00	0.00	0.00	0.00
401-512-459-0006 CIP WTP Garage	0	0.00	0.00	29.16	0.00	(29.16)	0.00
TOTAL CAPITAL OUTLAY	589,639	48,572.39	0.00	589,642.35	0.00	(3.35)	100.00
OTHER EXPENDITURES							
401-512-670-0000 Interest & Penalties	100	0.00	0.00	18,487.87	0.00	(18,387.87)	8,487.87
TOTAL OTHER EXPENDITURES	100	0.00	0.00	18,487.87	0.00	(18,387.87)	8,487.87
TOTAL SEWER TREATMENT	1,345,974	83,809.01	0.00	1,262,636.45	0.00	83,337.55	93.81

401-SEWER FUND
UTILITY BILLING

% OF YEAR COMPLETED: 100.00

EXPENDITURES	CURRENT BUDGET	CURRENT PERIOD	PRIOR YEAR PO ADJUST.	Y-T-D BALANCE	TOTAL ENCUMBERED	BUDGET BALANCE	% OF BUDGET
PERSONAL SERVICES							
401-513-103-0000 Salaries & Wages	17,300	940.77	0.00	18,068.24	0.00	(768.24)	104.44
401-513-104-0000 FICA Tax	1,350	67.49	0.00	1,304.95	0.00	45.05	96.66
401-513-105-0000 Group Health Insurance	3,900	295.72	0.00	3,548.65	0.00	351.35	90.99
401-513-106-0000 Retirement	1,580	85.95	0.00	1,587.72	0.00	(7.72)	100.49
401-513-108-0000 Overtime/ Extra Help	280	14.19	0.00	191.59	0.00	88.41	68.43
TOTAL PERSONAL SERVICES	24,410	1,404.12	0.00	24,701.15	0.00	(291.15)	101.19
CONTRACTUAL SERVICES							
401-513-214-0000 Travel	200	0.00	0.00	0.00	0.00	200.00	0.00
TOTAL CONTRACTUAL SERVICES	200	0.00	0.00	0.00	0.00	200.00	0.00
COMMODITIES							
401-513-341-0000 Supplies & Materials	4,000	0.00	0.00	2,006.16	0.00	1,993.84	50.15
TOTAL COMMODITIES	4,000	0.00	0.00	2,006.16	0.00	1,993.84	50.15
TOTAL UTILITY BILLING	28,610	1,404.12	0.00	26,707.31	0.00	1,902.69	93.35

401-SEWER FUND
ADMIN & GENERAL

% OF YEAR COMPLETED: 100.00

EXPENDITURES	CURRENT BUDGET	CURRENT PERIOD	PRIOR YEAR PO ADJUST.	Y-T-D BALANCE	TOTAL ENCUMBERED	BUDGET BALANCE	% OF BUDGET
PERSONAL SERVICES							
401-514-103-0000 Salaries & Wages	1,800	325.00	0.00	2,725.00	0.00	(925.00)	151.39
401-514-104-0000 FICA Tax	140	24.79	0.00	208.24	0.00	(68.24)	148.74
401-514-105-0000 Group Health Insurance	0	56.05	0.00	774.07	0.00	(774.07)	0.00
401-514-106-0000 Retirement	0	9.00	0.00	36.00	0.00	(36.00)	0.00
401-514-108-0000 Overtime/Extra Help	0	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL PERSONAL SERVICES	1,940	414.84	0.00	3,743.31	0.00	(1,803.31)	192.95
CONTRACTUAL SERVICES							
401-514-218-0000 Postage	8,000	728.64	0.00	9,103.01	0.00	(1,103.01)	113.79
401-514-220-0000 Advertising	0	0.00	0.00	338.16	0.00	(338.16)	0.00
401-514-223-0000 Professional Services	10,000	4,004.76	0.00	96,731.50	0.00	(86,731.50)	967.32
401-514-226-0000 Insurance & Bonds	12,000	0.00	0.00	9,009.28	0.00	2,990.72	75.08
401-514-226-0001 Insurances & Bonds/GL	30,000	0.00	0.00	37,287.68	0.00	(7,287.68)	124.29
401-514-230-0000 Contracted Services	15,000	94.50	0.00	10,457.53	0.00	4,542.47	69.72
401-514-230-0001 Cont Serv/Consent Decre	0	0.00	0.00	0.00	0.00	0.00	0.00
401-514-232-0000 Bank Charges	50	25.70	0.00	78.70	0.00	(28.70)	157.40
TOTAL CONTRACTUAL SERVICES	75,050	4,853.60	0.00	163,005.86	0.00	(87,955.86)	217.20
COMMODITIES							
401-514-341-0000 Supplies & Materials	0	1,414.65	0.00	2,369.25	0.00	(2,369.25)	0.00
401-514-348-0000 Charges by Other Funds	41,022	3,159.25	0.00	37,911.00	0.00	3,111.00	92.42
401-514-353-0000 Computer Software	12,000	0.00	0.00	13,991.99	0.00	(1,991.99)	116.60
401-514-399-0000 Miscellaneous Expenses	1,000	157.97	0.00	1,083.65	0.00	(83.65)	108.37
TOTAL COMMODITIES	54,022	4,731.87	0.00	55,355.89	0.00	(1,333.89)	102.47
CAPITAL OUTLAY							
401-514-465-0000 Depreciation Expense	0	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL CAPITAL OUTLAY	0	0.00	0.00	0.00	0.00	0.00	0.00
OTHER EXPENDITURES							
401-514-568-0000 Transfers	0	0.00	0.00	0.00	0.00	0.00	0.00
401-514-670-0000 Interest & Penalties	200	0.00	0.00	0.00	0.00	200.00	0.00
401-514-676-0000 Regulatory Commission	12,000	0.00	0.00	11,053.45	0.00	946.55	92.11
401-514-677-0000 R & R Requirement	71,000	0.00	0.00	64,576.39	0.00	6,423.61	90.95
401-514-677-0001 SB234 Requirement	174,000	0.00	0.00	144,692.68	0.00	29,307.32	83.16
TOTAL OTHER EXPENDITURES	257,200	0.00	0.00	220,322.52	0.00	36,877.48	85.66
TOTAL ADMIN & GENERAL	388,212	10,000.31	0.00	442,427.58	0.00	(54,215.58)	113.97

401-SEWER FUND
CAPITAL OUTLAY

% OF YEAR COMPLETED: 100.00

EXPENDITURES	CURRENT BUDGET	CURRENT PERIOD	PRIOR YEAR PO ADJUST.	Y-T-D BALANCE	TOTAL ENCUMBERED	BUDGET BALANCE	% OF BUDGET
CONTRACTUAL SERVICES							
401-515-216-0000 Depreciation Acc Mtn Tr	0	0.00	0.00	75,662.75	0.00	(75,662.75)	0.00
401-515-216-0001 Depreciation Acct Mnt/	0	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL CONTRACTUAL SERVICES	0	0.00	0.00	75,662.75	0.00	(75,662.75)	0.00
TOTAL CAPITAL OUTLAY	0	0.00	0.00	75,662.75	0.00	(75,662.75)	0.00
TOTAL EXPENDITURES	2,960,000	159,089.67	0.00	2,904,034.69	0.00	55,965.31	98.11
REVENUE OVER/(UNDER) EXPENDITURES	0	93,175.10	0.00	(46,969.75)	0.00	46,969.75	0.00

CITY OF ELKINS
AGENDA ITEM REPORT

Meeting Date:	July 15, 2024
Section:	New business
Category:	Action Item
Agenda Item Name:	Approval of Sewer Invoices
Recommended By:	Whitney L Hymes - Wastewater Superintendent/Cheif Operator
Summary:	Crim Law invoice #438 =$1,160.00
Fiscal Impact:	Total = $1,160.00
Recommendation:	Consider for Approval
Attachments:	1. 2024-07-01 City of Elkins (Sanitary Bd - June)

City of Elkins

June 2024

Sanitary Board Matters

Crim Law Office, PLLC
842 South Chestnut Street
Post Office Drawer 1920
Clarksburg, West Virginia 26302-1920
Phone: (304)918-1001
Fax: (304)918-1005
www.wvlawyers.com

City of Elkins - Sanitary Board
401 Davis Street
Elkins, WV 26241

Invoice

Invoice Number	438
Invoice Date	07/01/2024
Payment Due On	07/15/2024
Amount Due	**$1,160.00**

City of Elkins - Sanitary Board - Municipality

Fees

Date	Description	Staff	Rate	Hours	Total
06/05/2024	Email from Attorney Carroll	GSR	$100.00	0.10	$10.00
06/05/2024	Review of information for furnishing documents	GSR	$100.00	0.60	$60.00
06/05/2024	Detailed email from Mayor Marco	GSR	$100.00	0.20	$20.00
06/06/2024	Review of information from Attorney Carroll	GSR	$100.00	0.40	$40.00
06/06/2024	Conference with Attorney Carroll	GSR	$100.00	0.50	$50.00
06/06/2024	Email from W. Hymes	GSR	$100.00	0.10	$10.00
06/07/2024	Email to W. Hymes	GSR	$100.00	0.10	$10.00
06/07/2024	Conference concerning litigation and review of documents	GSR	$100.00	0.80	$80.00
06/07/2024	Email to Attorney Carroll	GSR	$100.00	0.10	$10.00
06/07/2024	Email from Attorney Carroll	GSR	$100.00	0.10	$10.00
06/07/2024	Email from W. Hymes	GSR	$100.00	0.10	$10.00
06/10/2024	Email to Attorney Carroll and conference with him	GSR	$100.00	0.50	$50.00
06/10/2024	Review of sewer line extension agreement for UHC and conference with Attorney Judy	GSR	$100.00	0.90	$90.00
06/10/2024	Email to W. Hymes	GSR	$100.00	0.10	$10.00
06/10/2024	Conference with Mayor about work experience program	GSR	$100.00	0.40	$40.00

06/10/2024	Email from Mayor Marco	GSR	$100.00	0.10	$10.00
06/12/2024	Email from W. Hymes about agreement	GSR	$100.00	0.10	$10.00
06/12/2024	Email to Mayor and W. Hymes about reimbursement program and review of information	GSR	$100.00	0.50	$50.00
06/14/2024	Email from W. Hymes about agreement	GSR	$100.00	0.10	$10.00
06/14/2024	Review of draft discovery responses and email from Attorney Carroll	GSR	$100.00	0.60	$60.00
06/14/2024	Email from W. Hymes about responses	GSR	$100.00	0.10	$10.00
06/14/2024	Email from W. Hymes about meeting	GSR	$100.00	0.10	$10.00
06/14/2024	Email to W. Hymes about meeting	GSR	$100.00	0.10	$10.00
06/14/2024	Review of information from W. Hymes about 312 S. Randolph Avenue	GSR	$100.00	0.70	$70.00
06/14/2024	Review of final version of discovery responses	GSR	$100.00	0.40	$40.00
06/17/2024	Receive and review various emails concerning 312 South Randolph Avenue	GSR	$100.00	0.70	$70.00
06/18/2024	Receive and review updated information on 312 S. Randolph Avenue	GSR	$100.00	0.50	$50.00
06/18/2024	Review of information from Attorney Carroll and conference concerning the same	GSR	$100.00	0.60	$60.00
06/18/2024	Email from Attorney Benincosa	GSR	$100.00	0.20	$20.00
06/18/2024	Email from W. Hymes	GSR	$100.00	0.10	$10.00
06/24/2024	Review of documents from Attorney Carroll	GSR	$100.00	0.50	$50.00
06/24/2024	Receive and review agreement from Attorney Judy	GSR	$100.00	0.40	$40.00
06/25/2024	Email to Attorney Judy from W. Hymes	GSR	$100.00	0.10	$10.00
06/25/2024	Email to Attorney Judy	GSR	$100.00	0.10	$10.00
06/25/2024	Review of information and conference with Attorney Carroll	GSR	$100.00	0.60	$60.00
					$1,160.00

Subtotal	**$1,160.00**
Total	**$1,160.00**
Total Balance Due	**$1,160.00**

Approved/Reviewed By Whitney Hymes (WWTP Superintendent/Chief Operator) on 07/02/2024

Whitney L. Hymes

CITY OF ELKINS
AGENDA ITEM REPORT

<table>
<tr><td>Meeting Date:</td><td>July 15, 2024</td></tr>
<tr><td>Section:</td><td>New business</td></tr>
<tr><td>Category:</td><td>Action Item</td></tr>
<tr><td>Agenda Item Name:</td><td>Consideration of BIDS for the Vacuum Truck Dumping Station</td></tr>
<tr><td>Recommended By:</td><td>Whitney L. Hymes - Wastewater Superitendent/Cheif Operator</td></tr>
<tr><td>Summary:</td><td>Bid Opening was held on July 10, 2024 at 3:00pm</td></tr>
<tr><td>Fiscal Impact:</td><td>Hulls’ Contracting Inc.
Total BID: $268,500.00
Deductive Alternative #1: $5,000
Deductive Alternative #2: $60,000
Green River Group, LLC
Total BID: $392,000
Deductive Alternative #1: $15,000
Deductive Alternative #2: $62,000
Polino Contracting, Inc
Total BID: $396,921.00
Deductive Alternative #1: $12,517.00
Deductive Alternative #2: $58,240.00</td></tr>
<tr><td>Recommendation:</td><td>Consider for Approval</td></tr>
<tr><td>Attachments:</td><td>1. 240710 Elkins Vacuum Truck Dumping Station (342-544)</td></tr>
</table>

BID TABULATION

CITY OF ELKINS
RANDOLPH COUNTY, WEST VIRGINIA

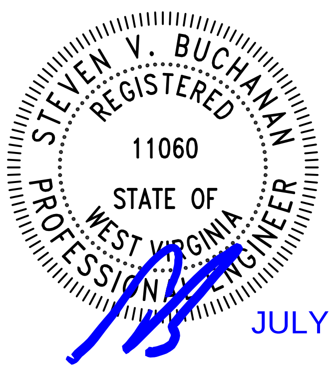
VACUUM TRUCK DUMPING STATION

CEC PROJECT 342-544

Civil & Environmental Consultants, Inc.

3:00 PM, WEDNESDAY, JULY 10, 2024

BIDDER	TOTAL BID	DEDUCTIVE ALTERNATE #1	DEDUCTIVE ALTERNATE #2
Hulls' Contracting Inc.	$268,500.00	$5,000.00	$60,000.00
Green River Group, LLC	$392,000.00	$15,000.00	$62,000.00
Polino Contracting, Inc.	$396,921.00	$12,517.00	$58,240.00



JULY 10, 2024

CITY OF ELKINS
AGENDA ITEM REPORT

Meeting Date:	July 15, 2024
Section:	New business
Category:	Action Item
Agenda Item Name:	Cybersecurity Policy for Sanitary Department
Recommended By:	Whitney L. Hymes - Wastewater Superintendent/ Cheif Operator
Summary:	This proposed Cybersecurity policy is a living changing document created for the purpose of establishing guidelines for the City of Elkins computer security while offering protection of the organization's networks and its content or knowledge base, and to minimize the risk of internal and external cyber threats. This policy was created due to the implementation of PSC Rule 5.16.24 [GENERAL INVESTIGATION INTO CYBERSECURITY OF WATER AND SEWER UTILITIES] *See Attachment* CASE NO. 24-0460-PWD-W-GI CASE NO. 24-0461-PSD-S-GI Attachment B was submitted July 10, 2024
Fiscal Impact:	N/A
Recommendation:	Consider for Approval
Attachments:	1. CYBERSECURITY POLICY AND PROCEDURES Draft 2 2. Cybersecurity Order 5.16.24

CYBERSECURITY POLICY AND PROCEDURES

1. **Purpose:**

The purpose of this policy is to establish the City of Elkins guidelines for computer security and protection of an organization's networks and its content or knowledge base, and to minimize the risk of internal and external cyber threats.

2. **Scope:**

This policy applies to all City elected officials, appointed officials, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by the City of Elkins.

3. **Policy:**

The City of Elkins is committed to building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. In order to achieve this, the City will identify, evaluate, and take steps to avoid or mitigate risk to the City's information assets and prevent unauthorized digital or physical access, damage, theft, compromise, or interference to the City's information systems and facilities. These steps include implementing and operating controls to manage the City's information security risks and ensuring that all users of information assets are aware of their responsibilities in protecting those assets while complying with all applicable federal, state, or other regulations

4. Responsibilities

Roles and responsibilities must be separated so that a single individual, account, or function cannot intentionally or unintentionally subvert a critical process. Controls must also be put in place so that no single person can access, modify, or use assets without authorization or detection. Achieving and maintaining cybersecurity is a shared responsibility. Information Technology Manager, once appointed, will ensure that a written Cybersecurity Policy is implemented, reviewed and updated on a periodic basis; including providing training and updates to City staff; confirm identification, acquisition, and implementation of information system software and hardware; identify locations where Personally Identifiable Information (PII) is stored and accessible; provide input for who should have access to PII and with what types of privileges or access rights, performing periodic classification assessments and ensuring regular reviews to update and manage changes to risk; assess system vulnerabilities and implement security tools and safeguards for protecting PII; ensure implementation, enforcement, and effectiveness of IT Security policies and procedures; plan, execute, and lead security audits across the City; facilitate an understanding and awareness that security requires participation and support at all organizational levels; and oversee daily activities and use of information systems to ensure employees, business partners, and contractors adhere to these policies and procedures. Under the direction of the IT Manager, once appointed, the Information Technology Administrator will help implement and enforce the items outlined in this policy. They will manage logs and events of all systems, and conducting periodic reviews to ensure our cybersecurity. All users, including employees, elected officials, appointed officials, contractors, must comply with all aspects of this policy. Users are responsible for the acceptable use and security of infrastructure and data.

5. Standards:

5.1 Asset Management

An inventory of all approved hardware and software on the City's network and systems will be maintained that documents the following:

- The employee in possession of the hardware or software
- Date of purchase
- Serial number
- Type of device and description (OS, Processor type, RAM, Manufacture, etc.)
- For licensed software: # of licenses, license renewal date(s), other restrictions, etc.

5.2 Personally Identifiable Information (PII)

An inventory of all current PII information by type and location will be maintained. The following table will be used to inventory PII.

Location	**PII by type**	**Essential**	**Location**	**Owner**
Website				
Contractors				
File in a staff office				
File in building				
File offsite				
Desktop				
HR System				
Financial System				
Laptop				
Flash drive				
Cell phones				
Tablets				
Other				

With the exception of the Police Department who have their own records retention policy, each manager will determine if PII being collected by their department is essential. If PII is not essential, it will either not be collected, or (if collected) will be destroyed per West Virginia's records retention schedule and as per City policy and procedures. The City will not collect sensitive information, such as Social Security numbers if there is no legitimate business need.

The West Virginia Identity Theft Protection Act, **West Virginia Code Section 61-3-54** prohibits anyone (individual, private or public corporation, or business) who maintains Social Security numbers from:

- Printing a consumer's SSN on any mailed materials not requested by the consumer unless redacted
- Printing a consumer's SSN on a card used by the consumer that is required to access products or services
- Publicly posting or displaying a consumer's SSN, such as on a website

Exceptions include requirements by state or federal laws, including statute records (such as W2s, W4s, 1099s, etc.) that are required by law to be made available to the public for use for internal verification or administrative processes, or for enforcing a judgment or court order

5.3 Identity Management, Authentication and Access Control

Information Technology Manager, once appointed, is responsible for ensuring that access to the City's systems and data is appropriately controlled. All systems housing City data (including laptops, desktops, tablets, and cell phones) are required to be protected with a password or other form of authentication. Except for the instances noted in this policy, users with access to the City systems and data shall not share passwords with anyone.

The City has established the following password configuration requirements for all systems and applications (where applicable):

- Minimum password length: minimum 10 characters using number, sign, upper and lower case letters.
- Password complexity: use a passphrase rather than a password
- Prohibited reuse for six (6) iterations
- PIN"S no less than 6 characters.
- Changed periodically (every 180 days)
- Invalid login attempts set to lock after three Employees are encouraged to follow further safeguards such as:
- Not allowing PII on mobile storage media
- Utilizing Locking file cabinets
- Not allowing PII left on desktops
- Encrypting sensitive files on computers
- Requiring password protection
- Enabling multi-factor authentication
- Following the record retention plan and destroying records no longer required Where possible, multi-factor authentication will be used when users authenticate to the City's systems.
- Users are granted access only to the system data and functionality necessary for their job responsibilities.
- Privileged and administrative access is limited to authorized users who require escalated access for their job responsibilities and where possible will have two accounts: one for administrator functions and a standard account for day-to-day activities.
- Once appointed, all user access requests must be approved by the Information Technology Manager.

• Once appointed, the Information Technology Manager shall make sure all system access is removed of all users who separate from the City within 48 hours.

On an annual basis, a review of user access will be conducted by the departments under the direction of the Information Technology Manager, once appointed, to confirm compliance with the access control policies outlined above.

5.4 Awareness and Training

City staff are required to complete City assigned security training:

1. Upon hire and within 30 days of receiving login credentials
2. Annually

On an annual basis, the IT Manager, once appointed, will conduct email phishing exercises of its users. The purpose of these tests is to help educate users on common phishing scenarios. It will assess the level of awareness and comprehension of phishing, understanding, and compliance with policy around safe handling of emails containing links and/or attachments, and the ability to recognize a questionable or fraudulent message.

5.5 Data Security

5.5.1 Data Classification

Users must adhere to the Records Retention Policy regarding the storage and destruction of data. Data residing on City's systems must be continually evaluated and classified into the following categories:

• Users' Personal Use: Includes individual user's personal data, emails, documents, etc. This policy does not apply to a user's personal information.

• Marketing or Informational Material: Includes already-released marketing material, commonly known information, data freely available to the public, etc. and this policy does not apply

. • Operational: Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.

• Confidential: Any information deemed confidential. The following list provides guidelines on what type of information is typically considered confidential. Confidential data may include:

- Employee or customer Social Security numbers or personally identifiable information (PII)

- Personnel files o Protected Health Information (PHI)
- Network diagrams and security configurations
- Privileged communications regarding legal matters.
- Passwords/passphrases o Bank account information and routing numbers
- Payroll information o Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

5.5.2 Data Storage

The following guidelines apply to storage of the different types of organizational data

. • Operational: Operational data should be stored on a server that gets the most frequent backups. Some type of system- or disk-level redundancy is encouraged.

• Confidential: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard or code secured. No thumb drive, external hard drives will be left in unsecured areas where the ability for others to have access or ability to transport data.

5.5.3 Data Transmission

The following guidelines apply to the transmission of the different types of organizational data. •

Confidential: Confidential data shall not be 1) Transmitted outside the City’s network without the use of strong encryption 2) Left on voicemail systems, either inside or outside the organization's network. 3) Transmitted via email, outside of the organization’s network. 4) Placed on external storage devices for the purpose of transmission outside our network.

Data while transmitted, includes any data sent across the City’s network or any data sent to or from a City-owned or City-provided system. Types of transmitted data that shall be encrypted include:

• VPN tunnels

• Remote access sessions

• Web applications • Email and email attachments

• Remote desktop access

• Communications with applications/databases

5.5.4 Data Destruction

Employees must follow State's and City's records retention policy and procedures before destroying any data.

• Confidential: Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply to data located on City-owned or City-provided systems, devices, media, etc.:

- Storage media (CD's, DVD's, storage devices): Physical destruction is required, some shredders may be able to perform this function.
- Hard drives/systems/mobile storage media: At a minimum, DoD three (3) pass data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the City shall use the most secure commercially available methods for data wiping. Alternatively, the City may physically destroy the storage media.

5.5.5 Data Storage

Stored Data includes any data located on City-owned or City-provided systems, devices, media, etc.

Examples of encryption options for stored data include:

• Whole disk encryption • Encryption of partitions/files

• Encryption of disk drives

• Encryption of personal storage media/USB drives

• Encryption of backups

• Encryption of data generated by applications

6. Information Protection Processes and Procedures:

6.1 Secure Software Development

Where applicable, all software development activities performed by City or by vendors on behalf of the organization shall employ secure coding practices including those outlined below.

A minimum of 2 software environments for the development of software systems should be available – development/training and a production environment. Software developers or programmers are required to develop in the development/training environment and promote objects into the production environments. The development/training environment is used for assurance testing by the end-user and the developer. The production environment should be used solely by the end-user for production data and applications. Compiling objects and the source code is not allowed in the production environment.

6.2 Contingency Planning

The City's business contingency capability is based upon cloud and local backups of all critical business data. This critical data is defined as "the data that is critical to successful organization operation". Full data backups will be performed on a daily basis. Confirmation that backups were performed successfully will be conducted daily. Testing of cloud backups and restoration capability will be performed on a monthly basis.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the Information Technology Manager.

The following are some examples of possible business contingency scenario procedures:

• In the event that one or more of City 's systems or applications are deemed corrupted or inaccessible, the Information Technology Manager, once appointed, will work with the respective vendor(s) to restore data from the most recent cloud and local backup and, if necessary, acquire replacement hardware.

• In the event that the location housing the City systems are no longer accessible, the Information Technology Manager, once appointed, will work with the respective vendor(s) to acquire any necessary replacement hardware and software, implement these at one of the City's other sites, and restore data from the most recent cloud, off-site, or local backup.

6.3 Network Infrastructure

The City will protect its electronic communications network from the Internet by utilizing a firewall. For maximum protection, the network devices shall meet the following configuration standards:

• Vendor recommended, and industry standard configurations will be used.

• Changes to firewall and router configuration will be approved by Information Technology Manager

. • Both router and firewall passwords shall be secured and difficult to guess.

• The default policy for the firewall for handling inbound traffic shall be to block all packets and connections unless the traffic type and connections have been specifically permitted.

• Inbound traffic containing ICMP (Internet Control Message Protocol) traffic shall not be passed in from the Internet, or from any un-trusted external network.

• All web services running on routers shall be disabled.

• Simple Network Management Protocol (SNMP) Community Strings shall be made (changed from the default "public") "private".

6.4 Network Servers

Servers typically accept connections from several sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk associated with that system, so it is particularly important to secure network servers.

• Unnecessary files, services, and ports shall be removed or blocked. If possible, a server hardening guide, which is available from the leading operating system manufacturers, shall be followed.

• Network servers, even those meant to accept public connections, shall be protected by a firewall or access control list.

• When possible, a standard installation process shall be developed for the City's network servers. A standard process will provide consistency across servers no matter which employee or contractor handles the installation.

• Clocks on network servers shall be synchronized with the City's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

6.5 Network Segmentation

Network segmentation is used to limit access to data within the City network based upon data sensitivity. The City maintains two wireless networks. The guest/public wireless network will grant the user internet access only. Access to the secure wireless network is limited to the City staff and devices, and provides the user access to the intranet.

Under the direction of the Information Technology Manager, a third-party network administrator manages the network, monitors firewall logs, and operating system event logs. The Information Technology Manager authorizes vendor access to the system components as required for maintenance.

7. Protective Technology:

7.1 Email Filtering

The City shall filter email, at a minimum of, the Internet gateway and/or the mail server. This filtering will help reduce spam, viruses, or other messages that may be deemed either contrary to this policy or a potential risk to the City's IT security.

Additionally, email or anti-malware programs may be implemented to identify and quarantine emails that are deemed suspicious.

7.2 Internet Filtering

The IT Department, once established, shall block access to internet websites and protocols that are deemed inappropriate or pose a security risk. Some examples of blocked categories are adult/sexually explicit material, advertisements, hacking, violence and hate content.

7.3 Network Vulnerability Assessments

On a quarterly basis, the IT Department, once established, will perform both internal and external network vulnerability assessments. The purpose of these assessments is to establish a comprehensive view of the organization’s network as it appears internally and externally. These evaluations will be conducted under the direction of Information Technology Manager to identify weaknesses with the network configuration that could allow unauthorized and/or unsuspected access to the organization's data and systems.

In addition, annual penetration testing will be run to identify weaknesses or vulnerabilities that will need to be addressed.

8. Anomalies and Events:

The following logging activities are conducted by IT System Administrator/ Information Technology Manager, once appointed:

• Domain Controllers - Active Directory event logs will be configured to log the following security events: account creation, escalation of privileges, login failures, and excessive repeated login attempts.

• Application Servers - Logs from application servers (e.g., web, email, database servers) will be configured to log the following events: errors, faults, login failures, and excessive repeated login attempts.

• Network Devices - Logs from network devices (e.g., firewalls, network switches, routers) will be configured to log the following events: errors, faults, login failures, and excessive repeated login attempts.

Passwords should not be contained in logs. Passwords displayed on posted notes or that are visible to other individuals is strictly prohibited.

Logs of the above events will be reviewed by the IT System Administrator, utilizing a SIEM (Security Information and Event Management), at least once per month. Event logs will be configured to maintain record of the above events for at least three months.

9. Security Continuous Monitoring:

9.1 Anti-Malware Tools

All City servers and workstations shall utilize endpoint protection software to protect systems from malware and viruses. Real-time scanning will be enabled on all systems and weekly malware scans will be performed. A monthly review of the endpoint protection software dashboard will be conducted by IT System Manager, once appoined to confirm the status of virus definition updates and scans.

9.2 Patch management

All software updates and patches will be distributed to all City systems as follows:

• Workstations shall be configured to install software updates every night automatically.

• Server software updates shall be manually installed at least quarterly

. • Any exceptions shall be documented.

10. Response Planning

The City's annual security awareness training shall include direction and guidance for the types of security incidents users could encounter, what actions to take when an incident is suspected, and who is responsible for responding to an incident. A security incident, as it relates to the City's information assets, can be defined as either an Electronic or Physical Incident.

Information Technology Manager, once appointed, is responsible for coordinating all activities during a significant incident, including notification and communication activities and the chain of escalation and deciding if/when outside agencies, need to be contacted.

10. Electronic Incidents:

10.1 This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes to a virus outbreak or a suspected Trojan or malware infection. When an electronic incident is suspected, the steps below should be taken in order.

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.

2. Once appointed, report the incident to the IT System Administrator or Information Technology Manager.

3. Contact the third-party service provider (and/or computer forensic specialist) as needed. The remaining steps should be conducted with the assistance of the third-party IT service provider and/or computer forensics specialist.

4. Disable the compromised account(s) as appropriate.

5. Backup all data and logs on the machine, or copy/image the machine to another system.

6. Determine exactly what happened and the scope of the incident.

7. Determine how the attacker gained access and disable it.

8. Rebuild the system, including a complete operating system reinstall.

9. Restore any needed data from the last known good backup and put the system back online.

10. Take actions, as possible, to ensure that the vulnerability will not reappear.

11. Conduct a post-incident evaluation. What can be learned? What could be done differently?

10.2 Physical Incidents

A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain City's information. All instances of a suspected physical security incident should be reported immediately to the IT System Administrator or Information Technology Manager once appointed.

10.3 Notification

If an electronic or physical security incident is suspected of having resulted in the loss of, or unauthorized access to employee PPI or third-party/customer data, notify the City Attorney's office for direction on procedures for notification of the public or affected entities as well as necessary government agencies.

11. Recovery & Restoration:

Recovery processes and procedures shall be executed and maintained to ensure timely restoration of systems and/or assets affected by cybersecurity events.

Information Technology Manager, once appointed, is responsible for managing and directing activities during an incident, including the recovery steps.

Recovery planning and processes are improved by incorporating lessons learned into future activities.

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet service providers, owners of the affected systems, victims, and vendors.

External communications should only be handled by designated individuals at the direction of the City Administrator. Recovery activities are communicated to internal stakeholders, executives, and management teams.

12. References:

West Virginia Administrative

West Virginia Revised Code Records, public reports and meetings West Virginia Identity Theft Protection Act

City of Elkins HR Rules City of Elkins Use of City Information Technology Policy & Procedures

City of Elkins Social Media Policy and Procedures

13. Review of Policy and Procedures:

This policy will be reviewed annually or as state and federal regulations are revised and necessitate a change in the policy or procedures.

Adopted: July 2024 Appendix B –

Confidentiality and Non-Disclosure Agreement This Confidentiality and Nondisclosure Agreement (the "Agreement") is entered into by and between City of Elkins ("Disclosing Party") and ________________________ ("Receiving Party") for the purpose of preventing the unauthorized disclosure of Confidential Information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and confidential information ("Confidential Information").

1. Definition of Confidential Information. For purposes of this Agreement, "Confidential Information" shall include all information or material that has or could have commercial value or other utility in the business in which Disclosing Party is engaged. Examples of Confidential Information include the following:

   - Employee or customer Social Security numbers or personal information
   - Customer data • Entity financial data
   - Product and/or service plans, details, and schematics,
   - Network diagrams and security configurations
   - Communications about entity legal matters
   - Password
   - Bank account information and routing numbers
   - Payroll information
   - Credit card information

- Any confidential data held for a third party

2. Exclusions from Confidential Information. Receiving Party's obligations under this Agreement do not extend to information that is:
(a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party;
(b) discovered or created by the Receiving Party before disclosure by Disclosing Party;
(c) learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or
(d) is disclosed by Receiving Party with Disclosing Party's prior written approval.

3. Obligations of Receiving Party. Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive benefit of the Disclosing Party. Receiving Party shall carefully restrict access to Confidential Information to employees, contractors, and third parties as is reasonably required and shall require those persons to sign nondisclosure restrictions that are at least as protective as those in this Agreement. Receiving Party shall not, without the prior written approval of Disclosing Party, use for Receiving Party's own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of Disclosing Party, any Confidential Information. Receiving Party shall return to Disclosing Party any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to Confidential Information immediately if Disclosing Party requests it in writing.

4. Time Periods. The nondisclosure provisions of this Agreement shall survive the termination of this Agreement and Receiving Party's duty to hold Confidential Information in confidence shall remain in effect until the Confidential Information no longer qualifies as a confidential or until Disclosing Party sends Receiving Party written notice releasing Receiving Party from this Agreement, whichever occurs first.

5. Relationships. Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venture or employee of the other party for any purpose.

6. Severability. If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as best to affect the intent of the parties.

7. Integration. This Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations, and understandings. This Agreement may not be amended except in a writing signed by both parties.

8. Waiver. The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights.

This Agreement and each party's obligations shall be binding on the representatives, assigns, and successors of such party. Each party has signed this Agreement through its authorized representative.

Disclosing Party

By: ________________________________

Printed Name: _____________________

Title: ______________________________

Dated: _____________________________

Receiving Party By: ________________________________

Printed Name: ______________________

Title: ______________________________

Dated: _____________________________

PUBLIC SERVICE COMMISSION
OF WEST VIRGINIA
CHARLESTON

At a session of the PUBLIC SERVICE COMMISSION OF WEST VIRGINIA in the City of Charleston on the 16th day of May 2024.

CASE NO. 24-0460-PWD-W-GI
CASE NO. 24-0461-PSD-S-GI

GENERAL INVESTIGATION INTO CYBERSECURITY
OF WATER AND SEWER UTILITIES

COMMISSION ORDER

The Commission opens a general investigation to examine water and sewer system cybersecurity.

DISCUSSION

The Public Service Commission was created by the Legislature for the purpose of exercising regulatory authority over public utilities to serve the interests of the public. Its function is to require such entities to perform in a manner designed to safeguard the interests of the public and the utilities.[1] Furthermore, the Commission may investigate all practices of public utilities in the State.[2]

The Commission has jurisdiction over water and sewer utilities in the State. Further, water and sewer utilities are required to "establish and maintain adequate and suitable facilities, safety appliances or other suitable devices, and shall perform such service in respect thereto as shall be reasonable, safe and sufficient for the security and convenience of the public."[3]

Cyberattacks against water and sewer utilities are increasing throughout the United States.[4] Cyberattacks threaten the distribution of clean and safe drinking water to the public. In addition, cyberattacks can create significant costs to the public and the affected utilities. Vulnerability to cyberattacks threatens water and sewer service at all levels.

---

[1] Boggs v. Public Serv. Comm'n, 154 W. Va. 146, 174 S.E.2d 331(1970).
[2] W. Va. Code § 24-2-2(a).
[3] W. Va. Code § 24-3-1.
[4] Alert (AA21-287A), Ongoing Cyber Threats to U.S. Water and Wastewater Systems, https://www.cisa.gov/uscert/ncas/alerts/aa21-287a.

Water and sewer utilities are key segments of our infrastructure. Thus, improving cybersecurity for water and sewer utilities is a high priority for the State. Therefore, the Commission will open this general investigation as a means to assess the vulnerability of water and sewer utilities under Commission jurisdiction to cyberattacks.

To initiate this process, the Commission will require all water and sewer utilities to obtain a cyber threat vulnerability assessment. While the Commission does not have specific requirements related to cyber threat vulnerability assessments, state law requires all water and sewer utilities to "maintain adequate and suitable facilities, safety appliances or other suitable devices, and shall perform such service in respect thereto as shall be reasonable, safe and sufficient for the security and convenience of the public."[5]

Moreover, a water or sewer system shall "inspect its plant and facilities in such manner and with such frequency as is necessary to ensure a reasonably complete knowledge as to conditions and adequacy at all times. Such inspections must comply with the legally applicable requirements of the Minimum Federal Safety Standards (Federal Occupational Safety and Health Administration) and the Bureau for Public Health and the Department of Environmental Protection."[6]

Pursuant to the National Primary Drinking Water Regulations,[7] states are required to conduct periodic sanitary surveys of public water utilities.[8] The Federal Environmental Protection Agency (EPA) interprets the regulations regarding sanitary surveys to include an evaluation of the adequacy of the cybersecurity of any operational technology used in the production and distribution of safe drinking water.[9] The West Virginia Bureau for Public Health and Department of Health, are the state agencies responsible for conducting sanitary surveys.[10]

Thus, to initiate this process, the Commission will require all water and sewer utilities to obtain a cybersecurity vulnerability assessment. To assist water and sewer utilities in this endeavor, the EPA[11] and the Department of Homeland

---

[5] W. Va. Code § 24-3-1.
[6] Rule 7.1.5 of the Commission's Rules for the Government of Sewer Utilities (Sewer Rules), 150 C.S.R. 5; Rule 7.1.2 of the Commission's Rules for the Government of Water Utilities (Water Rules), 150 C.S.R. 7.
[7] *See* 40 C.F.R. parts 141 and 142.
[8] *See*, *e.g.*, 40 C.F.R. part 142.16(b)(3).
[9] *See* "Evaluating Cybersecurity During Public Water System Sanitary Surveys," https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf.
[10] *See*, *e.g.*, Rule 6.1, Public Water Systems, 64 C.S.R. 3.
[11] *See* "Cybersecurity Assessments," https://www.epa.gov/waterresilience/cybersecurity-assessments. To contact the EPA regarding its Water Sector Cybersecurity Evaluation Program,

Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)[12], provide cybersecurity assessment programs at no cost. In addition, the EPA provides a tool that produces an assessment report and risk mitigation plan for the entity. This tool is called the EPA Water Cybersecurity Assessment Tool (WCAT).[13] Therefore, each water utility and sewer utility subject to the jurisdiction of the Commission must, within sixty (60) days of the entry of this Order, certify to the Commission in a filing in this general investigation that it has contacted either the EPA or CISA to have a cybersecurity vulnerability assessment performed. Once the EPA or CISA has performed the cybersecurity vulnerability assessment, a water or sewer utility must certify[14] to the Commission that an assessment was completed, provide the date(s) of completion, and identify the entity that performed the assessment.[15]

In lieu of an EPA or CISA assessment, a water or sewer system may have a cybersecurity vulnerability assessment performed by a different entity at its own cost. Any cybersecurity vulnerability assessment performed by an entity or individual outside of the EPA or CISA's program identified above must conform, at a minimum, with the EPA's Cybersecurity Checklist for Public Water System Sanitary Surveys (Checklist).[16] A water and sewer utility that chooses to have an assessment performed at its own cost must, within sixty (60) days of the entry of this Order, certify to the Commission that it has scheduled a cyberattack vulnerability assessment, and identify the individual or entity that will perform the assessment. Once the cybersecurity vulnerability assessment is performed, a water or sewer utility must certify to the Commission that the assessment was completed, provide the date(s) of completion, and identify the entity that performed the assessment.

---

see https://www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program.

[12] A free cybersecurity assessment can be administered by a CISA cybersecurity advisor. To contact a regional cybersecurity advisor, *see* https://www.cisa.gov/about/regions. For more information, *see* https://www.cisa.gov/sites/default/files/2024-03/fact-sheet-top-cyber-actions-for-securing-water-systems.pdf.

[13] https://www.epa.gov/system/files/documents/2023-03/EPA%20Water%20Cybersecurity%20Assessment%20Tool%201.0_0.xlsx. More information may be found at https://www.epa.gov/system/files/documents/2023-10/epa-cybersecurity-fact-sheet_508.pdf.

[14] The certification must substantially comply with the form attached to this Order as Attachment B.

[15] Given the sensitive nature of the assessments, the Commission will not collect the results of the assessments or any other documents related thereto.

[16] The Checklist can be found at Section 5 and Appendix A of "Evaluating Cybersecurity During Public Water System Sanitary Surveys," https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf.

The Commission further recognizes that a larger water or sewer utility may have policies and procedures in place to assess and address cyberthreats. If such is the case, the water or sewer utility, within sixty (60) days of the entry of this Order, should certify that it has policies and procedures in place to conduct periodic cyberattack vulnerability assessments, the date of the last assessment, and identify the individual or entity that performed the assessment.

Once an assessment is complete, a water or sewer utility will be required to develop a plan to address cyber threats. In addition, the water or sewer utility will be required to designate an individual employee responsible for compliance with that plan and to attend cybersecurity training for water and sewer utilities. These issues will be addressed in a later Commission Order in this general investigation.

FINDINGS OF FACT

1. Cyberattacks against water and sewer utilities are increasing throughout the United States.

2. The Federal Environmental Protection Agency (EPA) interprets the regulations regarding sanitary surveys to include an evaluation of the adequacy of the cybersecurity of any operational technology used in the production and distribution of safe drinking water.[17]

CONCLUSIONS OF LAW

1. The Commission has jurisdiction over water and sewer utilities in the State.

2. All water and sewer utilities are required to "maintain adequate and suitable facilities, safety appliances or other suitable devices, and shall perform such service in respect thereto as shall be reasonable, safe and sufficient for the security and convenience of the public."[18]

3. Because of threats of cyberattacks, it is reasonable for the Commission to open a general investigation and require all water and sewer utilities to have cybersecurity vulnerability assessments performed as discussed in this Order.

---

[17] *See* "Evaluating Cybersecurity During Public Water System Sanitary Surveys," https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf.

[18] W. Va. Code § 24-3-1.

4. Notice of this general investigation should be provided to all water and sewer utilities.

ORDER

IT IS THEREFORE ORDERED that the Commission opens a general investigation in the cybersecurity of water and sewer utilities.

IT IS FURTHER ORDERED that within sixty (60) days of the entry of this Order, each water and sewer utility shall certify that it has scheduled a cyberattack vulnerability assessment, or that it has policies and procedures in place to assess and address cybersecurity threats, as discussed in this Order. Certification of the assessment completion shall be made using Attachment B attached hereto.

IT IS FURTHER ORDERED that the Executive Secretary publish a copy of Attachment A once in newspapers of general circulation in each of the following cities: Beckley, Bluefield, Charleston, Clarksburg, Elkins, Fairmont, Huntington, Keyser, Lewisburg, Logan, Martinsburg, Morgantown, Moundsville, Parkersburg, Point Pleasant, Weirton, and Wheeling. The Executive Secretary shall thereafter file proof of publication of each notice in this proceeding.

IT IS FURTHER ORDERED that the Executive Secretary serve a copy of this Order on all water and sewer utilities providing service in West Virginia, the Office of the Governor, West Virginia Water Development Authority, West Virginia Department of Environmental Protection, West Virginia Department of Health and Human Resources Bureau for Public Health, Department of Homeland Security, West Virginia Office of Technology, West Virginia Emergency Management Division, by electronic service, or by United States First Class Mail, and on Staff by hand delivery.

A True Copy, Teste,

Karen Buckley

Karen Buckley, Executive Secretary

JAF/lcw
240460c

PUBLIC SERVICE COMMISSION
OF WEST VIRGINIA
CHARLESTON

CASE NO. 24-0460-PWD-W-GI
CASE NO. 24-0461-PSD-S-GI

GENERAL INVESTIGATION INTO
CYBERSECURITY OF WATER AND
SEWER UTILITIES

Cybersecurity Water and Sewer Utilities

On May 16, 2024, the Public Service Commission of West Virginia (Commission) opened a general investigation into the cybersecurity of water and sewer utilities. Water and sewer utilities must provide responsive information as specified in the May 16, 2024 Order to the Executive Secretary of the Commission, Karen Buckley, at P.O. Box 812, Charleston, WV 25323, by Monday, July 15, 2024. Interested parties may review the order opening the general investigation online at http://www.psc.state.wv.us/

PUBLIC SERVICE COMMISSION OF WEST VIRGINIA

Attachment B

PUBLIC SERVICE COMMISSION
OF WEST VIRGINIA
CHARLESTON

CASE No. 24-0460-PWD-W-GI
CASE No. 24-0461-PSD-S-GI

GENERAL INVESTIGATION INTO CYBERSECURITY OF WATER AND SEWER UTILITIES

CYBERSECURITY ASSESSMENT CERTIFICATION

Pursuant to the Commission Order entered on May 16, 2024, in Case Nos. 24-0460-PWD-W-GI and 24-0461-PSD-S-GI, City of Elkins WWTP (Wastewater)(Utility Name) provides the following cybersecurity assessment certification.

Utility Name: City of Elkins WWTP (Wastewater)

ADDRESS: Mailing: 401 Daivs Ave Elkins, WV 26241
Physical: 5 Riverbend Rd Elkins, WV 26241

PHONE NUMBER: (304) 636-1122

Date of Cybersecurity Assessment: 7/10/2024 @ 11:00AM (Wednesday)

Person or Company Completing Assessment: Jimmy Cady-Cybersecurity Analyst
Horsley Witten Group, Inc

Type of Assessment (self or third party): Third Party

Whitney L. Hymes
I, Wastewater Superintendent/Chief Operator **(name of certifying person) hereby certify that the public utility system named above has conducted or reviewed and updated an annual cybersecurity assessment.**

Signature of Owner or Operator: ________________________ Date: 7/10/2024

COMPLETED AND SUBMITTED TO:

Office of the Executive Secretary
Public Service Commission of West Virginia
201 Brooks Street
PO Box 812
Charleston, WV 25323