

GRAND HAVEN BOARD OF LIGHT AND POWER MEETING AGENDA

Thursday, June 19, 2025

Meeting to be held at 1700 Eaton Drive

6:00 PM

1. Call to Order / Roll Call / Excuse Absent Members
2. Approve Meeting Agenda (1) \*
3. Pledge of Allegiance
4. Public Comment Period
5. Consent Agenda (1)
  - A. Approve Minutes
    1. May 15, 2025 Special Meeting Minutes \*
    2. May 15, 2025 Closed Session Meeting Minutes
    3. May 15, 2025 Regular Meeting Minutes \*
  - B. Receive and File: May Financial Statements, Power Supply & Retail Sales Dashboards \*
  - C. Receive and File: May Key Performance Indicators (KPI) Dashboard \*
  - D. Receive and File: MPPA ESP Resource Position Report (dated 5/30/2025) \*
  - E. Approve Payment of Bills (\$3,252,921.77 in total)
    1. In the amount of \$2,732,788.41 from the Operation & Maintenance Fund
    2. In the amount of \$520,133.36 from the Renewal & Replacement Fund
  - F. Approve Confirming Purchase Orders (\$174,714 in total)
    1. PO #23415, Get-R-Cut, \$22,063 (Tree Work from Storm Damage)
    2. PO #23417, CSX, \$5,018 (Annual Crossing Fees)
    3. PO #23431, Flory Line Construction, \$62,633 (Line Work from Storm Damage)
    4. PO #23445, Charter Communications, \$15,000 (FY26 Internet Service)
    5. PO #23448, Landis & Gyr, \$40,000 (FY26 Grid Analytics Software Subscription)
    6. PO #23449, Landis & Gyr, \$30,000 (FY26 AMI Software Subscription)
6. General Manager's Report \*
  - A. Approve Purchase Orders (\$338,387 in total) (1)
    1. PO #23422, Koppers, \$15,393 (Distribution Wood Poles x 23 for BLP Stock)
    2. PO #23424, Altec, \$251,794 (AT48P Bucket Truck)
    3. PO #23434, Tri-Cities Broadcasting, \$6,000 (FY26 WAWL Outreach)
    4. PO #23435, Holland Litho, \$17,000 (FY26 Printing Services)
    5. PO #23436, WGHN, \$8,200 (FY26 WHGN Outreach)
    6. PO #23437, Boileau Communications, \$40,000 (FY26 Customer Communication)
  - B. Approve FY 2025 Utility Write-offs (1)\*
  - C. Energy Waste Reduction (1) \*
  - D. Policy Review (1) \*
7. Chairman's Report
  - A. General Manager Salary Evaluation (1)
8. Other Business (4)
9. Public Comment Period
10. Adjourn

Notes:

(1) Board Action Required

(2) Future Board Action

\* Information Enclosed

(3) Information RE: Policy or Performance

(4) General Information for Business or Education

GRAND HAVEN BOARD OF LIGHT AND POWER  
MINUTES  
MAY 15, 2025

A special meeting of the Grand Haven Board of Light and Power was held on Thursday, May 15, 2025, at 5:30 PM at the Board's office located at 1700 Eaton Drive in Grand Haven, Michigan.

The meeting was called to order at 5:31 PM by Chairperson Westbrook.

**Present:** Directors Crum, Knoth, Polyak, Welling, and Westbrook.

**Absent:** None.

**Others Present:** General Manager Rob Shelley, Secretary to the Board Danielle Martin, Ron Bultje of Dickinson Wright, and Kevin Yombor of Kaufman Dolowich (attending remotely).

**25-05A** Director Welling, supported by Director Knoth, moved to approve the meeting agenda.

**Roll Call Vote:**

In favor: Directors Crum, Knoth, Polyak, Welling and Westbrook; Opposed: None.  
Motion carried.

**Public Comment Period:** None.

**25-05B** At 5:32 PM Director Welling, supported by Director Knoth, moved to enter closed session pursuant to Section 8(1)(e) of the Open Meetings Act to discuss with BLP attorneys trial or settlement strategy pertaining to the David Walters litigation, because an open meeting would have a detrimental financial impact upon the litigating or settlement position of the BLP.

**Roll Call Vote:**

In favor: Directors Crum, Knoth, Polyak, Welling and Westbrook; Opposed: None.  
Motion carried.

**25-05C** At 6:10 PM Director Welling, supported by Director Polyak, moved to end closed session and re-enter open session.

**Roll Call Vote:**

In favor: Directors Crum, Knoth, Polyak, Welling and Westbrook; Opposed: None.  
Motion carried.

**Adjournment**

At 6:11 PM by motion of Director Polyak, supported by Director Welling, the May 15, 2025 Board meeting was unanimously adjourned.

Respectfully submitted,

Danielle Martin  
Secretary to the Board

DM

GRAND HAVEN BOARD OF LIGHT AND POWER  
MINUTES  
MAY 15, 2025

A regular meeting of the Grand Haven Board of Light and Power was held on Thursday, May 15, 2025, at 6:00 PM at the Board's office located at 1700 Eaton Drive in Grand Haven, Michigan and electronically via live Zoom Webinar.

The meeting was called to order at 6:14 PM by Chairperson Westbrook.

**Present:** Directors Crum, Knoth, Polyak, Welling, and Westbrook.

**Absent:** None.

**Others Present:** General Manager Rob Shelley, Secretary to the Board Danielle Martin, Finance Manager Lynn Diffell, Operations and Power Supply Manager Erik Booth, Distribution and Engineering Manager Austin Gagnon, Information Technology Specialist Dan Deller, Ron Bultje of Dickinson Wright, and Dan Kasbohm of Utility Financial Solutions.

**25-06A** Director Welling, supported by Director Knoth, moved to approve the meeting agenda.

**Roll Call Vote:**

In favor: Directors Crum, Knoth, Polyak, Welling and Westbrook; Opposed: None.

Motion carried.

**Pledge of Allegiance**

**Public Comment Period:** None.

**25-06B** Director Welling, supported by Director Polyak, moved to approve the consent agenda.

The consent agenda includes:

- Approve the minutes of the April 28, 2025 Regular Board Meeting
- Receive and File the April Financial Statements, Power Supply and Retail Sales Dashboards
- Receive and File the April Key Performance Indicator (KPI) Dashboard
- Receive and File the MPPA Energy Services Project Resource Position Report dated 04/30/2025
- Approve payment of bills in the amount of \$2,175,179.98 from the Operation & Maintenance Fund
- Approve payment of bills in the amount of \$713,828.64 from the Renewal & Replacement Fund

**Roll Call Vote:**

In favor: Directors Crum, Knoth, Polyak, Welling and Westbrook; Opposed: None.

Motion carried.

GRAND HAVEN BOARD OF LIGHT AND POWER  
MINUTES  
MAY 15, 2025

**25-06C** Director Welling, supported by Director Crum, moved to approve the Purchase Orders. The Purchase Orders include:

- Purchase Order #23391 to Altec in the amount of \$358,642 for a TA60 bucket truck
- Purchase Order #23403 to the City of Grand Haven in the amount of \$414,608 for fiscal year 2026 ground water monitoring
- Purchase Order #23404 to the City of Grand Haven in the amount of \$6,796 for the fiscal year 2026 impoundment inspection
- Purchase Order #23406 to Rehmann in the amount of \$38,910 for backup network servers and labor
- Purchase Order #23409 to Midwest Construction in the amount of \$993,000 for the Eaton Drive building remodel
- Purchase Order #23410 to Materials Testing Consultants in the amount of \$6,000 for soil bearings for the Eaton Drive building remodel

**Roll Call Vote:**

In favor: Directors Crum, Knoth, Polyak, Welling and Westbrook; Opposed: None.  
Motion carried.

**25-06D** Director Welling, supported by Director Polyak, moved to approve the Board Resolution Regarding David Walters Litigation (Attachment A).

**Roll Call Vote:**

In favor: Directors Crum, Knoth, Polyak, Welling and Westbrook; Opposed: None.  
Motion carried.

**25-06E** Director Welling, supported by Director Crum, moved to approve the Resolution to Approve the Fiscal Year 2026 Budget (Attachment B).

Finance Manager Lynn Diffell reviewed the budget and capital plan. There were no significant changes from last month's presentation. Any potential rate changes discussed in the Cost-of-Service Study would have a net zero effect on income and therefore would not impact the budget. The Environmental Remediation Surcharge will collect \$1 million for Harbor Island obligations. The Low-Income Energy Assistance Fund surcharge could be up to \$1.25 per meter per month as determined by the State. The State mandated Energy Waste Reduction surcharge is not yet known. Payments to the City of Grand Haven are expected to be \$1.8 million. The biggest expense within the budget is \$20 million for purchased power. The MERS pension program was 95% funded as of December 2023 and the 2024 report will be available in July. The five-year capital plan is \$26.5 million. At the fiscal year end, working cash is expected to be \$27.6 million.

GRAND HAVEN BOARD OF LIGHT AND POWER  
MINUTES  
MAY 15, 2025

**Roll Call Vote:**

In favor: Directors Crum, Knoth, Polyak, Welling and Westbrook; Opposed: None.  
Motion carried

**25-06F** Director Welling, supported by Director Knoth, moved to approve the Resolution to Approve the Fiscal Year 2026 Capital Plan (Attachment C).

**Roll Call Vote:**

In favor: Directors Crum, Knoth, Polyak, Welling and Westbrook; Opposed: None.  
Motion carried

**25-06G** Dan Kasbohm from Utility Financial Solutions (UFS) presented the Cost-of-Service Study.

UFS utilizes key financial targets to measure the health of a utility. BLP has a good debt coverage ratio and cash balance; however, with no adjustments, operating income will drop below the optimal level in the next five years. This can be remedied with some small rate adjustments.

The study examined how much the BLP is spending to serve each customer class and how much the BLP is then collecting from each customer class. UFS looks for a window of plus or minus ten percent of the cost of service. The study found two classes fall outside of the ten percent window; we are collecting more from General Service Secondary customers than the actual cost to serve them and are collecting less from General Service Large Secondary compared to the actual cost to serve them. UFS suggests making small rate adjustments to these two groups to bring them closer to the actual cost of service. The proposed adjustments would have a net zero effect on BLP income.

The study found the monthly service charge for all classes is currently below the actual cost of service. UFS recommends increasing the monthly service charges and decreasing the energy charges for a net zero impact. UFS also recommends resetting the PSCA from \$0.059/Kwh to \$0.069/Kwh. This would increase energy rate charges by one penny but drop the PSCA by one penny, having a net zero impact.

The General Manager explained no Board action is being requested today. Staff hopes to bring any proposed rate changes, along with information on the State mandated surcharges, for Board approval in July.

**No formal action taken.**

GRAND HAVEN BOARD OF LIGHT AND POWER  
MINUTES  
MAY 15, 2025

**25-06H** Catherine Vollmer and Sofia Vigeant from Great Blue Research presented the Customer Satisfaction Study.

The survey was conducted in digital and phone format from late February to early April. Responses were divided into two categories: residential and commercial. 518 residential surveys were completed, and 58 commercial surveys were completed. Data highlights for each group are:

**Residential**

- Average positive rating across all organizational characteristics was 85.9% (the national average was 63.6%).
- 90.8% of respondents were satisfied with their interaction with office personnel and 88.1% were satisfied with their interaction with field personnel (both higher than the national average).
- 90.4% of respondents were satisfied with the BLP's online management system and 93.8% were "very" or "somewhat" confident in the BLP's ability to restore power after a major storm or weather event.
- The top two priorities ranked by importance for residential respondents were having reliable power to their home and the cost of electricity. Reduction of carbon in the energy portfolio was ranked as the least important factor for residential respondents.
- 79% of respondents would "strongly" or "somewhat" support the BLP owning small local gas fired generation.

**Commercial**

- Average positive rating across all organizational characteristics was 85.8% (the national average was 69.5%).
- 95.7% of respondents were satisfied with their interaction with office personnel and 100% were satisfied with their interaction with field personnel (both higher than the national average).
- 100% of respondents were satisfied with the BLP's online management system and 98.2% were "very" or "somewhat" confident in the BLP's ability to restore power after a major storm or weather event.
- The top two priorities ranked by importance for residential respondents were having reliable power to their home and the cost of electricity. Reduction of carbon in the energy portfolio was ranked as the least important factor for commercial respondents.
- 89.7% of respondents would "strongly" or "somewhat" support the BLP owning small local gas fired generation.

**No formal action taken.**

GRAND HAVEN BOARD OF LIGHT AND POWER  
MINUTES  
MAY 15, 2025

**25-06I** The Board's self-evaluation process was discussed. By consensus, the results will be reviewed at a special meeting held at 4:00PM on July 17, 2025. The meeting will be held off site prior to the regular meeting scheduled for 6:00PM.

**No formal action taken.**

**25-06J** The General Manager's annual performance evaluation was discussed. By consensus, the evaluation will be conducted at 4:30PM on June 19, 2025 prior to the regular meeting scheduled for 6:00PM. The evaluation will be conducted in closed session as requested by the General Manager and as permitted by Section 8(1)(a) of the Open Meetings Act.

**No formal action taken.**

**Other Business**

- The General Manager reported proposals were received today for the administration of the State mandated Energy Waste Reduction program. The Board will need to choose between using the State's or MPPA's contractor. The total estimated cost is \$1 million. The deadline to join the State's program is July 1<sup>st</sup> so Board action will be required at its meeting in June.

**Public Comment Period:** None.

**Adjournment**

At 8:11PM by motion of Director Welling, supported by Director Knoth, the May 15, 2025 Board meeting was unanimously adjourned.

Respectfully submitted,

Danielle Martin  
Secretary to the Board

DM

GRAND HAVEN BOARD OF LIGHT AND POWER  
MINUTES  
MAY 15, 2025

Attachment A

**GRAND HAVEN BOARD OF LIGHT & POWER**

**RESOLUTION REGARDING DAVID WALTERS LITIGATION**

WHEREAS, the Grand Haven Board of Light and Power (“BLP”) is a Defendant in a lawsuit initiated by David Walters (“Walters”), David Walters v. Grand Haven Board of Light & Power, Case No. 24-7759-CD, in the 20th Circuit Court for the County of Ottawa (the “Lawsuit”); and

WHEREAS, in the Lawsuit, Walters alleges that BLP terminated him in breach of his employment agreement, as well as in retaliation for reporting suspected violations of the law, in violation of Michigan’s Whistleblower Protection Act. Walters also alleges that the BLP has violated Michigan’s Open Meetings Act; and

WHEREAS, BLP denies Walter’s allegations, and asserts that BLP properly terminated Walters pursuant to Paragraph 10.C of his July 1, 2022 Employment Agreement; and

WHEREAS, BLP attended a mediation with Walters on April 18, 2025. The Parties did not reach a resolution at mediation; and

WHEREAS, BLP desires to try and resolve this Lawsuit without additional legal fees and costs.

THEREFORE, BE IT RESOLVED, BLP instructs its attorney, Kaufman Dolowich, to serve upon Walters an Offer of Judgment consistent with the presentation by Kaufman Dolowich in closed session on this date. This Offer of Judgment would resolve all claims set forth in the Complaint filed by Plaintiff, dated April 19, 2024, and be inclusive of all interest, costs, fees, and expense incurred through the date of the entry of said Judgment.

**RESOLUTION DECLARED ADOPTED**

Dated: May 15, 2025

\_\_\_\_\_  
Danielle Martin, Board Secretary  
Grand Haven Board of Light & Power

**CERTIFICATION**

I hereby certify that the foregoing is a true and complete copy of a resolution adopted by the Grand Haven Board of Light & Power, at a meeting held on May 15, 2025, and that public notice of said meeting was given pursuant to, and in compliance with, Act 267 of the Public Acts of Michigan of 1976, as amended.

Dated: May 15, 2025

\_\_\_\_\_  
Robert Shelley, General Manager  
Grand Haven Board of Light & Power



GRAND HAVEN BOARD OF LIGHT AND POWER  
MINUTES  
MAY 15, 2025

Attachment B

**GRAND HAVEN BOARD OF LIGHT & POWER**

**RESOLUTION TO APPROVE THE FISCAL YEAR 2026 BUDGET**

WHEREAS, the Board of Light and Power has established a budget which includes operating and nonoperating revenue and expenses for the fiscal year 2026; and

WHEREAS, the Board of Light and Power has included projections for retail sales along with purchased power, employee and other expenses.

THEREFORE, BE IT RESOLVED, the Board of Light and Power believes that these projections are reasonable and based on the best practices; and

BE IT FURTHER RESOLVED, the Board of Light and Power hereby approves the budget plan as presented for fiscal year 2026.

**RESOLUTION DECLARED ADOPTED**

Dated: May 15, 2025

---

Danielle Martin, Board Secretary  
Grand Haven Board of Light & Power

**CERTIFICATION**

I hereby certify that the foregoing is a true and complete copy of a resolution adopted by the Grand Haven Board of Light & Power, at a meeting held on May 15, 2025, and that public notice of said meeting was given pursuant to, and in compliance with, Act 267 of the Public Acts of Michigan of 1976, as amended.

Dated: May 15, 2025

---

Robert Shelley, General Manager  
Grand Haven Board of Light & Power

GRAND HAVEN BOARD OF LIGHT AND POWER  
MINUTES  
MAY 15, 2025

Attachment C

**GRAND HAVEN BOARD OF LIGHT & POWER**

**RESOLUTION TO APPROVE THE FISCAL YEAR 2026 CAPITAL PLAN**

WHEREAS, the Board of Light and Power has established a five-year capital plan for the fiscal years 2026-2030; and

WHEREAS, the Board of Light and Power has included estimated costs for projects anticipated to begin in the fiscal year 2026 and purchases for capitalized inventory.

THEREFORE, BE IT RESOLVED, the Board of Light and Power believes that these projections are reasonable and based on the best practices and recent engineering studies; and

BE IT FURTHER RESOLVED, the Board of Light and Power hereby approves the five-year capital plan as presented for fiscal year 2026.

**RESOLUTION DECLARED ADOPTED**

Dated: May 15, 2025

---

Danielle Martin, Board Secretary  
Grand Haven Board of Light & Power

**CERTIFICATION**

I hereby certify that the foregoing is a true and complete copy of a resolution adopted by the Grand Haven Board of Light & Power, at a meeting held on May 15, 2025, and that public notice of said meeting was given pursuant to, and in compliance with, Act 267 of the Public Acts of Michigan of 1976, as amended.

Dated: May 15, 2025

---

Robert Shelley, General Manager  
Grand Haven Board of Light & Power

**GRAND HAVEN BOARD OF LIGHT AND POWER**  
**STATEMENT OF NET POSITION**  
**FOR THE MONTH ENDING MAY 2025**

	<u>MAY 2025</u>	<u>MAY 2024</u>
<b>ASSETS</b>		
<b>CURRENT ASSETS</b>		
CASH AND CASH EQUIVALENTS	\$29,140,164	\$22,983,939
ACCOUNTS RECEIVABLE	4,111,380	3,839,760
PREPAID	1,290	1,401
	<hr/> 33,252,834	<hr/> 26,825,100
<b>NON-CURRENT ASSETS</b>		
DEPOSITS HELD BY MPIA	10,318,558	8,588,617
DEPOSITS HELD BY MPPA	2,500,000	2,500,000
ADVANCE TO CITY OF GRAND HAVEN	504,180	628,997
MITIGATION FUND	17,166,560	14,344,046
2021A BOND FUND	0	5,682,547
2021A BOND REDEMPTION FUND	1,171,641	1,163,007
	<hr/> 31,660,939	<hr/> 32,907,214
<b>CAPITAL ASSETS</b>		
CONSTRUCTION IN PROGRESS	3,043,193	3,898,649
PROPERTY, PLANT AND EQUIPMENT	68,047,118	66,525,483
LESS ACCUMULATED DEPRECIATION	(31,769,927)	(32,227,548)
	<hr/> 39,320,384	<hr/> 38,196,584
<b>TOTAL ASSETS</b>	<hr/> <hr/> \$104,234,157	<hr/> <hr/> \$97,928,898
<b>DEFERRED OUTFLOWS/(INFLOWS)</b>		
PENSION/OPEB RELATED	3,736,804	4,681,112
	<hr/>	<hr/>
<b>LIABILITIES</b>		
<b>CURRENT LIABILITIES</b>		
ACCOUNTS PAYABLE	1,425,269	1,315,795
SERIES 2021A BOND CURRENT	2,517,842	2,533,642
ACCRUED PAYROLL LIABILITIES	252,383	198,017
CUSTOMER DEPOSITS	976,300	978,655
ACCRUED TRANSFER FUND	143,074	137,086
	<hr/> 5,314,868	<hr/> 5,163,195
<b>LONG TERM LIABILITIES</b>		
ASSET RETIREMENT OBLIGATION - MITIGATION	17,024,842	16,648,725
ACCRUED SICK AND PTO	288,026	260,549
SERIES 2021A BOND	15,500,000	17,900,000
NET PENSION LIABILITIES	5,491,563	6,301,362
NET OTHER POST EMPLOYMENT BENEFIT	929,482	500,888
	<hr/> 39,233,913	<hr/> 41,611,524
<b>TOTAL LIABILITIES</b>	<hr/> 44,548,781	<hr/> 46,774,719
<b>NET POSITION</b>		
BEGINNING OF THE YEAR	56,080,669	48,794,255
YTD INCREASE IN NET ASSETS	7,341,511	7,041,036
<b>NET POSITION</b>	<hr/> 63,422,180	<hr/> 55,835,291
<b>TOTAL LIABILITIES AND EQUITY</b>	<hr/> <hr/> \$107,970,961	<hr/> <hr/> \$102,610,010

**GRAND HAVEN BOARD OF LIGHT AND POWER**  
**STATEMENT OF REVENUES, EXPENSES AND CHANGES IN NET POSITION**  
**FOR THE MONTH OF MAY 2025**

	Current Period Actual	YTD Actual	YTD Budget	Variance Over (Under)	Percent Variance Actual vs Budget	Previous Year Current Period	Previous Year YTD	Variance Over (Under)	Percent Variance Actual vs Last Year
<b>Operating Revenue</b>									
Residential Sales	\$ 908,392	\$ 12,318,057	\$ 11,999,305	\$ 318,752	2.66%	\$ 856,312	\$ 11,677,817	\$ 640,240	5.48%
Commercial Sales	841,729	9,732,448	9,657,413	75,035	0.78%	789,837	9,380,621	351,827	3.75%
Industrial Sales	939,594	10,547,689	10,951,282	(403,593)	-3.69%	924,516	10,738,981	(191,292)	-1.78%
Municipal Sales	74,366	911,356	918,739	(7,383)	-0.80%	73,241	904,137	7,219	0.80%
Total Charges for Services	2,764,081	33,509,550	33,526,739	(17,189)	-0.05%	2,643,906	32,701,556	807,994	2.47%
Street Lighting	28,179	309,153	308,000	1,153	0.37%	28,012	310,035	(882)	-0.28%
Other Revenue	19,070	683,688	274,633	409,055	148.95%	49,194	346,284	337,404	97.44%
<b>Total Operating Revenue</b>	<b>2,811,330</b>	<b>34,502,391</b>	<b>34,109,372</b>	<b>393,019</b>	<b>1.15%</b>	<b>2,721,112</b>	<b>33,357,875</b>	<b>1,144,516</b>	<b>3.43%</b>
<b>Operating Expenses</b>									
Net Purchased Power	1,762,513	17,941,146	18,469,950	(528,804)	-2.86%	1,418,206	16,735,262	1,205,884	7.21%
Distribution Operations	142,933	1,215,280	1,639,733	(424,453)	-25.89%	127,575	1,396,389	(181,109)	-12.97%
Distribution Maintenance	480,207	3,053,679	3,236,831	(183,152)	-5.66%	301,899	3,123,093	(69,414)	-2.22%
Energy Optimization	30,703	181,194	297,916	(116,722)	-39.18%	11,095	141,613	39,581	27.95%
Administration	268,162	2,635,710	2,862,326	(226,616)	-7.92%	246,708	2,664,099	(28,389)	-1.07%
Legacy Pension Expense	6,845	142,678	458,332	(315,654)	-68.87%	35,260	618,445	(475,767)	-76.93%
<b>Operating Expenses Before Depreciation</b>	<b>2,691,363</b>	<b>25,169,687</b>	<b>26,965,088</b>	<b>(1,795,401)</b>	<b>-6.66%</b>	<b>2,140,743</b>	<b>24,678,901</b>	<b>490,786</b>	<b>1.99%</b>
<b>Operating Changes Before Depreciation</b>	<b>119,967</b>	<b>9,332,704</b>	<b>7,144,284</b>	<b>2,188,420</b>	<b>30.63%</b>	<b>580,369</b>	<b>8,678,974</b>	<b>653,730</b>	<b>7.53%</b>
Depreciation	183,232	2,028,913	1,999,077	29,836	1.49%	171,462	1,908,849	120,064	6.29%
<b>Operating Changes</b>	<b>(63,265)</b>	<b>7,303,791</b>	<b>5,145,207</b>	<b>2,158,584</b>	<b>41.95%</b>	<b>408,907</b>	<b>6,770,125</b>	<b>533,666</b>	<b>7.88%</b>
Nonoperating Revenue/(Expenses)	75,553	876,579	566,700	309,879	54.68%	100,445	970,774	(94,195)	-9.70%
Asset Retirement Expense	-	24,698	-	24,698	#DIV/0!	-	123,492	(98,794)	-80.00%
Environmental Surcharge	69,221	870,924	916,663	(45,739)	-4.99%	69,811	870,763	161	0.02%
<b>Non-Operating Revenue/(Expenses)</b>	<b>144,774</b>	<b>1,772,201</b>	<b>1,483,363</b>	<b>288,838</b>	<b>19.47%</b>	<b>170,256</b>	<b>1,965,029</b>	<b>(192,828)</b>	<b>-9.81%</b>
Transfers to City of Grand Haven	(143,074)	(1,734,481)	(1,676,337)	(58,144)	3.47%	(137,086)	(1,694,118)	(40,363)	2.38%
<b>Increase in Net Assets</b>	<b>\$ (61,565)</b>	<b>\$ 7,341,511</b>	<b>\$ 4,952,233</b>	<b>\$ 2,389,278</b>	<b>48.25%</b>	<b>\$ 442,077</b>	<b>\$ 7,041,036</b>	<b>\$ 300,475</b>	<b>4.27%</b>

**GRAND HAVEN BOARD OF LIGHT AND POWER  
POWER SUPPLY DASHBOARD  
FOR THE MONTH OF MAY 2025**

<b><u>Power Supply for Month (kWh)</u></b>	<b><u>FY2025</u></b>		<b><u>FY2024</u></b>	
Net Purchased (Sold) Power	14,191,944	66.98%	14,896,133	67.28%
Renewable Energy Purchases	6,997,149	33.02%	7,245,735	32.72%
<b>Monthly Power Supply Total</b>	<b>21,189,093</b>		<b>22,141,868</b>	
Days in Month	31		31	
Average Daily kWh Supply for Month	<b>683,519</b>		<b>714,254</b>	
% Change	-4.30%			

<b><u>Power Supply FYTD</u></b>	<b><u>FY2025</u></b>		<b><u>FY2024</u></b>	
Net Purchased (Sold) Power	185,167,029	73.08%	190,674,416	75.04%
Renewable Energy Purchases	68,220,391	26.92%	63,409,658	24.96%
<b>FYTD Power Supply Total</b>	<b>253,387,420</b>		<b>254,084,074</b>	
FYTD Days (from 7/1)	335		336	
<b>Average Daily kWh Supply FYTD</b>	<b>756,380</b>		<b>756,203</b>	
% Change	0.02%			

	<b><u>FY2025</u></b>	<b><u>FY2024</u></b>
Net Purchased Power Expenses	\$17,941,146	\$16,735,262
% Change	7.21%	
<b>Net Energy Expenses per kWh Supplied to System FYTD</b>	<b>\$0.07081</b>	<b>\$0.06587</b>
% Change	7.50%	

**GRAND HAVEN BOARD OF LIGHT AND POWER  
SALES DASHBOARD  
FOR THE MONTH OF MAY 2025**

<u>Monthly Retail Customers</u>	<u>FY2025</u>		<u>FY2024</u>	
Residential	13,275	87.49%	13,218	87.52%
Commercial	1,658	10.93%	1,644	10.89%
Industrial	130	0.86%	126	0.83%
Municipal	110	0.72%	115	0.76%
<b>Total</b>	<b>15,173</b>		<b>15,103</b>	
 <u>Monthly Energy Sold (kWh)</u>				
Residential	5,732,604	28.85%	5,547,327	27.70%
Commercial	5,853,071	29.46%	5,755,790	28.74%
Industrial	7,639,893	38.45%	8,073,231	40.31%
Municipal	576,298	2.90%	585,548	2.92%
Retail Monthly Total	19,801,866	99.67%	19,961,896	99.67%
Street Lighting	66,420	0.33%	66,349	0.33%
<b>Total Monthly Energy Sold</b>	<b>19,868,286</b>		<b>20,028,245</b>	
 Days in Primary Meter Cycle	 30		 30	
<b>kWh Sold per Day</b>	<b>662,276</b>		<b>667,608</b>	
% Change	-0.80%			

<u>Energy Sold (kWh) FYTD</u>	<u>FY2025</u>		<u>FY2024</u>	
Residential	82,650,272	33.10%	78,957,573	31.62%
Commercial	70,451,798	28.22%	68,791,480	27.55%
Industrial	88,367,816	35.39%	93,520,458	37.45%
Municipal	7,488,748	3.00%	7,572,097	3.03%
Retail Energy Sold Total FYTD	248,958,634	99.71%	248,841,608	99.66%
Street Lighting	731,618	0.29%	855,293	0.34%
<b>Energy Sold FYTD</b>	<b>249,690,252</b>		<b>249,696,901</b>	
 Weighted Days in Meter Cycles FYTD	 334		 335	
<b>kWh Sold per Day</b>	<b>747,576</b>		<b>745,364</b>	
% Change	0.30%			

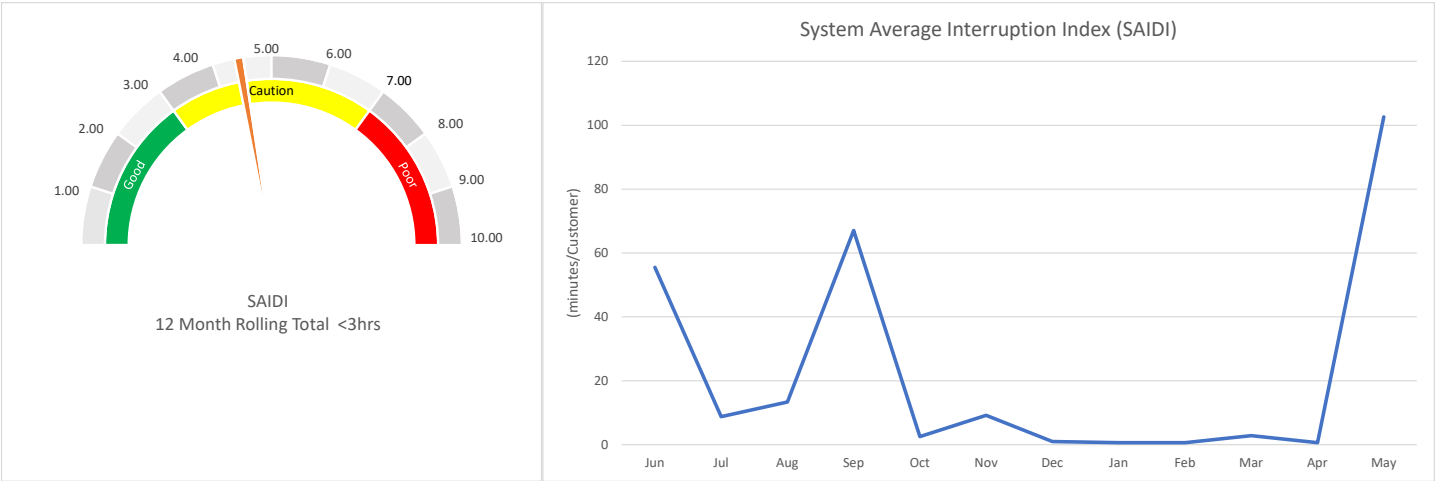
<u>Sales Revenue FYTD net ERS</u>	<u>FY2025</u>	<u>Average Rate (\$/kWh)</u>	<u>FY2024</u>	<u>Average Rate (\$/KWh)</u>	<u>Percent Change \$/kWh</u>
Residential	\$12,318,057	\$0.1490	\$11,677,816	\$0.1479	0.77%
Commercial	\$9,732,448	\$0.1381	\$9,380,621	\$0.1364	1.31%
Industrial	\$10,547,689	\$0.1194	\$10,738,981	\$0.1148	3.95%
Municipal	\$911,356	\$0.1217	\$904,137	\$0.1194	1.92%
<b>Retail Sales Revenue FYTD</b>	<b>\$33,509,550</b>	<b>\$0.1346</b>	<b>\$32,701,556</b>	<b>\$0.1314</b>	<b>2.42%</b>
Street Lighting	\$309,153		\$310,035		
<b>Total Sales Revenue FYTD (Excl. Wholesale)</b>	<b>\$33,818,703</b>	<b>\$0.1354</b>	<b>\$33,011,591</b>	<b>\$0.1322</b>	

	<u>FY2025</u>	<u>FY2024</u>
Approx. Distribution Losses FYTD	1.16%	1.43%
<b>Net Energy Expenses/kWh Sold FYTD</b>	<b>\$0.07163</b>	<b>\$0.06681</b>
% Change	7.22%	

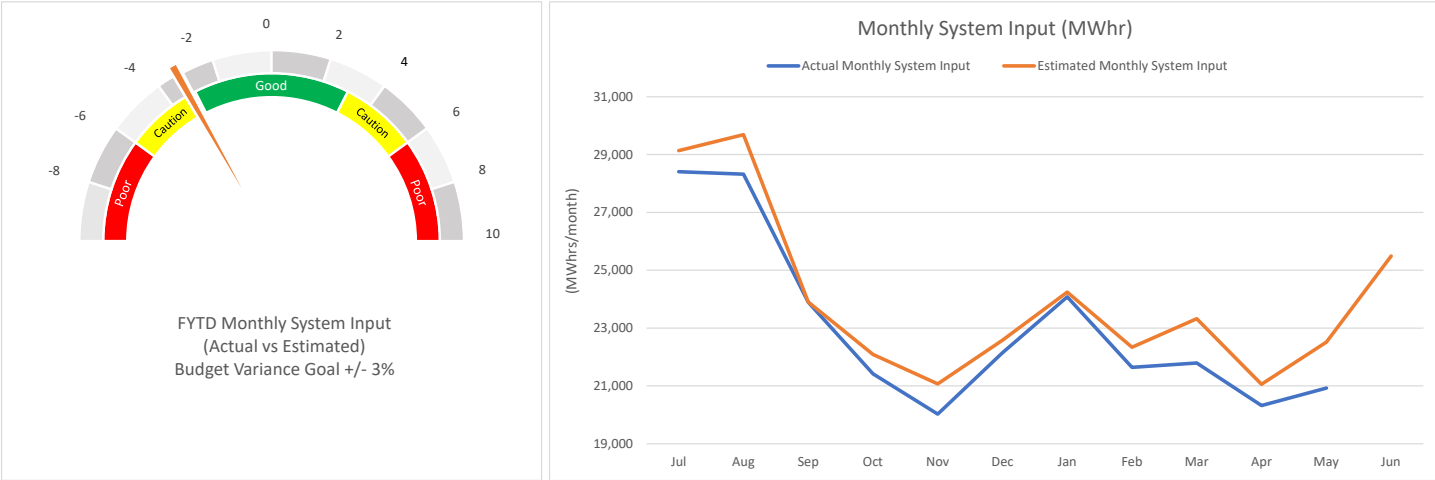
GHBLP Key Performance Indicators

June 12, 2025

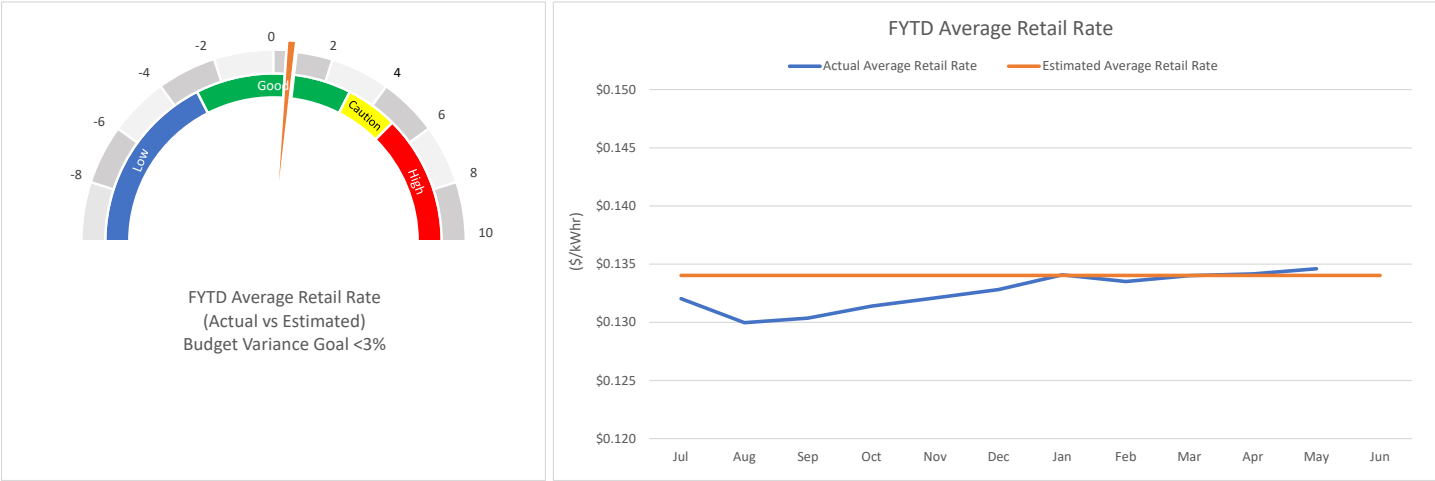
1) Reliability



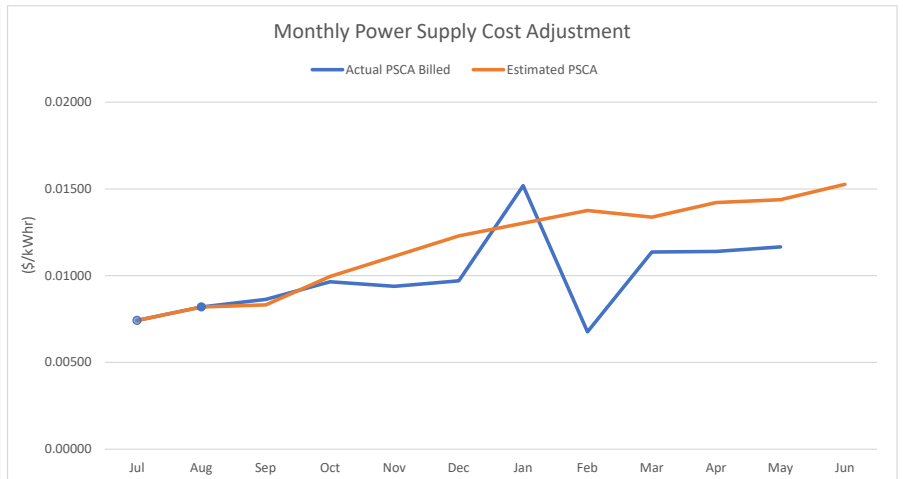
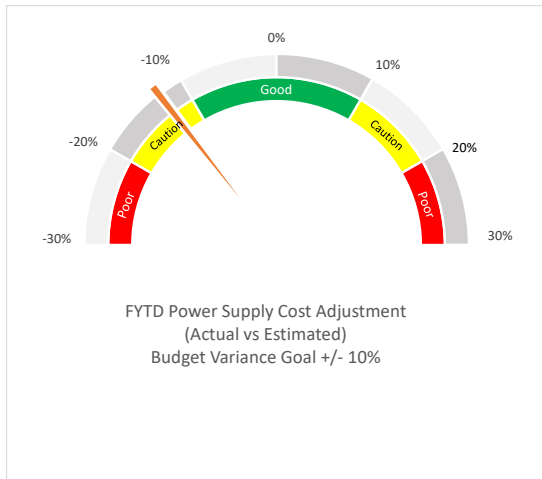
2) Power Supply



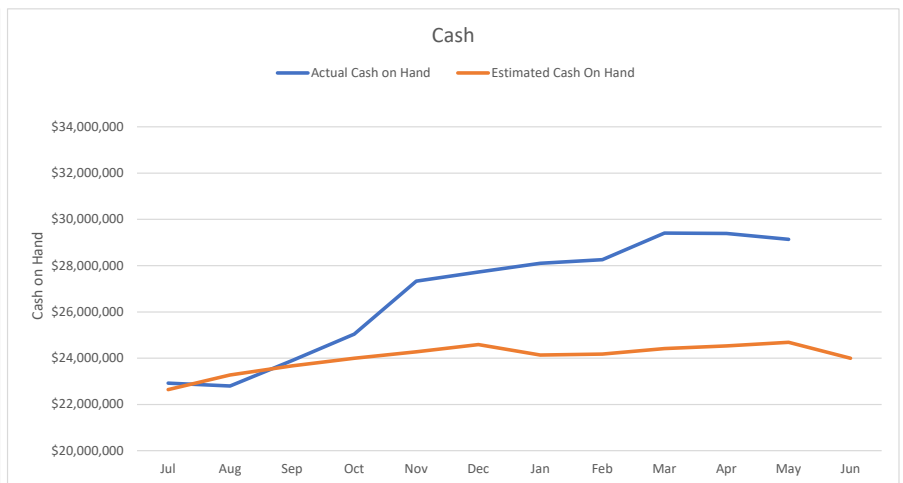
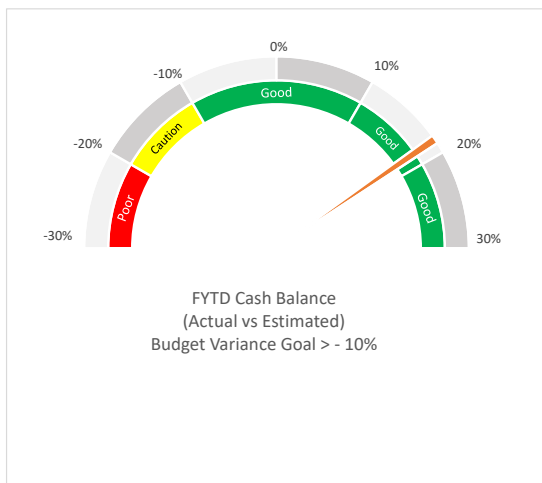
3) Average Retail Revenue per kWh



#### 4) Rates/PSCA



#### 5) Financial



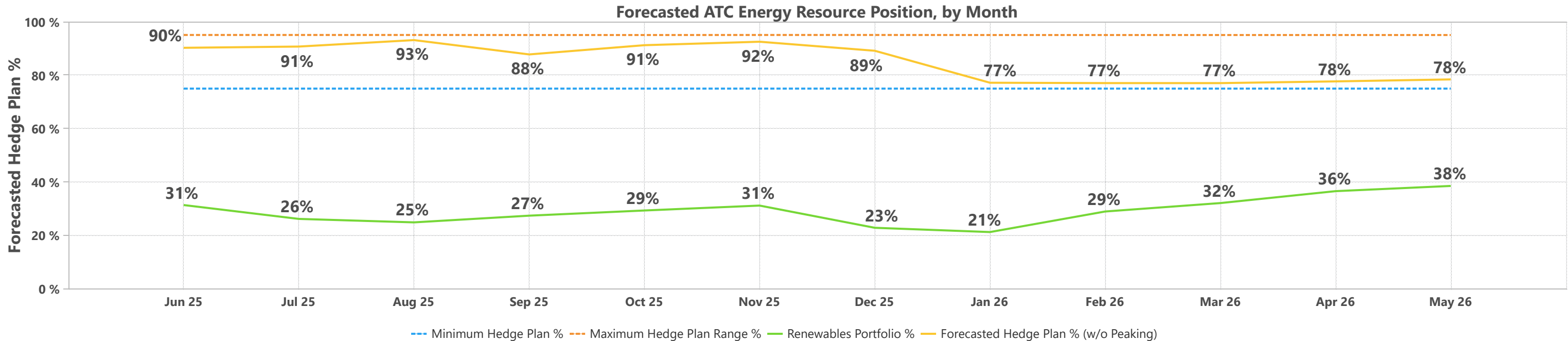


GRAN is forecasted to have an average of 85% of Around the Clock (ATC) Power Supply hedged over the upcoming 12 months, and Renewable Energy Resources are forecasted to provide an average of 29% towards load. Total Resources are forecasted to cost an average of \$52.37 Per MWh, and Market Balancing Energy is forecasted to come in at an average of \$46.36 per MWh. When including Locational Basis this results in a Total Forecasted Power Supply weighted average cost of \$52.30 over the upcoming 12 months.

Forecasted Prompt 12 Months Energy Resource Position for GRAN

Power Supply, MWh	Jun 25	Jul 25	Aug 25	Sep 25	Oct 25	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	Apr 26	May 26
Total Resources, MWh	22,194	25,065	25,658	20,261	18,807	17,904	19,214	18,024	16,542	17,373	15,669	16,878
Project Assets	1,717	1,579	1,545	1,556	1,701	1,655	1,639	1,657	1,488	1,694	1,612	1,673
Landfill Project	1,717	1,579	1,545	1,556	1,701	1,655	1,639	1,657	1,488	1,694	1,612	1,673
Contracted Power Supply	20,477	23,485	24,113	18,705	17,106	16,250	17,575	16,367	15,054	15,679	14,057	15,205
Contracted ESP Renewable PPAs	5,977	5,628	5,283	4,747	4,327	4,360	3,266	3,285	4,712	5,530	5,751	6,604
Contracted Bilateral Energy Transactions	14,501	17,858	18,830	13,958	12,778	11,890	14,310	13,082	10,342	10,149	8,306	8,601

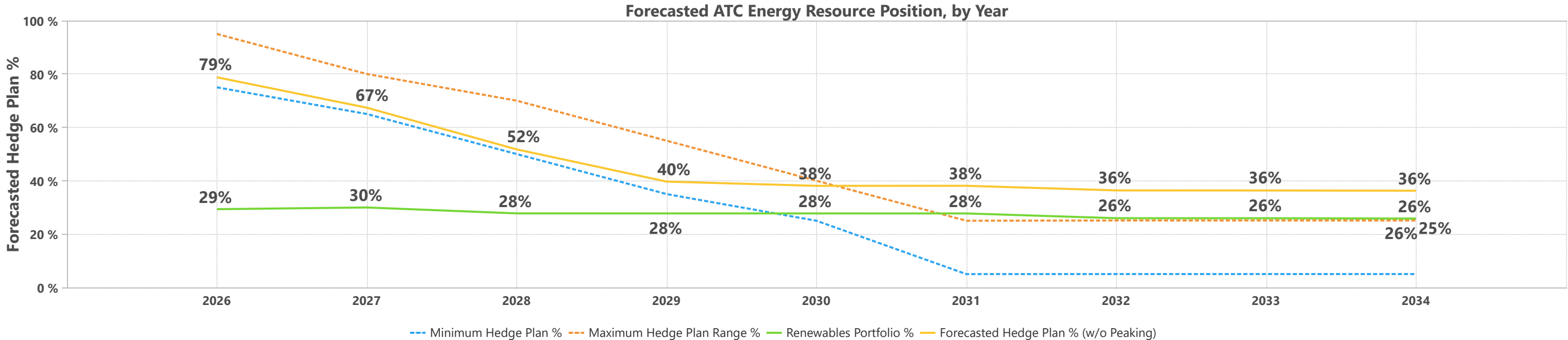
Total Power Supply	Jun 25	Jul 25	Aug 25	Sep 25	Oct 25	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	Apr 26	May 26
Forecasted Hedge Plan % (w/o Peaking)	90%	91%	93%	88%	91%	92%	89%	77%	77%	77%	78%	78%
Minimum Hedge Plan %	75%	75%	75%	75%	75%	75%	75%	75%	75%	75%	75%	75%
Maximum Hedge Plan Range %	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%
Renewables Portfolio %	31%	26%	25%	27%	29%	31%	23%	21%	29%	32%	36%	38%
Forecasted Load	(24,607)	(27,647)	(27,566)	(23,099)	(20,627)	(19,362)	(21,569)	(23,378)	(21,492)	(22,574)	(20,191)	(21,542)
Forecasted Market Balancing, MWh	(2,413)	(2,583)	(1,907)	(2,839)	(1,821)	(1,458)	(2,355)	(5,354)	(4,950)	(5,201)	(4,522)	(4,664)
Forecasted Hedge % (w/ Peaking)	90%	91%	93%	88%	91%	92%	89%	77%	77%	77%	78%	78%



Forecasted Outer Years Energy Resource Position for GRAN

Power Supply, MWh	2026	2027	2028	2029	2030	2031	2032	2033	2034
Total Resources, MWh	215,667	183,992	140,957	107,834	103,261	103,070	98,163	97,876	97,422
Project Assets	19,325	13,564	7,493	7,493	7,493	7,490	2,654	2,654	2,382
Landfill Project	19,325	13,564	7,493	7,493	7,493	7,490	2,654	2,654	2,382
Contracted Power Supply	196,341	170,429	133,464	100,341	95,768	95,580	95,509	95,222	95,040
Contracted ESP Renewable PPAs	60,986	68,289	68,133	67,920	67,736	67,548	67,400	67,190	67,008
Contracted Bilateral Energy Transactions	135,355	102,139	65,331	32,422	28,032	28,032	28,109	28,032	28,032

Total Power Supply	2026	2027	2028	2029	2030	2031	2032	2033	2034
Forecasted Hedge Plan % (w/o Peaking)	79%	67%	52%	40%	38%	38%	36%	36%	36%
Minimum Hedge Plan %	75%	65%	50%	35%	25%	5%	5%	5%	5%
Maximum Hedge Plan Range %	95%	80%	70%	55%	40%	25%	25%	25%	25%
Renewables Portfolio %	29%	30%	28%	28%	28%	28%	26%	26%	26%
Forecasted Load	(273,796)	(273,096)	(272,438)	(271,809)	(271,182)	(270,541)	(269,898)	(269,300)	(268,724)
Forecasted Market Balancing, MWh	(58,129)	(89,104)	(131,481)	(163,975)	(167,921)	(167,471)	(171,736)	(171,423)	(171,301)
Forecasted Hedge % (w/ Peaking)	79%	67%	52%	40%	38%	38%	36%	36%	36%



Forecasted Prompt 12 Months Energy Resource Cost for GRAN

Project Asset Costs are as forecasted in the MPPA Financial Plan, including fixed costs and all other anticipated costs in addition to Energy costs.

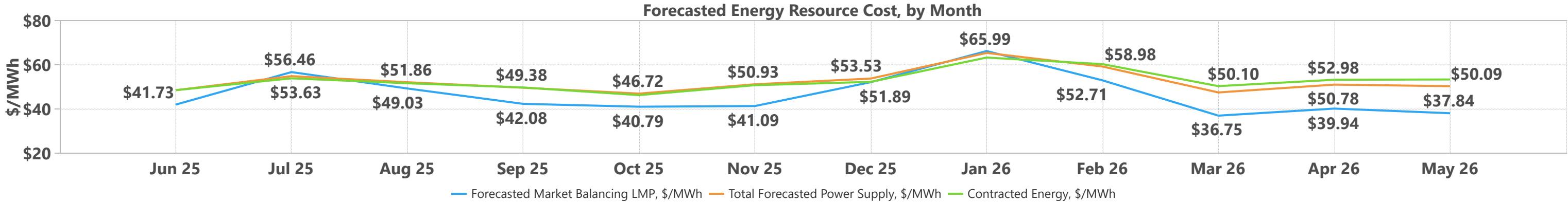
Power Supply \$'s	Jun 25	Jul 25	Aug 25	Sep 25	Oct 25	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	Apr 26	May 26
Total Resources, \$'s	(\$1,071,247)	(\$1,344,115)	(\$1,318,997)	(\$1,002,686)	(\$865,656)	(\$904,602)	(\$999,642)	(\$1,136,173)	(\$993,404)	(\$870,377)	(\$830,201)	(\$896,402)
Project Assets	(\$192,646)	(\$195,899)	(\$180,738)	(\$182,027)	(\$137,671)	(\$194,173)	(\$191,977)	(\$196,648)	(\$177,654)	(\$142,926)	(\$193,227)	(\$202,123)
Landfill Project	(\$192,646)	(\$195,899)	(\$180,738)	(\$182,027)	(\$137,671)	(\$194,173)	(\$191,977)	(\$196,648)	(\$177,654)	(\$142,926)	(\$193,227)	(\$202,123)
Contracted Power Supply	(\$878,601)	(\$1,148,215)	(\$1,138,259)	(\$820,659)	(\$727,985)	(\$710,429)	(\$807,666)	(\$939,525)	(\$815,750)	(\$727,451)	(\$636,975)	(\$694,280)
Contracted ESP Renewable PPAs	(\$278,887)	(\$261,706)	(\$245,965)	(\$226,918)	(\$206,813)	(\$207,997)	(\$154,673)	(\$160,120)	(\$227,951)	(\$269,172)	(\$279,611)	(\$320,933)
Contracted Bilateral Energy Transactions	(\$599,713)	(\$886,509)	(\$892,294)	(\$593,741)	(\$521,172)	(\$502,432)	(\$652,993)	(\$779,405)	(\$587,799)	(\$458,279)	(\$357,364)	(\$373,347)

Locational Basis, \$'s	Jun 25	Jul 25	Aug 25	Sep 25	Oct 25	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	Apr 26	May 26
Locational Basis (Projects)	(\$966)	(\$602)	(\$977)	(\$350)	\$340	(\$668)	\$770	(\$1,362)	(\$1,281)	\$114	\$1,485	(\$549)
Locational Basis (Contracted Power Supply)	(\$14,362)	(\$19,552)	(\$15,948)	(\$18,176)	(\$24,107)	(\$20,862)	(\$33,434)	(\$31,810)	(\$11,896)	(\$5,099)	(\$15,936)	(\$5,513)

Power Supply \$/MWh	Jun 25	Jul 25	Aug 25	Sep 25	Oct 25	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	Apr 26	May 26
Power Supply \$/MWh												
Project Assets												
Landfill Project	\$112.22	\$124.06	\$116.98	\$117.00	\$80.94	\$117.35	\$117.16	\$118.70	\$119.42	\$84.36	\$119.87	\$120.83
Contracted Power Supply												
Contracted ESP Renewable PPAs	\$46.66	\$46.50	\$46.56	\$47.81	\$47.79	\$47.70	\$47.36	\$48.74	\$48.38	\$48.67	\$48.62	\$48.60
Contracted Bilateral Energy Transactions	\$41.36	\$49.64	\$47.39	\$42.54	\$40.79	\$42.26	\$45.63	\$59.58	\$56.83	\$45.16	\$43.03	\$43.41

Locational Basis, \$/MWh	Jun 25	Jul 25	Aug 25	Sep 25	Oct 25	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	Apr 26	May 26
Locational Basis (Projects)	\$0.56	\$0.38	\$0.63	\$0.22	(\$0.20)	\$0.40	(\$0.47)	\$0.82	\$0.86	(\$0.07)	(\$0.92)	\$0.33
Locational Basis (Contracted Power Supply)	\$0.70	\$0.83	\$0.66	\$0.97	\$1.41	\$1.28	\$1.90	\$1.94	\$0.79	\$0.33	\$1.13	\$0.36

Total Power Supply	Jun 25	Jul 25	Aug 25	Sep 25	Oct 25	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	Apr 26	May 26
Forecasted Market Balancing LMP, \$/MWh	\$41.73	\$56.46	\$49.03	\$42.08	\$40.79	\$41.09	\$51.89	\$65.99	\$52.71	\$36.75	\$39.94	\$37.84
Forecasted Market Balancing LMP, \$'s	(\$100,703)	(\$145,796)	(\$93,525)	(\$119,453)	(\$74,281)	(\$59,905)	(\$122,205)	(\$353,272)	(\$260,926)	(\$191,105)	(\$180,610)	(\$176,490)
Total Forecasted Power Supply, \$/MWh	\$48.25	\$54.62	\$51.86	\$49.38	\$46.72	\$50.93	\$53.53	\$65.13	\$58.98	\$47.24	\$50.78	\$50.09
Total Forecasted Power Supply Costs, \$'s	(\$1,187,277)	(\$1,510,064)	(\$1,429,446)	(\$1,140,666)	(\$963,704)	(\$986,037)	(\$1,154,511)	(\$1,522,617)	(\$1,267,507)	(\$1,066,467)	(\$1,025,262)	(\$1,078,954)



Forecasted Outer Years Energy Resource Cost for GRAN

Project Asset Costs are as forecasted in the MPPA Financial Plan, including fixed costs and all other anticipated costs in addition to Energy costs.

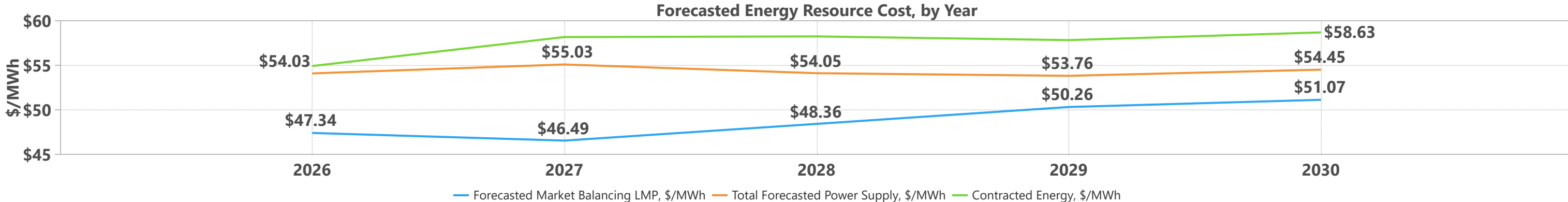
Power Supply \$'s	2026	2027	2028	2029	2030
Total Resources, \$'s	(\$11,830,798)	(\$10,691,769)	(\$8,200,974)	(\$6,229,122)	(\$6,054,203)
Project Assets	(\$2,121,355)	(\$1,492,827)	(\$862,621)	(\$884,885)	(\$907,489)
Landfill Project	(\$2,121,355)	(\$1,492,827)	(\$862,621)	(\$884,885)	(\$907,489)
Contracted Power Supply	(\$9,709,444)	(\$9,198,942)	(\$7,338,353)	(\$5,344,237)	(\$5,146,714)
Contracted ESP Renewable PPAs	(\$2,962,561)	(\$3,362,932)	(\$3,402,332)	(\$3,439,295)	(\$3,478,810)
Contracted Bilateral Energy Transactions	(\$6,746,882)	(\$5,836,010)	(\$3,936,021)	(\$1,904,942)	(\$1,667,904)

Locational Basis, \$'s	2026	2027	2028	2029	2030
Locational Basis (Projects)	(\$4,391)	(\$5,172)	(\$912)	(\$837)	(\$843)
Locational Basis (Contracted Power Supply)	(\$205,387)	(\$189,629)	(\$165,183)	(\$140,647)	(\$135,507)

Power Supply \$/MWh	2026	2027	2028	2029	2030
Power Supply \$/MWh					
Project Assets					
Landfill Project	\$109.77	\$110.06	\$115.12	\$118.10	\$121.11
Contracted Power Supply					
Contracted ESP Renewable PPAs	\$48.58	\$49.25	\$49.94	\$50.64	\$51.36
Contracted Bilateral Energy Transactions	\$49.85	\$57.14	\$60.25	\$58.76	\$59.50

Locational Basis, \$/MWh	2026	2027	2028	2029	2030
Locational Basis (Projects)	\$0.23	\$0.38	\$0.12	\$0.11	\$0.11
Locational Basis (Contracted Power Supply)	\$1.05	\$1.11	\$1.24	\$1.40	\$1.41

Total Power Supply	2026	2027	2028	2029	2030
Forecasted Market Balancing LMP, \$/MWh	\$47.34	\$46.49	\$48.36	\$50.26	\$51.07
Forecasted Market Balancing LMP, \$'s	(\$2,752,074)	(\$4,142,122)	(\$6,358,663)	(\$8,240,571)	(\$8,574,993)
Total Forecasted Power Supply, \$/MWh	\$54.03	\$55.03	\$54.05	\$53.76	\$54.45
Total Forecasted Power Supply Costs, \$'s	(\$14,792,650)	(\$15,028,693)	(\$14,725,732)	(\$14,611,178)	(\$14,765,547)

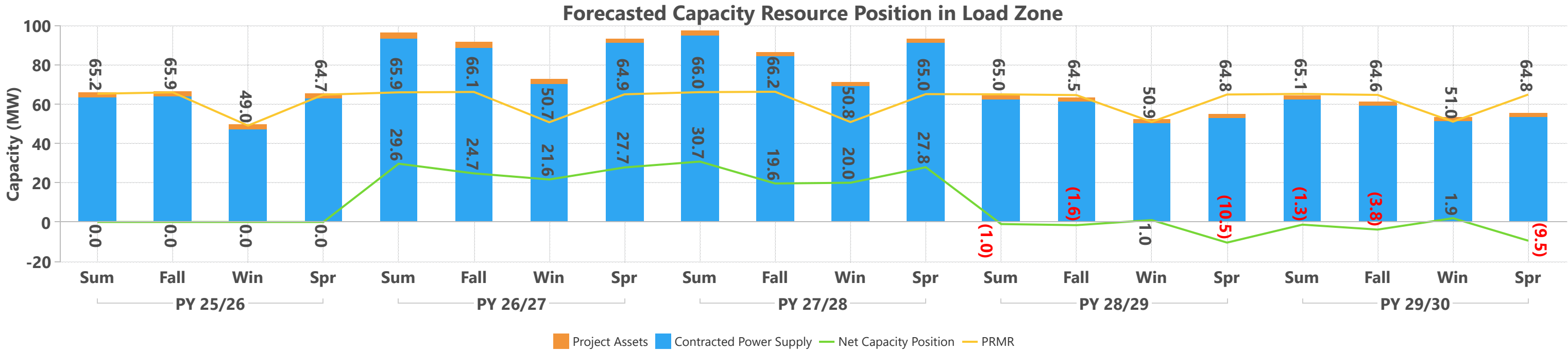


Forecasted Outer Years Capacity Resource Position for GRAN

Capacity Resources, MW	PY 25/26				PY 26/27				PY 27/28				PY 28/29				PY 29/30			
	Sum	Fall	Win	Spr	Sum	Fall	Win	Spr	Sum	Fall	Win	Spr	Sum	Fall	Win	Spr	Sum	Fall	Win	Spr
Net Capacity Position	0.0	0.0	0.0	0.0	29.6	24.7	21.6	27.7	30.7	19.6	20.0	27.8	(1.0)	(1.6)	1.0	(10.5)	(1.3)	(3.8)	1.9	(9.5)
Zone 7	0.0	0.0	0.0	0.0	29.6	24.7	21.6	27.7	30.7	19.6	20.0	27.8	(1.0)	(1.6)	1.0	(10.5)	(1.3)	(3.8)	1.9	(9.5)
Contracted Power Supply	63.4	64.0	47.2	62.8	93.5	88.8	70.3	91.2	95.2	84.3	69.3	91.4	62.5	61.4	50.4	52.8	62.3	59.3	51.5	53.8
Contracted Bilateral Capacity Transactions	50.7	56.0	44.8	51.8	78.4	77.3	67.2	77.3	79.7	74.1	66.5	77.5	55.0	54.3	48.7	50.1	55.6	54.0	50.0	51.3
Contracted ESP Renewable PPAs	12.7	8.0	2.4	11.0	15.1	11.5	3.1	13.9	15.5	10.2	2.8	13.9	7.5	7.2	1.7	2.8	6.7	5.3	1.5	2.6
Planning Reserve Margin Requirement	(65.2)	(65.9)	(49.0)	(64.7)	(65.9)	(66.1)	(50.7)	(64.9)	(66.0)	(66.2)	(50.8)	(65.0)	(65.0)	(64.5)	(50.9)	(64.8)	(65.1)	(64.6)	(51.0)	(64.8)
PRMR	(65.2)	(65.9)	(49.0)	(64.7)	(65.9)	(66.1)	(50.7)	(64.9)	(66.0)	(66.2)	(50.8)	(65.0)	(65.0)	(64.5)	(50.9)	(64.8)	(65.1)	(64.6)	(51.0)	(64.8)
Project Assets	1.8	1.9	1.8	1.9	2.0	2.0	2.0	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
Landfill Project	1.8	1.9	1.8	1.9	2.0	2.0	2.0	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5

Net Contracted Bilateral Capacity	PY 25/26			PY 26/27			PY 27/28			PY 28/29			PY 29/30		
	Net Bilat MW	Net Bilat \$'s	\$/kw-mo.	Net Bilat MW	Net Bilat \$'s	\$/kw-mo.	Net Bilat MW	Net Bilat \$'s	\$/kw-mo.	Net Bilat MW	Net Bilat \$'s	\$/kw-mo.	Net Bilat MW	Net Bilat \$'s	\$/kw-mo.
Total Net Capacity Bilats	(50.8)	(\$2,234,724)	\$3.69	(75.1)	(\$3,864,492)	\$4.29	(74.5)	(\$3,831,299)	\$4.29	(52.0)	(\$2,975,371)	\$4.77	(52.7)	(\$3,014,516)	\$4.77
Sum	(50.7)	(\$235,950)	\$1.55	(78.4)	(\$1,015,036)	\$4.32	(79.7)	(\$1,033,970)	\$4.32	(55.0)	(\$787,057)	\$4.77	(55.6)	(\$795,312)	\$4.77
Fall	(56.0)	(\$675,658)	\$4.02	(77.3)	(\$997,389)	\$4.30	(74.1)	(\$951,859)	\$4.28	(54.3)	(\$776,036)	\$4.77	(54.0)	(\$771,574)	\$4.77
Win	(44.8)	(\$666,111)	\$4.96	(67.2)	(\$852,918)	\$4.23	(66.5)	(\$843,277)	\$4.23	(48.7)	(\$695,997)	\$4.77	(50.0)	(\$714,426)	\$4.77
Spr	(51.8)	(\$657,004)	\$4.23	(77.3)	(\$999,148)	\$4.31	(77.5)	(\$1,002,193)	\$4.31	(50.1)	(\$716,281)	\$4.77	(51.3)	(\$733,203)	\$4.77

Net Capacity Position	PY 25/26			PY 26/27			PY 27/28			PY 28/29			PY 29/30		
	Market Cap MW	Market Cap \$'s	Total Cap \$'s	Market Cap MW	Market Cap \$'s	Total Cap \$'s	Market Cap MW	Market Cap \$'s	Total Cap \$'s	Market Cap MW	Market Cap \$'s	Total Cap \$'s	Market Cap MW	Market Cap \$'s	Total Cap \$'s
Total Net Capacity Position	0.0	\$0	(\$2,234,724)	5.4	\$372,600	(\$3,491,892)	4.9	\$382,200	(\$3,449,099)	(2.6)	(\$212,625)	(\$3,187,996)	(2.4)	(\$199,500)	(\$3,214,016)
Sum	0.0	\$0	(\$235,950)	0.0	\$0	(\$1,015,036)	0.0	\$0	(\$1,033,970)	0.0	\$0	(\$787,057)	0.0	\$0	(\$795,312)
Fall	0.0	\$0	(\$675,658)	0.0	\$0	(\$997,389)	19.6	\$382,200	(\$569,659)	0.0	\$0	(\$776,036)	0.0	\$0	(\$771,574)
Win	0.0	\$0	(\$666,111)	21.6	\$372,600	(\$480,318)	0.0	\$0	(\$843,277)	0.0	\$0	(\$695,997)	0.0	\$0	(\$714,426)
Spr	0.0	\$0	(\$657,004)	0.0	\$0	(\$999,148)	0.0	\$0	(\$1,002,193)	(10.5)	(\$212,625)	(\$928,906)	(9.5)	(\$199,500)	(\$932,703)

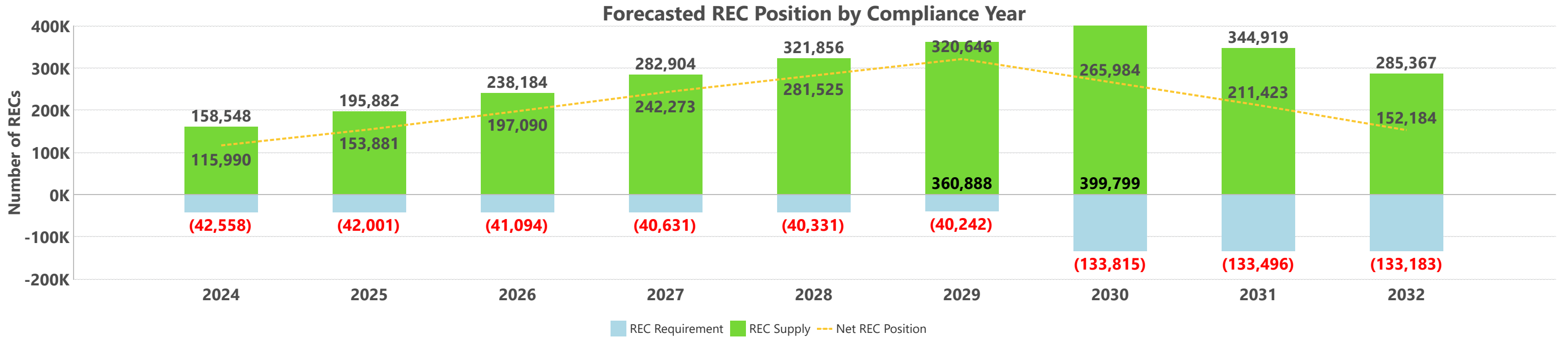


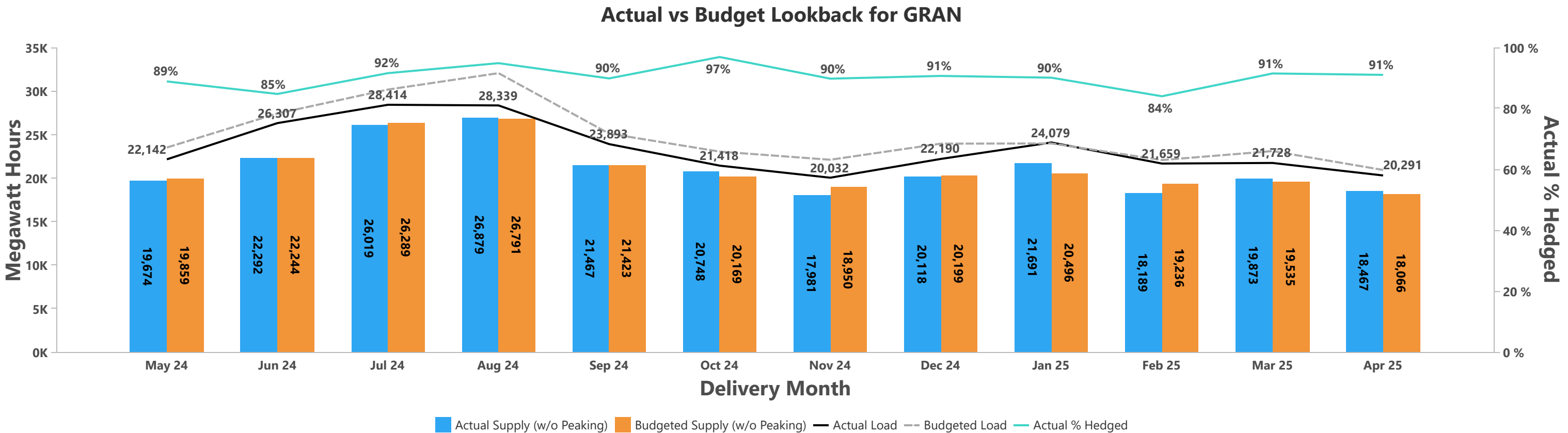
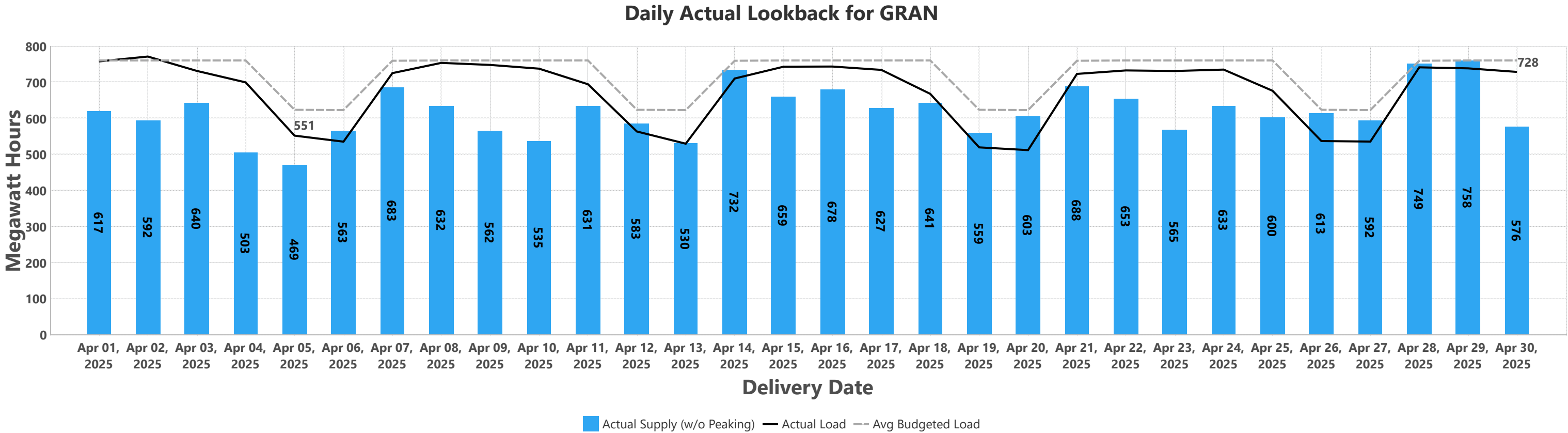
Forecasted Renewable Energy Credit (REC) Position for GRAN

Forecasted REC volumes are based on actual meter data when available and use the latest modeled generation for future timeframes.  
Available Banked RECs in a compliance year reflect the forecasted Net REC Position at the end of the previous year.

Compliance Year	2024	2025	2026	2027	2028	2029	2030	2031	2032
Net REC Position	115,990	153,881	197,090	242,273	281,525	320,646	265,984	211,423	152,184
Available Banked RECs	158,548	115,990	153,881	197,090	242,273	281,525	320,646	265,984	211,423
Hedge Policy REC Requirement	(42,558)	(42,001)	(41,094)	(40,631)	(40,331)	(40,242)	(133,815)	(133,496)	(133,183)
Assembly Solar		10,386	10,610	10,550	10,497	10,447	10,392	10,336	10,289
Assembly Solar Phase II		8,671	8,793	8,746	8,702	8,658	8,612	8,568	8,530
Beebe		6,015	5,802	5,802	5,801	5,803	5,802	5,801	5,802
Brandt Woods Solar		3,707	4,515	4,492	4,477	4,447	4,425	4,403	4,389
Hart Solar			161	7,628	7,618	7,582	7,559	7,537	7,527
Invenergy Calhoun Solar		12,155	13,758	13,710	13,670	13,629	13,584	13,538	13,506
Landfill Project (EDL)		15,592	14,457	8,697	2,638	2,643	2,643	2,643	2,638
Landfill Project (NANR)		4,658	4,839	4,839	4,839	4,839	4,839	4,836	
Pegasus		17,953	17,545	17,545	17,547	17,549	17,548	17,544	17,545
White Tail Solar		755	3,824	3,805	3,794	3,767	3,748	3,729	3,719

Compliance Year	2024	2025	2026	2027	2028	2029	2030	2031	2032
3 Year Avg Retail Sales	(283,721)	(280,006)	(273,963)	(270,875)	(268,874)	(268,282)	(267,629)	(266,991)	(266,365)
Hedge Policy REC Target %	15.0%	15.0%	15.0%	15.0%	15.0%	15.0%	50.0%	50.0%	50.0%
Hedge Policy REC Requirement	(42,558)	(42,001)	(41,094)	(40,631)	(40,331)	(40,242)	(133,815)	(133,496)	(133,183)
VGP REC %	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
VGP REC Requirement	0	0	0	0	0	0	0	0	0





GRAND HAVEN BOARD OF LIGHT AND POWER  
GENERAL MANAGER'S REPORT  
BOARD MEETING OF JUNE 19, 2025

5. B. The BLP Financial Statements and Dashboards for the month ending May 31, 2025, are provided for your information. These financial statements represent the BLP's financial position through 92% of the fiscal year.

<b>Income Statement Budget Variance</b>	
	<b><u>over(under)</u></b>
Total Charges for Service	\$ (16,036)
Other Revenue	409,055
	393,019
Purchased Power	(528,804)
Departments Salary and Fringe	(356,189)
Departments Other	(478,034)
Other	(432,376)
	(1,795,402)
Depreciation	29,836
Non-Operating Revenue (Expenses)	288,838
Transfers to City of Grand Haven	58,144
Increase in Net Assets	\$ 2,389,278

**INCOME STATEMENT**

**Operating Charge revenues** are 91% of annual budgeted revenues. Industrial charges are below budget, yet Residential charges are above budget. We are experiencing an unexpected decrease in usage from our largest industrial customer this year. In total, Kwh's and Sales per Kwh are very close to budget. See below:

<b>Retail Sales Budget Variance</b>			
Kwh Over (Under) Budget	-0.48%	(1,191,120)	Kwh \$ (159,639)
Sales\$ per Kwh Over (Under) Budget	0.43%	\$ 0.00057	per Kwh \$ 142,451
			\$ (17,188)

**Operating expenses** are 85% of annual budgeted operating expenses. All departments are under budget. Purchased power Kwh's purchased are 3% under budget. See below:

<b>Purchased Power Budget Variance</b>			
Kwh Over (Under) Budget	-3.27%	(8,552,448)	Kwh \$ (603,052)
Cost Over (Under) Budget per Kwh	0.42%	\$ 0.29302	per Kwh \$ 74,248
			\$ (528,804)



GRAND HAVEN BOARD OF LIGHT AND POWER  
GENERAL MANAGER'S REPORT  
BOARD MEETING OF JUNE 19, 2025

Year-to-Date **Renewable Energy Purchases equal 68,220,391 Kwh's, or 26.9%, of total power purchases.**

**The Increase in Net Position for the year is equal to \$7,341,511.**

**BALANCE SHEET**

**Cash and Cash Equivalents are \$29,140,164.** This is \$11M above the minimum cash reserve of \$18M and does not include funds set aside for remediation, bond funds and working capital held with MPIA and MPPA.

The **Capital Plan** approved for FY25 was \$5,747,500. As of May 31, 2025, 54% of the capital projects budgeted funds have been disbursed.

5. F. Confirm Purchase Orders – There are six (6) confirming Purchase Orders on the Consent Agenda this month of **\$174,714** for your confirmation.

Confirming Purchase Orders on the Consent Agenda are either routine expenses within approved budgeted parameters, with prequalified and approved contractors or vendors, services or supplies that may have required immediate attention, again using prequalified and approved contractors or vendors when possible or change orders under a previously approved PO (and we are seeking after the fact concurrence/confirmation of the expenditure by the Board).

The PO number, contractor name, associated dollar value, and short description of this item are listed on the agenda.

All applicable purchasing policy provisions associated with these Purchase Orders were followed. Budgeted funds are available. Staff is recommending approval. (Board action is requested through the approval of the Consent Agenda).

6. A. Approve Purchase Orders – There are six (6) Purchases Order totaling **\$338,387** on the regular agenda.

The PO number, contractor name, associated dollar value, and short description of this item are listed on the agenda.

I, or an appropriate staff member, can answer any further questions you may have regarding these items.

All applicable purchasing policy provisions associated with these items were followed. Capital planning or budgeted funds are available. Staff is recommending approval of these Purchase Orders. (Board action is requested).

GRAND HAVEN BOARD OF LIGHT AND POWER  
GENERAL MANAGER'S REPORT  
BOARD MEETING OF JUNE 19, 2025

RS/dm

Attachments 6/12/25



# Memorandum

To: Rob Shelley  
From: Lynn Diffell  
cc:  
Date: June 19, 2025  
Subject: Proposed 2025 Year End Write-Offs

The attached listing is my recommendation for the fiscal year end write-offs. A comparison to last year is as follows:

	<u>2025</u>	<u>2024</u>
<u>Electrical Sales</u>		
All Other Electrical Sales - Number	80	96
All Other Electrical Sales - Amount	\$11,213.83	\$12,628.53
<u>Miscellaneous Accounts Receivable</u>		
Misc. Accounts Receivable - Number	0	3
Misc. Accounts Receivable - Amount	<u>\$0.00</u>	<u>\$13,214.00</u>
 Total Proposed Write-Offs	 <u>\$11,213.83</u>	 <u>\$25,842.53</u>
 Per Customer Account	 \$140.17	 \$131.55
% of Annual Retail Sales	.030%	.034%

We do continue collection efforts on these accounts, which includes reporting the balances to a collection agency.

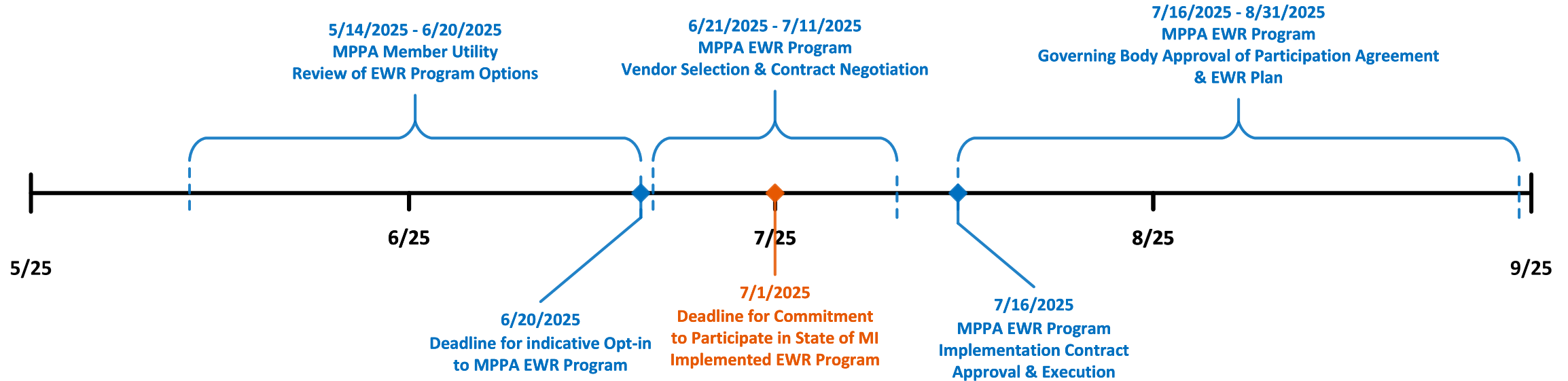
I recommend the Board approve the following.

**Move to write off \$11,213.83 in electrical sales as bad debts.**



# Public Act 229

## Energy Waste Reduction (EWR) Legislative Compliance Timeline



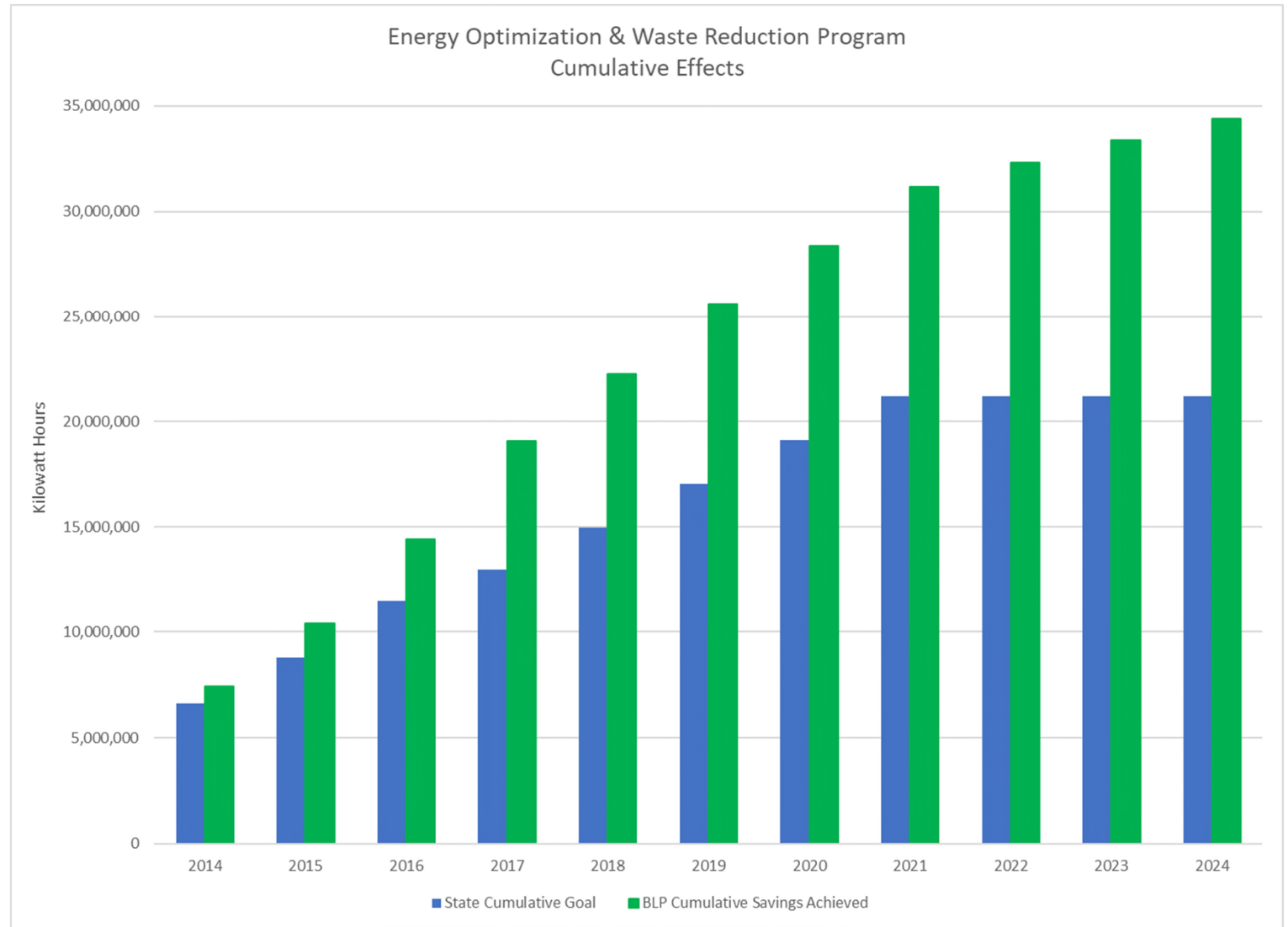
# Energy Waste Reduction Program for 2026 & 2027

**Presentation to Board of Directors**  
**June 19, 2025**



# ENERGY WASTE REDUCTION

- ✓ Over **\$4,300,000** invested in local energy efficiency programs since 2012.
- ✓ Over **4.3 MW** of Energy Demand Reduction.
- ✓ Over **34,000,000 kWhrs** Claimed Energy Savings Cumulatively.



# NEW STATE REQUIREMENTS



## **PA 229 - ENERGY WASTE REDUCTION (EWR)**

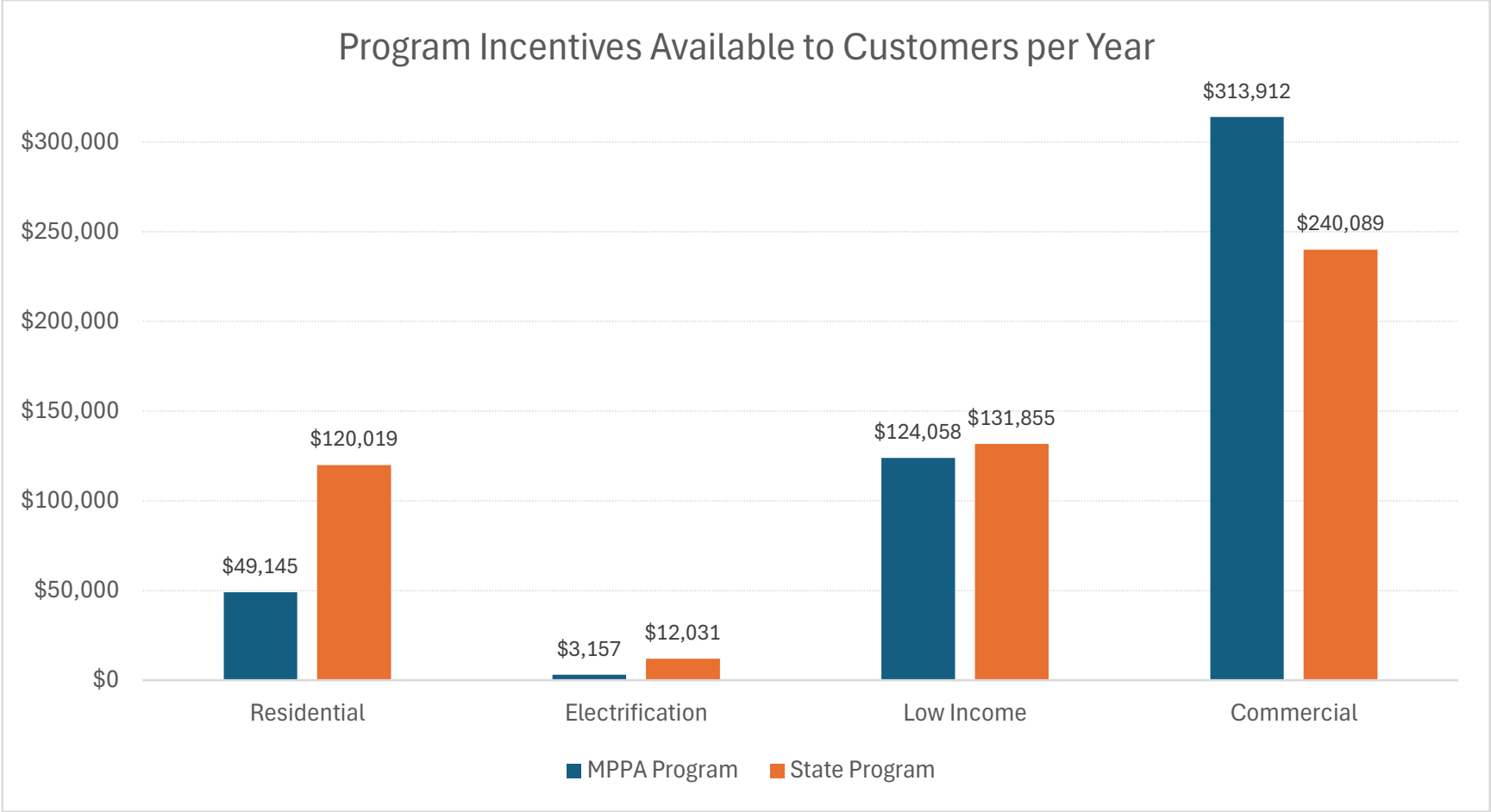
1.5% OF ENERGY SALES STARTING IN 2026

DEVELOPMENT OF LOW-INCOME PROGRAM  
THAT IS 25% OF TOTAL PROGRAM SPENDING

### **Two Options:**

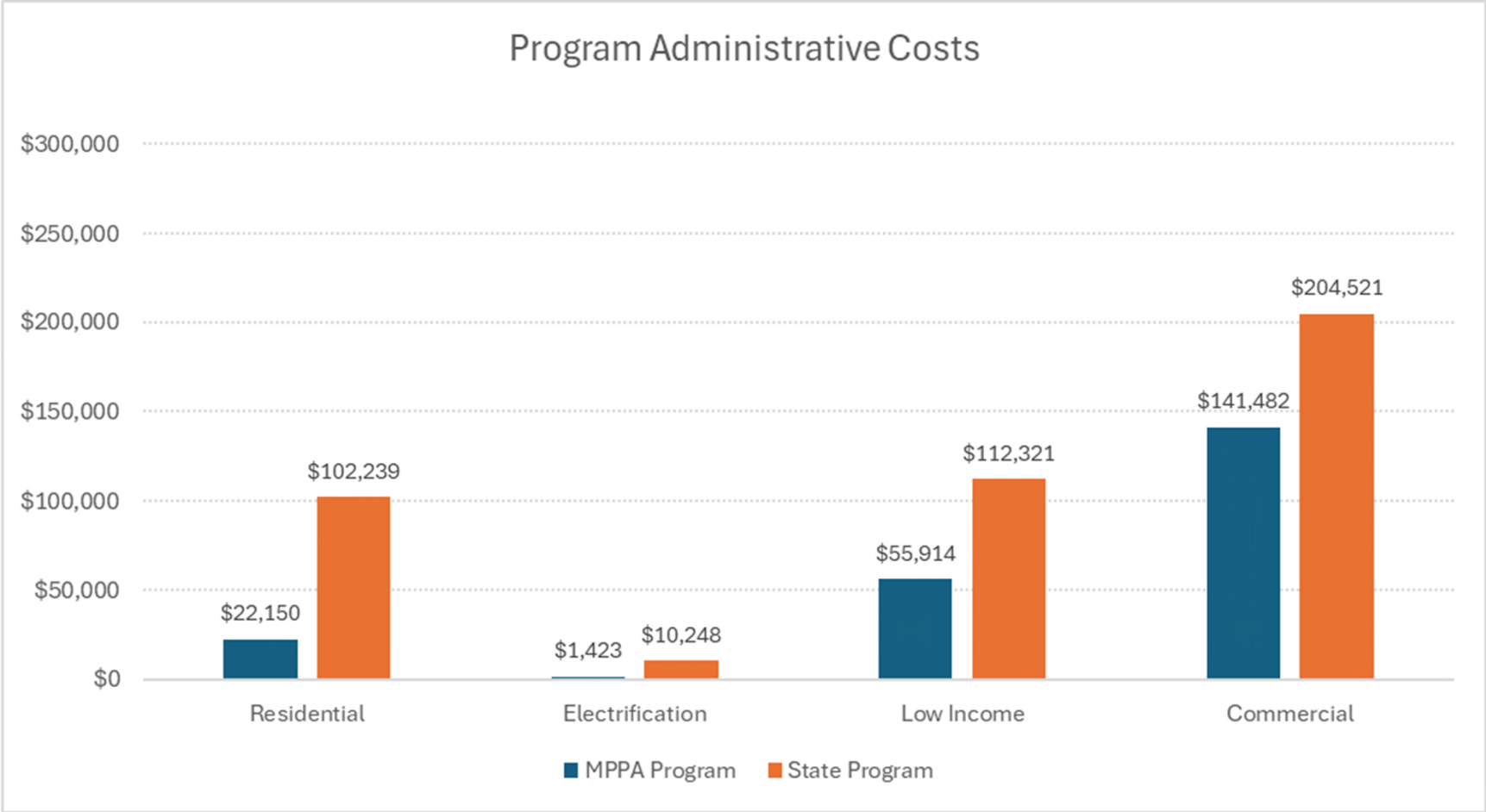
1. State Administered Program (2-year commitment)
  - A. State picks the program administrator
    - i. Clear Results - \$933,323/year
2. MPPA Administered Program (4-year commitment)
  - A. Low bid out of 2 companies that submitted proposals
    - i. Franklin Energy - \$711,411/year

# Incentives Available to Each Customer Class





# Program Administrative Costs



# Calculations

State EWR Program Average Annual Cost for 2026-2027 (1.35% Savings Goal)

Utility	Budget Category/Customer Class	Total Annual Program Budget	% of Funding
Grand Haven	Residential	\$222,258	24%
	Residential Efficient Electrification	\$22,279	2%
	Residential Low Income	\$244,176	26%
	Commercial & Industrial Prescriptive & Custodial	\$444,610	48%
	Total	\$933,323	100%

\* Data provided by MPPA on 5/28/2025

Low Income Subsidization across all customer classes

Residential Total with Low Income Prorata	\$331,180	35%
Commercial & Industrial with Low Income Prorata	\$602,143	65%

Additional Program Costs

3rd Part Audit	\$53,250	to cover 10% of requirement
Renewable Energy Credit Costs (\$/MWh)	\$6.50	

## Rate Structure Determination

	Current Customers per Rate Class (total)	Previous Calendar Year Electric Sales (kWh)	Savings from EWR 1.35% (MWh)	Savings from RECs 0.15% (MWh)	Quoted Program Costs \$	REC Substitute \$	3rd Party Audit Share \$	Streetlight Share \$	Total Program Costs \$	Monthly Customer Fixed Charge \$/Month
Residential	13,275	87,946,421	1,187	132	\$331,180.44	\$857.48	\$17,204	\$907	\$350,149.24	\$2.20
Commercial & Industrial										
General Service - Large Primary	50	120,512,746	1,627	181	\$393,822.56	\$1,175.00	\$23,575	\$1,243	\$419,815.46	\$699.69
General Service - Large Secondary	215	32,656,127	441	49	\$106,716.67	\$318.40	\$6,388	\$337	\$113,760.14	\$44.09
General Service - Primary	10	1,918,560	26	3	\$6,269.65	\$18.71	\$375	\$20	\$6,683.45	\$55.70
General Service - Secondary	1,623	28,364,634	383	43	\$92,692.54	\$276.56	\$5,549	\$293	\$98,810.39	\$5.07
Lighting Service	NA	808,209	11	1	\$2,641.14	\$7.88	\$158			
Commercial & Industrial Total		184,260,276	2,488	276	\$602,142.56	\$2,654.02	\$53,250		\$639,069.44	
Combined Total		272,206,697	3,675	408	\$933,323.00				\$989,218.68	

## Nest Steps



Board Action being requested today:

Award the Energy Waste Reduction Program to the State Administrator

Board Action that will be requested next month:

Approve the rate structure that will be implemented on customers bills at the end of 2025.

Policy Name	Last Approved	Comments
Billing Outside Parties Policy	5/22/2014	Removed specific dollar amounts. The policy now refers to a separate rate sheet which is regularly updated.
Cash Reserve Policy	New	
De Minimis Benefits Policy	11/9/2015	Format update for consistency, no other changes.
Employee Handbook Update Policy	New	Enables the General Manager to approve routine Handbook updates.
Employee Recognition Policy	4/5/2016	Updated program dollars and frequency. Now incentivises performance along with longevity.
Energy Risk Management Policy	7/18/2012	Added heading page for consistency, no other changes.
Executive Management PTO Matching Option	11/12/2013	Updated to list 457 instead of HCSP. The HCSP option is no longer allowed by regulation.
Investment Policy	New	
Payment Card Security Policy	2/28/2019	Added heading page for consistency, no other changes.
Purchasing Authority	New	
Purchasing Policy	2/16/2023	
Record Retention Policy	New	Policy officially adopts the State of Michigan retention schedules. The separate procedure for compliance has not changed.
Retiree Recognition Policy	2/24/2000	Updated program dollars due to selective gift catalog availability.
Social Security Number Privacy Policy	4/27/2006	Format update for consistency, no other changes.
Technology Use Policy	7/25/2016	General minor updates were made. Policy gives the General Manager the authority to make routine updates in the future.

Highlighted denotes not included in this package

# Grand Haven Board of Light & Power Policy

<b>Title</b>	Billing Outside Parties
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	10/02/1989, 09/30/1993, 05/25/1995, 12/21/1995, 05/22/2014
<b>Responsible Person</b>	General Manager

## Introduction

Billing outside parties for work performed and/or materials provided by the Board.

## Policy

### 1. Miscellaneous Work

- a. Effective November 1, 1989, all miscellaneous work performed for outside parties, which is chargeable to them, is to be billed as follows:
  - i. Labor will be billed at direct wages of the employees actually working on the job plus direct engineering time, if any, plus current rate for fringes and non-productive time, plus 10% to cover supervision costs. The current fringe rate is listed on the Labor and Equipment Rate Sheet.
  - ii. The materials will be charged on a LIFO basis or, if it is specifically purchased, at actual purchase price plus 10% handling and inventory costs. If a realizable salvage value on items replaced is recognized, it will be deducted prior to the application of the handling and inventory charge.
  - iii. Equipment rates will be billed per hour at the current rates assigned by the General Manager as listed on the Labor and Equipment Rate Sheet.

### 2. Sale of In-Stock Materials to Customers

- a. Customers who own their own equipment are to make every attempt to obtain equipment, materials, supplies, etc., from other sources than the BLP. The BLP will aid customers with the provision of stock inventory items when all other attempts by the customer to obtain the equipment have failed and/or in an emergency basis, or as Engineering and Distribution deem appropriate. The price of the equipment is to be contractor's replacement cost, plus 20%.

### 3. Damage to BLP Equipment

- a. The BLP will accumulate all the costs of repair to damaged equipment and bill the appropriate party.

# Grand Haven Board of Light & Power Policy

<b>Title</b>	De Minimis Benefits
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	11/09/2015
<b>Responsible Person</b>	General Manager

## Introduction

The Internal Revenue Service defined de minimis fringe benefits as “one for which, considering its value and the frequency with which it is provided, is so small as to make accounting for it unreasonable or impractical”. De minimis benefits are excluded under Internal Revenue Code section 132(a)(4) and include items which are not specifically excluded under other sections of the Code.

## Policy

1. Employee compensation may include additional De Minimis benefits as provided at the discretion of the General Manager within the annual budget.

# Grand Haven Board of Light & Power Policy

<b>Title</b>	Employee Handbook Update
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	None
<b>Responsible Person</b>	General Manager

## Introduction

Governing Boards must ensure adequate personnel policies are in place to comply with employment laws and reduce organizational risk while avoiding excessive Board involvement in day-to-day operations. The purpose of the Employee Handbook Update Policy is to define what type of handbook provisions the General Manager has authority to update and what type of provisions require Board approval.

## Policy

1. The General Manager is authorized to periodically review and update the Employee Handbook.
2. Board approval is required for handbook changes which:
  - a. Have a significant financial impact on the organization, or
  - b. Have a direct impact on the General Manager's compensation package including paid holidays, employer retirement plan contributions, paid time off accrual rates, and similar items.

# Grand Haven Board of Light & Power Policy

<b>Title</b>	Employee Recognition
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	"Years of Service Awards" adopted 03/02/1987, 11/04/1992, 01/20/2000, 04/30/2001, and 04/05/2016
<b>Responsible Person</b>	General Manager

## Introduction

In recognition of an employee's length of service and job performance, the Employer will implement the following employee recognition program.

## Policy

1. The Employee Recognition program is available only to full time employees.
2. Recognition pay will be distributed to employees in a single direct deposit, subject to normal payroll deductions and taxes, the first regular payroll in December each year.
3. Years of service will be based on completed years of service through December 31<sup>st</sup> of each year and calculated using the employee's most recent hire date.
  - a. Example: An employee hired March 1, 2025 would receive the 5 year service incentive in December 2030.
4. Employees who are terminated, become deceased, quit employment, or have a leave of absence more than 90 days during the current calendar year, are not entitled to that year's recognition benefit.
5. Employees retiring during the calendar year will receive a pro-rated benefit paid out in their final paycheck reflecting their time as an active employee for that year.
  - a. Example: An employee who retires June 30<sup>th</sup> would be eligible to receive 50% of the incentive at the appropriate completed years of service level.
6. An employee must receive an overall performance rating of "proficient" or better on their most recent performance evaluation to qualify for the recognition incentive.
7. The General Manager is authorized to adjust this program to reflect reasonable and customary changes due to inflation or other market-driven factors, provided the program remains within budgetary constraints.
8. Incentives will be awarded according to the following schedule:



Years of Service	Incentive Amount	Years of Service	Incentive Amount
1		11	\$1,050
2		12	\$1,100
3		13	\$1,150
4		14	\$1,200
5	\$500	15	\$1,500
6	\$550	16	\$1,550
7	\$600	17	\$1,600
8	\$650	18	\$1,650
9	\$700	19	\$1,700
10	\$1,000	20+	\$2,000

## Grand Haven Board of Light & Power Policy

<b>Title</b>	Energy Risk Management
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	07/18/2012
<b>Responsible Person</b>	General Manager

# **Grand Haven Board of Light & Power**

## **Energy Risk Management (ERM) Policy**

### **1. Policy Purpose**

The purpose of this document is to formalize the policies of the Grand Haven Board of Light & Power (BLP) regarding managing energy risks. Accordingly, this policy will set forth BLP's:

- energy risk management objectives
- energy risk governance structure and responsibilities
- scope of business activities governed by this policy
- transaction authority delegations
- credit management practices and requirements

BLP intends that its energy risk management program will support the advancement of its strategic plan, conform to its existing policies and contracts, and will properly manage its business and financial risks through:

- prudent oversight
- adequate mitigation of risks consistent with each member's risk tolerance
- sufficient internal controls and procedures

Managing the energy risks of BLP's business entails the coordination of resources and activities among multiple departments within BLP.

### **2. Energy Risk Management Objectives**

The mission of BLP is to provide reliable, cost effective and environmentally responsible electric utility services to our local retail customers.

Managing energy risk on behalf of the utility is consistent with the purpose and mission of BLP, and also serves the following objectives:

- maintain risk within their desired tolerances for a defined period into the future
- mitigate price volatility to customers
- maintain the value of the utility's assets/resources
- participate in commodity markets and derivative instruments for hedging, and not for speculative purposes
- set forth credit risk management practices
- define the authority granted by the BLP Board to the BLP General Manager (GM) to execute and delegate authority to execute energy related transactions
- promote a risk management culture and set appropriate risk mitigation measures
- provide for adequate BLP Board oversight of energy transactions

### 3. Scope of Business Activities Governed by this Policy

The scope of this policy is designed to address the management of energy risk associated with BLP and transactions made by BLP, including but not limited to:

- commercial operational risk
- commodity price risk
- volumetric risk
- operations risk
- power delivery and congestion risk
- counterparty contract and credit risk

Definitions of these risks along with a more complete list of the risks that BLP needs to manage are included in Appendix A.

### 4. Risk Governance Structure and Responsibilities

The BLP Board shall be responsible for oversight of the Energy Risk Management program consistent with this Policy. Supporting controls, policies and procedures will be implemented and aligned throughout the risk governance structure with distinct roles and responsibilities that result in a comprehensive risk control environment. Governance and controls include the organizational structure, policies, reporting process and procedures, establishment of risk tolerances and power supply objectives, and appropriate segregation of responsibilities.

The governance structure includes the following elements:

#### a. BLP Board of Directors (BLP Board) – Responsibilities and Duties:

- possess a basic understanding of BLP's energy risk management procedures and practices as they relate to BLP entering into market transactions on its behalf
- designate the electric utility's **Member Authorized Representative**
- determine authority limits of the Member Authorized Representative to approve risk management transactions or the delegation of such authority to MPPA
- affirm the energy hedging strategies and services provided by MPPA as outlined in the MPPA Hedge Policy through oversight of its Member Authorized Representative and his or her participation on the appropriate Hedge Committee

#### b. MPPA Board – Responsibilities and Duties

- possess a basic understanding of energy risk management in general and MPPA's program, policies, and procedures in particular
- approve MPPA risk management objectives
- approve General Manager and staff authority limits to conduct risk management transactions
- periodically review, make recommended changes to, and approve the Energy Risk Management Policy that establishes an overall framework for evaluation, management, and control of risk by the Agency

- approve Agency participation in specific commodity markets and the use of any derivative instruments
- receive reports by the independent risk management function of MPPA on MPPA's compliance with the ERM Policy

**c. Member Authorized Representative – Responsibilities and Duties**

- provide appropriate risk management information to the BLP Board
- gain appropriate approvals from the Board of Directors to approve MPPA's ERM and Hedge Policies and the selection of the Hedge Plan to be utilized
- gain appropriate approvals from the BLP Board for execution strategies and transaction authority delegations as they relate to the BLP entering into market transactions in accordance with transaction authority matrix included in Exhibit B
- approve participation in specific commodity markets and the use of any derivative instruments by BLP (if such transactions are allowed by MPPA's Board and the BLP Board as appropriate)
- receive reports by the independent risk management function of MPPA, as defined herein, on compliance with the BLP's hedge policy selection

**d. MPPA General Manager – Responsibilities and Duties**

- Assign MPPA staff to serve as members of the MPPA Internal Risk Management Committee
- possess authority to approve transactions within the limits identified in the Transaction Authority Matrix after receiving any necessary approvals specified therein
- determine proper organization, separation, or consolidation of functional activities
- assure prudent administrative procedures are established for execution of commodity and derivative transactions, contract controls, credit controls, transaction controls, risk monitoring and measurement requirements, settlement controls, and other energy risk management activities
- ensure that the identification and quantification of risks and related risk mitigation strategies are integrated into the strategic planning process.

**5. Transaction Authority Requirements**

The purpose of this section is to define the authority granted by the BLP Board through the Member Authorized Representative to the MPPA General Manager to execute and delegate authority to execute energy related transactions. Furthermore, it sets forth clarity and empowerment among those with transaction authority and is designed to encourage communication among individuals with transaction authority and the BLP Board. Changes to the Authority Matrix must be approved by BLP's Board of Directors using the Matrix to delegate transaction authority as it may relate to MPPA entering into market transactions on the BLP's behalf.

**a. Objectives**

The objectives of the BLP Transaction Authority Requirements are to define:

- who has authority to execute transactions and any limits placed on such authority

- the commodities and products that can be transacted
- counterparty contract and credit requirements
- the process for approving new commodities, products or locations
- BLP's intentions regarding hedging and speculating
- other relevant factors associated with due diligence in authorizing transactions to be executed

**b. Procedural Requirements**

The following defines procedural requirements that apply to all commodities and products transacted under this Transaction Authority Requirements document.

**Execution Authority**

Execution Authority is outlined by commodity through the Transaction Authority Matrix. Appendix B illustrates the initial Transaction Authority Matrix at the writing of this policy and serves as a template for future transaction authority matrices that may be developed. The Transaction Authority Matrix may be revised or amended at any time and for any reason by action of the BLP Board.

The Authority Matrix identifies Board authorized transactions for the Member Authorized Representative and explicitly provides for delegation of the Member Authorized Representative's authority to MPPA.

**Contract Requirements**

Transactions with counterparties shall only be permitted if MPPA has:

- an active, valid, and executed agreement enabling such transaction activity with that counterparty such as a "standard" EEI or ISDA as may be amended and approved as appropriate
- a long-form confirmation (used in-lieu-of a permanent agreement, when necessary, only if approved by the MPPA CFO)

**Credit Sleeving**

No sleeving transactions for credit purposes shall be executed. (Note: Sleeving is an arrangement where a more financially reputable entity acts as middleman for a smaller, undercapitalized entity in the purchase or sale of energy.)

**Record of Transactions and Deal Capture**

All transactions must be executed and captured in accordance with MPPA's Energy Risk Management Policy.

**Speculation**

No speculative transaction activities shall be permitted, and no speculative transaction positions shall be initiated. Transacting will be permitted only for purposes of hedging and portfolio optimization.

**Non-Standard Products Requiring Board Approval**

The BLP Board must approve any transaction that involves commodities or products that are not covered by the approved Authority Matrix.

**6. Credit Management Requirements**

The BLP is relying on MPPA to ensure that wholesale counterparties submit a copy of their company's most recent Creditworthiness Assessment from the Midwest Independent Transmission System Operator, Inc. (MISO) that is compiled in accordance with MISO's Credit Policy (Attachment L of the Energy Markets Tariff) to MPPA. The credit limit established as a result of the review performed by MISO will be used to establish the credit limit for bilateral transactions with each counterparty.

Counterparties will have continuous evaluation as they may, from time-to-time, appear in financial/trade publications that will be reviewed by MPPA. Items of risk significance relating to counterparties will be noted and cause reassessment. Such items will include, but are not limited to, downgrade events or business practices that are not conforming to appropriate ethics. In such event, or any other event occurs that triggers a review by MISO of the counterparty's creditworthiness, the new letter from MISO will promptly be requested and obtained from the counterparty before new transactions with that counterparty will be allowed.

If the proposed counterparty fails to meet the evaluated criteria, but there is a sufficient reason to justify transacting with the counterparty, then the counterparty will be required to make a prepayment for any purchases the counterparty makes from BLP. Based upon the results of the analysis for the counterparty, an unsecured transaction limit and a list of any special conditions will be prepared for the counterparty.

**7. Counterparty Concentration Risk Mitigation**

- BLP is relying on MPPA to ensure that they always maintain relations and agreements with at least three (3) counterparties that are actively trading in MISO.

**8. Written Agreements Covering Transactions**

MPPA shall not enter into a Power Purchase Commitment or "PPC," on behalf of the BLP, unless: (i) the PPC is covered by the Energy Services Agreement with the BLP; or (ii) the PPC is covered by a written agreement with the BLP, the form of which has been approved by the MPPA Board and the BLP Board and executed by MPPA and the BLP, and the BLP has delivered an opinion of local counsel, to the effect that the written agreement has been approved by the participating member's governing body and is a valid and binding agreement of the participating member, enforceable against it in accordance with its terms.

**9. Working Capital Requirements**

The BLP Board will maintain an adequate level of working capital on account with MPPA during the duration of a transaction that has been executed by MPPA on the BLP's behalf in accordance with the agreement between MPPA and the BLP covering the transaction.

**10. Financial and Physical Firmness of Energy**

The BLP will determine a minimum percentage level of its Plan's energy requirements that will be delivered at a firm price consistent with this Policy's Transaction Authority.

**11. Transaction Duration and Maturity Diversity**

The BLP will develop transaction criteria to ensure duration and maturity diversity.

**12. Policy Effective**

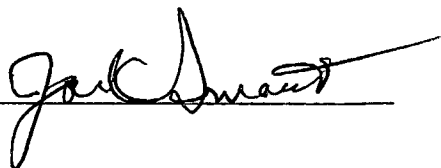
This Energy Risk Management Policy is in effect upon the BLP Board of Director's approval and shall remain in effect until a replacement policy has been approved by the Board superseding this Energy Risk Management Policy.

**13. Responsibility**

It shall be the responsibility of the Board of Directors, through its supervision and oversight of BLP's General Manager, to ensure compliance with this policy.

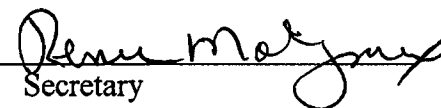
Approved: \_\_\_\_\_

Chair



Attest: \_\_\_\_\_

Secretary



Effective: \_\_\_\_\_

July 18, 2012



## Appendix A

### Definition of Risks

**Commercial operational risk** is the risk of loss from inadequate or failed internal processes, people, and systems or the lack of skills or tools to manage risk. This includes the lack of appropriate risk management policies and procedures including trading liquidity and separation of duties. It can also include the risk management skills or the people, resources and systems to manage the risk.

**Commodity market price risk** is the risk of loss due to potential fluctuations in the prices of an underlying energy commodity. In the wholesale power market, BLP has risk that commodity prices rise, spike or are generally high when it is short of meeting its firm supply obligations. BLP has risk that prices fall or are generally low when it has excess capacity or electric energy compared to its firm supply obligations.

Due to heavy reliance on coal generation units, BLP has a natural short position in the coal that it needs to supply fuel to its generating resources.

Commodity market price risk occurs across all tenures, from the hourly market to the long-term forward market (5 years +). BLP is exposed to commodity price risk for power, coal, natural gas, emission allowance (SO<sub>2</sub> and NO<sub>x</sub>), fuel oil and various bulk materials (e.g. ammonium, limestone) that exhibit price volatility.

**Contract risk or Counterparty performance risk** is the risk of a potential adverse occurrence of a counterparty's ability to operationally perform on an agreement or due to contractual provisions that leave MPPA with no recourse under an event of default.

**Concentration risk** is the risk of having large exposures to significant power supply components. Concentration risk can be found with suppliers (contract and credit risk), generation units (outage risk), unit technology (environmental), native load customers (smelters).

**Credit risk** is the risk of a potential adverse occurrence of a counterparty's ability to pay its obligations (debts) to BLP or the supplier declares bankruptcy and abrogates a supply contract that must be replaced during a time of higher commodity market prices.

**Delivery risk** is the risk that BLP cannot meet a firm supply obligation due to a transmission constraint. Delivery risk is natural to BLP in meeting its firm supply obligations and reliability of service. BLP can also be exposed to delivery risk in the transportation of its fuel supply.

**Cash margin risk** is the risk associated with inadequate cash flow resulting from margin requirements of a contractual agreement. For example, the EEI Master Agreement provides that counterparties may margin each other when they are overexposed above credit thresholds that were negotiated between the parties when the agreement was executed. Credit exposures include

replacement cost exposure on a mark-to-market basis when a counterparty's position is out-of-the money.

**Operations risk** is the risk associated with physical assets. This would include failures or outages associated with generation units, fuel delivery systems (weather or mechanical), generation step-up transformers, the transmission system, control systems, or other critical components associated with the production or delivery of electricity.

**Volumetric risk** is the risk that energy commodity volumes will vary from expected and result in a potential loss due to changing commodity market prices. The primary volumetric risks that BLP is exposed to are load forecast/ weather variability risk, forced outage/ de-rate risk, loss of load, and transmission delivery risk, and transmission congestion risk.

**Load forecast/weather variability risk** is the risk that actual loads differ from forecasted loads due to the error in weather forecasts and load forecasts. This risk is natural to BLP's portfolio since it serves retail load. Since this risk will result in BLP being unintentionally long or short in the spot market, it naturally results in hourly market price risk.

**Forced outage and de-rate risk** is the risk that a generating unit does not perform when it is expected to be available, or when it performs below expected capability. This risk is natural to BLP's portfolio since it owns and operates generation units to meet its load requirements. Since this risk will result in BLP being unintentionally short in the market, it also naturally results in market price risk.

**Loss of load risk** is the risk that BLP loses a significant portion of one of its customers' load, for example an industrial customer, and that the market price for electricity coincidentally falls below the sales price of the lost load and thereby creates a financial strain on BLP. However, if market prices for electricity remain above the sales price of a potential lost load it would create a financial benefit to BLP.

**Congestion risk** is the risk of negative price differentials between the location of power supplies and the demand location. If BLP needs to buy electricity and the transmission system is congested, it would pay a premium to secure the needed electricity, if it is available at all. If BLP has excess electricity to sell and the transmission system is congested, then it may not be able to sell the excess or may have to sell at a discounted price to a non-congested area. Congestion risk typically manifests itself in power commodity market price risk.

## Appendix B

### Bilateral Electric Power and Transmission Transaction Authority Matrix

The following outlines transaction limits, definitions, and procedural requirements for power and power transmission transactions including capacity.

Title	Product	Term	Required Transaction Approvals
MPPA GM or his delegated representative	Electric Power, Trans., and Capacity	> 1 Year	Any transaction with a term greater than one year must be approved by the Member Authorized Representative and the BLP Board of Directors who may identify price and/or volume restrictions
		> 1 Month $\leq$ 1 Year	Any transaction with a term greater than one month but less than or equal to one year must be approved by the Member Authorized Representative who may identify price and/or volume restrictions
		$\leq$ 1 Month	None, unless the appropriate Member Authorized Representative identifies in writing certain price and/or volume restrictions

In addition to the above term limits, any transaction over \$2,000,000 must be approved by the BLP Board of Directors.

### **Bilateral Electric Power and Transmission Transaction Trading Authority Matrix Explanations**

- Authorized products include electric power and transmission as well as bilateral ancillary services and capacity. MISO Module E Capacity as well as capacity transacted via the MISO and PJM capacity auctions are specifically authorized hereunder.
- MISO and/or PJM authorized products are Generation and Demand Awards, Import/Export Transactions, Ancillary Service Awards, and Financial Transmission Rights. All such products must follow all applicable MISO requirements.
- The transaction approval requirements apply to both purchases and sales

### **Delivery Locations**

Transacting at delivery locations outside the eastern interconnection is not permitted. Transacting at delivery locations that are normal to the daily course of business for MPPA, to the extent transmission is available, is authorized as follows:

**Unrestricted Delivery Locations**

- MISO – Michigan Hub
- MISO – Member Load Commercial Pricing (CP) node or any other CP Node within Michigan
- MISO – Cinergy Hub/Indiana Hub
- MISO – Minnesota Hub (for Marquette)

Transacting at any other delivery locations within the eastern interconnection must be approved consistent with the Authority Matrix above.

**Firmness of Power**

The product firmness of all transactions must be provided for in an executed agreement between MPPA and the appropriate counterparty. Sales commitments must never be more firm than the supply source.

**Transmission Firmness and Volume**

Transmission purchases need to be of equal firmness and volume to the energy component that such transmission purchase is associated with, unless approved otherwise consistent with the Authority Matrix above.

**Responsibility**

It shall be the responsibility of the BLP Board and the BLP General Manager to ensure compliance with this Authority Matrix.

Approved: Joel Hurst Chair      Attest: Debra Morgan Secretary

Effective: July 18, 2012

## Grand Haven Board of Light & Power Policy

<b>Title</b>	Executive Management Paid Time Off Matching Option
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	11/12/2013
<b>Responsible Person</b>	General Manager

### Introduction

With the access to smart phones, iPads and laptop remote access, the Executive Management team is finding it more and more difficult to break away from business to enjoy vacations and weekends away from work on an uninterrupted basis. It is the intent of this policy to provide the Executive Management team of the Board of Light and Power with an option to be reimbursed a portion of Paid Time Off accruals that are converted to their 457 account annually.

### Policy

1. Executive Management staff members who elect the annual conversion of their PTO accruals into their 457 account (per the Paid Time Off Cash Out Option provision of the employee handbook) will be reimbursed one-half of their PTO hours converted up to a maximum of 40 hours per calendar year.

## Grand Haven Board of Light & Power Policy

<b>Title</b>	Payment Card Security
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	02/28/2019
<b>Responsible Person</b>	General Manager

# **CITY OF GRAND HAVEN BOARD OF LIGHT & POWER**

## **Payment Card Security Policies For PCI DSS version 3.2**

Version 1.1 - 2019-02-28

### **CONFIDENTIAL INFORMATION**

This document is the property of CITY OF GRAND HAVEN BOAR; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of CITY OF GRAND HAVEN BOAR.

# Revision History

Changes	Approving Manager	Date
Initial Publication		2019-02-28



## INTRODUCTION AND SCOPE

### Introduction

This document explains CITY OF GRAND HAVEN BOAR's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. CITY OF GRAND HAVEN BOAR management is committed to these security policies to protect information utilized by CITY OF GRAND HAVEN BOAR in attaining its business goals. All employees are required to adhere to the policies described within this document.

### Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, CITY OF GRAND HAVEN BOAR's cardholder environment consists only of limited payment applications (typically point-of-sale systems) connected to the internet, but does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) C, version 3.2 revision 1.1, released January 2017. Should CITY OF GRAND HAVEN BOAR implement additional acceptance channels, add additional connected systems, begin storing cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of CITY OF GRAND HAVEN BOAR to determine the appropriate compliance criteria and implement additional policies and controls as needed.

## Requirement 1: Build and Maintain a Secure Network

### Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Access to the internet must be through a firewall, as must any direct connection to a vendor, processor, or service provider. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1)

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment. (PCI Requirement 1.3.3)
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized by management and controlled by the firewall. (PCI Requirement 1.3.4)
- Ensure the firewall allows only established connections into the network and denies any inbound connections not associated with a previously established session. (PCI Requirement 1.3.5)

Any mobile and/or employee-owned computers with direct connectivity the Internet (for example, laptops used by employees), which also have the ability to access the organization's cardholder data environment must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users. (PCI Requirement 1.4)

## **Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters**

### **Vendor Defaults**

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to: (PCI Requirement 2.1.1)

- Default encryption keys
- Passwords
- SNMP community strings
- Default passwords/passphrases on access points
- Other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks.

### **Configuration Standards for Systems**

Configuration standards for all system components must be developed and enforced. CITY OF GRAND HAVEN BOAR must insure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. (PCI Requirement 2.2)

Configuration standards must be updated as new vulnerability issues are identified, and they must be enforced on any new systems before they are added to the cardholder data environment. The standards must cover the following:

- Changing of all vendor-supplied defaults and elimination of unnecessary default accounts.
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (PCI Requirement 2.2.1)
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system. (PCI Requirement 2.2.2)
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure. (PCI Requirement 2.2.3)
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (PCI Requirement 2.2.5)

System administrators and any other personnel that configure system components must be knowledgeable about common security parameter settings for those system components. They must also be responsible to insure that security parameter settings set appropriately on all system components before they enter production. (PCI Requirement 2.2.4)

System administrators are responsible to insure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (PCI Requirement 2.5)

### **Non-Console Administrative Access**

Credentials for non-console administrative access must be encrypted. To be considered “strong cryptography,” industry-recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use: (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator’s password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.
- Must include administrator access to web-based management interfaces.
- Use vendor documentation and knowledge of personnel to verify that strong cryptography is in use for all non-console access and that for the technology in use it is implemented according to industry best practices and vendor recommendations.

## **Requirement 3: Protect Stored Cardholder Data**

## Prohibited Data

Processes must be in place to securely delete sensitive authentication data (defined below) post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Payment systems must not store of sensitive authentication data in any form after authorization (even if encrypted). Sensitive authentication data is defined as the following:

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)

## Displaying PAN

CITY OF GRAND HAVEN BOAR will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show at most only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. Policies and procedures for masking the display of PANs must mandate the following: (PCI Requirement 3.3)

- A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access.
- PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN.
- All other roles not specifically authorized to see the full PAN must only see masked PANs.

## Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

### Transmission of Cardholder Data

In order to safeguard sensitive cardholder data during transmission over open, public networks, CITY OF GRAND HAVEN BOAR will use strong cryptography and security protocols. These controls will be implemented as follows: (PCI Requirement 4.1)

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.

- The encryption strength is appropriate for the encryption methodology in use.

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. Weak encryption (for example, WEP, SSL) is not to be used as a security control for authentication or transmission. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI Requirement 4.2)

## **Requirement 5: use and Regularly Update Anti-Virus Software or Programs**

### **Anti-Virus Protection**

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all known types of malicious software. (PCI Requirement 5.1, 5.1.1)

For systems considered to be not commonly affected by malicious software, CITY OF GRAND HAVEN BOAR will perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. (PCI Requirement 5.1.2)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and be capable of as well as configured to generate audit logs. Anti-virus logs must also be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Steps must be taken to insure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. (PCI Requirement 5.3)

## **Requirement 6: Develop and Maintain Secure Systems and Applications**

### **Risk and Vulnerability**

CITY OF GRAND HAVEN BOAR will establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

Risk rankings are to be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating

vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. (PCI Requirement 6.1)

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. All applicable non-critical vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). (PCI Requirement 6.2)

Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. (PCI Requirement 6.4.6)

## **Requirement 7: Restrict Access to Cardholder Data by Business Need to Know**

### **Limit Access to Cardholder Data**

Access to CITY OF GRAND HAVEN BOAR's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)

Privileges must be assigned to individuals based on job classification and function (also called "role-based access control"). (PCI Requirement 7.1.3)

## **Requirement 8: Assign a Unique ID to Each Person with Computer Access**

### **User Accounts**

The following must be followed for all user accounts that have access to the system or systems that are part of the payment environment:

- Assign all users a unique ID before allowing them to access system components or cardholder data. (PCI Requirement 8.1.1)

- Limit repeated access attempts by locking out the user ID after not more than six attempts. (PCI Requirement 8.1.6)
- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (PCI Requirement 8.1.7)
- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. (PCI Requirement 8.1.8)

## **Vendor Accounts**

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. (PCI Requirement 8.1.5)

## **User Authentication**

In addition to assigning a unique ID for each user, ensure proper user-authentication management for non-consumer users (i.e.: employees and contractors) and administrators on all system components by employing at least one of the following methods to authenticate all users: (PCI Requirement 8.2)

Passwords/phrases must meet the following: (PCI Requirement 8.2.3)

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.

Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.

Change user passwords/passphrases at least every 90 days. (PCI Requirement 8.2.4)

Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. (PCI Requirement 8.2.5)

Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. (PCI Requirement 8.2.6)

## **Remote Access**

Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication. (PCI Requirement 8.3)

- Incorporate multi-factor authentication for all non-console access into the cardholder data environment for personnel with administrative access. (PCI Requirement 8.3.1)
- Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network. (PCI Requirement 8.3.2)

Document and communicate password/authentication policies and procedures to all users. (PCI Requirement 8.4)

Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: (PCI Requirement 8.5)

- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.
- Shared and generic user IDs are not used to administer any system components.

Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all appropriate personnel. (PCI Requirement 8.8)

## **Requirement 9: Restrict Physical Access to Cardholder Data**

### **Physically Secure All Areas and Media Containing Cardholder Data**

Appropriate facility entry controls must be used to limit and monitor physical access to systems in the cardholder data environment. (PCI Requirement 9.1)

Using video cameras, access control mechanisms, or both, individual physical access to sensitive areas shall be monitored. Collected data shall be reviewed and correlated with other entries. This data shall be stored for at least three months, unless otherwise restricted by law. (PCI Requirement 9.1.1)

All publicly accessible network jacks must have physical and/or logical controls to restrict access to the secure network by unauthorized personnel. (PCI Requirement 9.1.2)

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI Requirement 9.5)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.6)

- Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.6.1)
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.6.2)
- Management approval must be obtained prior to moving the media from the secured area. (PCI Requirement 9.6.3)



Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.7)

## **Destruction of Data**

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI Requirement 9.8)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI Requirement 9.8.1.a)

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI Requirement 9.8.1.b)

## **Protection of Payment Devices**

Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted. (PCI Requirement 9.9)

CITY OF GRAND HAVEN BOAR must maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: (PCI Requirement 9.9.1)

- Make and model of all devices.
- Location of each device (for example, the address of the site or facility where the device is located).
- Device serial number or other method of unique identification.

The payment devices must be periodically inspected. Check surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). (PCI Requirement 9.9.2)

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI Requirement 9.9.3)

- Employees must verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
- Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
- Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

## **Requirement 10: Regularly Monitor and Test Networks**

### **Audit Log Collection**

CITY OF GRAND HAVEN BOAR will implement technical controls that create audit trails in order to link all access to system components to an individual user. The automated audit trails created will capture sufficient detail to reconstruct the following events:

- All actions taken by any individual with root or administrative privileges. (PCI Requirement 10.2.2)
- All invalid logical access attempts (failed logins). (PCI Requirement 10.2.4)
- Any use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. (PCI Requirement 10.2.5)

CITY OF GRAND HAVEN BOAR's log generating and collecting solution will capture the following data elements for the above events:

- User identification. (PCI Requirement 10.3.1)
- Type of event. (PCI Requirement 10.3.2)
- Date and time. (PCI Requirement 10.3.3)
- Success or failure indication. (PCI Requirement 10.3.4)
- Origination of event. (PCI Requirement 10.3.5)
- Identity or name of affected data, system component, or resource. (PCI Requirement 10.3.6)

### **Audit Log Review**

CITY OF GRAND HAVEN BOAR's systems administrators will perform daily review of the audit logs. This review may be manual or automated but must monitor for and evaluate: (PCI Requirement 10.6.1)

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

The audit review must also check the logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. (PCI Requirement 10.6.2)

Subsequent to log review, systems administrators or other responsible personnel will follow up exceptions and anomalies identified during the review process. (PCI Requirement 10.6.3)

CITY OF GRAND HAVEN BOAR must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). (PCI Requirement 10.7)

## **Requirement 11: Regularly Test Security Systems and Processes**

### **Testing for Unauthorized Wireless Access Points**

At least quarterly, CITY OF GRAND HAVEN BOAR will perform testing to ensure there are no unauthorized wireless access points (802.11) present in the cardholder environment. (PCI Requirement 11.1)

The methodology must be adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components.
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.).
- Wireless devices attached to a network port or network device.

To facilitate the detection process, CITY OF GRAND HAVEN BOAR will maintain an inventory of authorized wireless access points including a documented business justification. (PCI Requirement 11.1.1)

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), the configuration must be capable of generating alerts to notify personnel. Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.10). (PCI Requirement 11.1.2)

### **Vulnerability Scanning**

At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), CITY OF GRAND HAVEN BOAR will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be performed at a minimum quarterly and repeated until passing results are obtained, or until all “high” vulnerabilities as defined in PCI Requirement 6.1 are resolved. Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.1)

Quarterly external vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.2)

For both internal and external vulnerability scans, CITY OF GRAND HAVEN BOAR shall perform rescans as needed to validate remediation of failures detected during previous scans, as well as after any significant change to the network. Scans must be performed and reviewed by qualified personnel. (PCI Requirement 11.2.3)

If segmentation is used to isolate the CDE from other networks, perform tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. These tests need to be done from multiple locations on the internal network, checking both for improper accessibility from the out-of-scope zones to the in-scope zone as well as the reverse. (PCI Requirement 11.3.4)

For all in-scope systems for which it is technically possible, CITY OF GRAND HAVEN BOAR must deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. The change detection software must be integrated with the logging solution described above, and it must be capable of raising alerts to responsible personnel. (PCI Requirement 11.5.1)

For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). (PCI Requirement 11.5)

## **Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors**

### **Security Policy**

CITY OF GRAND HAVEN BOAR shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI Requirement 12.1.1)

### **Critical Technologies**

CITY OF GRAND HAVEN BOAR shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI Requirement 12.3)

These policies must include the following:

- Explicit approval by authorized parties to use the technologies. (PCI Requirement 12.3.1)
- Authentication for use of the technology. (PCI Requirement 12.3.2)
- A list of all such devices and personnel with access. (PCI Requirement 12.3.3)
- Acceptable uses of the technologies. (PCI Requirement 12.3.5)
- Acceptable network locations for the technologies. (PCI Requirement 12.3.6)
- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. (PCI Requirement 12.3.8)
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. (PCI Requirement 12.3.9)

## **Security Responsibilities**

CITY OF GRAND HAVEN BOAR's policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

## **Incident Response Policy**

The IT Specialist shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI Requirement 12.5.3)

## **Incident Identification**

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within databases, logs, files or paper records.

## **Reporting an Incident**

The IT Specialist should be notified immediately of any suspected or real security incidents involving cardholder data:

Contact the IT Specialist to report any suspected or actual incidents. The Internal Audit's phone number should be well known to all employees and should page someone during non-business hours.

No one should communicate with anyone outside of their supervisor(s) or the IT Specialist about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the IT Specialist.

Document any information you know while waiting for the IT Specialist to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

### **Incident Response Policy (PCI Requirement 12.10.1)**

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.

#### **Visa**

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at [http://usa.visa.com/download/business/accepting\\_visa/ops\\_risk\\_management/cisp\\_what\\_to\\_do\\_if\\_compromised.pdf](http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf)

#### **MasterCard**

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at [http://www.mastercard.com/us/wce/PDF/12999\\_MERC-Entire\\_Manual.pdf](http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf). Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

#### **Discover Card**

Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

2. Alert all necessary parties. Be sure to notify:

- a. Merchant bank
  - b. Local FBI Office
  - c. U.S. Secret Service (if Visa payment data is compromised)
  - d. Local authorities (if appropriate)
3. Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: <http://www.ncsl.org/programs/lis/cip/priv/breach.htm>
  4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the IT Specialist will work with legal and management to identify appropriate forensic specialists.
  5. Eliminate the intruder's means of access and any related vulnerabilities.
  6. Research potential risks related to or damage caused by intrusion method used.

### **Root Cause Analysis and Lessons Learned**

Not more than one week following the incident, members of the IT Specialist and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

### **Security Awareness**

CITY OF GRAND HAVEN BOAR shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

### **Service Providers**

CITY OF GRAND HAVEN BOAR shall implement and maintain policies and procedures to manage service providers. (PCI Requirement 12.8)

This process must include the following:

- Maintain a list of service providers. (PCI Requirement 12.8.1)
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess. (PCI Requirement 12.8.2)
- Implement a process to perform proper due diligence prior to engaging a service provider. (PCI Requirement 12.8.3)
- Monitor service providers' PCI DSS compliance status. (PCI Requirement 12.8.4)

- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. (PCI Requirement 12.8.5)



# Grand Haven Board of Light & Power Policy

<b>Title</b>	Record Retention
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	None
<b>Responsible Person</b>	General Manager

## Introduction

Retention and disposal schedules define how long records need to be retained to satisfy administrative, fiscal, legal and historical requirements, and to specify if/when records can be destroyed.

## Policy

1. The Grand Haven Board of Light and Power adopts the “General Schedules for Local Government”, published by the State of Michigan’s Department of Technology, Management & Budget, as its minimum record retention policy.
2. Staff is authorized to identify schedules that are applicable to Board of Light and Power operations and establish procedures for compliance.

# Grand Haven Board of Light & Power Policy

<b>Title</b>	Retiree Recognition
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	02/24/2000
<b>Responsible Person</b>	General Manager

## Introduction

The Retiree Recognition Program is designed to formally acknowledge the service, achievements, and commitment of retiring employees. Through meaningful gestures of appreciation, we aim to express our gratitude and ensure each retiree feels valued and celebrated as they transition into retirement.

## Policy

1. The Board of Light & Power (BLP) will recognize retirees by presenting them with a “Selective Gift” catalog as follows:

a. <u>Years of Service</u>	<u>Catalog</u>	<u>BLP Cost</u>
6 through 9 years	5	\$100
10 through 14 years	6	\$150
15 through 19 years	7	\$250
20 through 24 years	8	\$350
25 years or more	9	\$500

2. The General Manager is authorized to adjust this program’s parameters including gift types and values to reflect reasonable and customary changes due to inflation, vendor offerings, or other market-driven factors, provided the program remains within budgetary constraints.

# Grand Haven Board of Light & Power Policy

<b>Title</b>	Social Security Number Privacy
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	04/27/2006
<b>Responsible Person</b>	General Manager

## Introduction

It is the policy of the Grand Haven Board of Light and Power (BLP) to comply with the Social Security Privacy Act, Act 454 of the Public Acts of 2004, MCL 445.81 et seq., to assure that the Social Security numbers gathered by Board of Light and Power (BLP) employees in the course and scope of their duties are maintained in privacy and protected from unlawful disclosure.

## Policy

1. Except as provided in subsection (2.) no BLP employee shall intentionally do any of the following with the Social Security number of an employee or other individual:
  - a. Publicly display all or more than four (4) sequential digits of the Social Security number.
  - b. Subject to subsection (3.) use all or more than four (4) sequential digits of the Social Security number of an individual.
  - c. Visibly print all or more than four (4) sequential digits of the Social Security number on any identification badge or card, membership card or permit or license.
  - d. Require an individual to use or transmit all or more than four (4) sequential digits of his or her Social Security number over the Internet or a computer system or network unless the connection is secure or the transmission is encrypted.
  - e. Require an individual to use or transmit all or more than four (4) sequential digits of his or her Social Security number to gain access to an Internet web site or a computer system or network unless the connection is secure, the transmission is encrypted, or a password or other unique personal identification number or other authentication device is also required to gain access to the Internet web site or computer system or network.
  - f. Include all or more than four (4) sequential digits of the Social Security number in or on any document or information mailed or otherwise sent to an individual if it is visible on or, without manipulation, from outside of the envelope or packaging.
  - g. Subject to subsection (3.), include all or more than four (4) sequential digits of the Social Security number in any document or information mailed to a person, unless any of the following apply:
    - i. State or federal law, rule, regulation, or court order or rule authorizes, permits, or requires that a Social Security number appear in the document.
    - ii. The document is sent as part of an application or enrollment process initiated by the individual.

- iii. The document is sent to establish, confirm the status of, service, amend, or terminate an account, contract, policy or employee or health insurance benefit or to confirm the accuracy of a Social Security number of an individual who has an account, contract, policy or employee or health insurance benefit.
  - iv. The document or information is a public record and is mailed or provided by the BLP in compliance with the Michigan Freedom of Information Act, 1976 PA 442, MCL 15.231 to 15.246.
  - v. The document or information is mailed in a manner or for a purpose consistent with subtitle A of Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 to 6809; with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191; or with Section 537 or 539 of the insurance code of 1956, 1956 PA 218, MCL 500.537 and 500.539; or their successors or replacements.
- 2. Subsection (I.) does not apply to any of the following:
  - a. A use of all or more than four (4) sequential digits of a Social Security number that is authorized or required by state or federal statute, rule, or regulation, by court order or rule, or pursuant to legal discovery or process.
  - b. Providing all or more than four (4) sequential digits of a Social Security number to a Title IV-D agency, law enforcement agency, court or prosecutor as part of a criminal investigation or prosecution.
- 3. It is not a violation of subsection (1.) (2.) or (7.) of this policy to use all or more than four (4) sequential digits of a Social Security number if the use is any of the following:
  - a. An administrative use of all or more than four (4) sequential digits of the Social Security number in the ordinary course of business, by a BLP employee or a vendor or contractor of the BLP to do any of the following:
    - i. Verify an individual's identity, identify an individual, or do another similar administrative purpose related to an account, transaction, product, services or employment.
    - ii. Investigate an individual's claim, credit, criminal or driving history.
    - iii. Detect, prevent or deter identity theft or another crime.
    - iv. Lawfully pursue or enforce a person's legal rights, including, but not limited to, an audit, collection, investigation or transfer of a tax, employee benefit, debt, claim, receivable or account or an interest in a receivable or account.
    - v. Lawfully investigate, collect or enforce a child or spousal support obligation or tax liability.
    - vi. Provide or administer employee or health insurance or membership benefits, claims, or retirement programs or to administer the ownership of shares of stock or other investments.
  - b. A use of all or more than four (4) sequential digits of a Social Security number as primary account number that meets both the following:
    - i. The use began before the effective date of this Act.
    - ii. The use is ongoing, continuous, and in the course of business. If the use is stopped for any reason, this subdivision no longer applies.
- 4. All or more than four (4) sequential digits of a Social Security number contained in a public record are exempt from disclosure under the Michigan Freedom of Information Act, 1976 PA 442, MCL 15.231 to 15.246, pursuant to Section 13(1)(d) of the Michigan Freedom of Information Act, MCL 15.243(1)(d) and the BLP will make a reasonable effort to redact this information when supplying material in response to Freedom of Information Act requests.

5. Only those BLP employees who must have access to Social Security numbers to perform their job functions shall have access to Social Security numbers, and access to Social Security numbers by any other employee of BLP is prohibited. BLP employees who are provided access to, or otherwise observe, Social Security numbers in error shall immediately notify their supervisor of this fact.
6. Documents which contain Social Security numbers that the BLP chooses to dispose of shall be destroyed by shredding.
7. A BLP employee who violates this Policy shall be subject to discipline up to and including termination.

# Grand Haven Board of Light & Power Policy

<b>Title</b>	Technology Use
<b>Adopted by the Board</b>	
<b>Previous Adoption Dates</b>	07/25/2016
<b>Responsible Person</b>	Distribution and Engineering Manager

## Introduction

Governing Boards must ensure adequate personnel policies are in place to comply with employment laws and reduce organizational risk while avoiding excessive Board involvement in day-to-day operations. Recognizing the ever-changing nature of technology, the Board authorizes the General Manager to update this policy from time to time as deemed necessary.

GHBLP IT systems provide critical resources that enable employees to perform their duties with efficiency and effectiveness. To maintain the integrity and proper functioning of these systems it is imperative that users understand and adhere to the foundational principles outlined in this policy. This policy encompasses the appropriate use of the following systems and resources:

- Use of IT Systems
- Computer and Network Data Security
- Internet, Email, Social Media and Instant Messaging (IM) Use
- Artificial Intelligence (AI)
- Bring Your Own Device (BYOD) and Guest Wi-Fi Use
- Acceptable Use and Unacceptable Use
- Devices and Support
- USB (Universal Serial Bus) Devices
- Software and App Installation
- Passwords and Security
- Enforcement Steps

The purpose of this Technology Use Policy is to protect GHBLP—along with our employees, customers, and partners—from risks associated with the misuse of our technology systems and data. Misuse can be either intentional or accidental, and the consequences can be significant. Potential impacts of such misuse include, but are not limited to, malware infections (e.g., computer viruses), legal or financial repercussions from data breaches, and productivity losses due to system downtime. Every GHBLP employee shares responsibility for safeguarding our IT systems and the data they contain. This policy outlines acceptable practices for handling data—whether transmitted, received, or stored on electronic devices and portable storage media—regardless of whether those devices are GHBLP-owned or personally owned. Adherence to this policy is mandatory for all employees and board members. If there is any uncertainty about how the policy applies to specific roles or situations, employees are encouraged to consult their manager or IT for

further clarification. In cases where provisions of this policy intersect with local laws (e.g., employee privacy laws), legal compliance takes precedence. Staff responsible for monitoring and enforcing this policy must ensure their actions are always aligned with applicable local regulations.

## **Policy**

### **1. Use of IT Systems**

- a. All data stored on GHBLP's IT systems is the property of GHBLP. Users should be aware that GHBLP cannot guarantee the confidentiality of any information stored on these systems, except where required by law. GHBLP data must be securely stored in designated locations (e.g., department-specific SharePoint drives) to prevent unauthorized access while ensuring legitimate access for authorized personnel.
- b. GHBLP reserves the right to monitor IT system usage and data at any time, except where restricted by privacy laws. This may include reviewing email content, data files, and user access history. Regular audits of networks and systems will be conducted to ensure compliance with this policy.

### **2. Computer and Network Data Security**

- a. Users must take all necessary precautions to prevent unauthorized access to GHBLP's computer systems and data. No data stored on a computer or network device should be assumed secure from access by other employees.
- b. Users must not send, upload, remove, or transfer GHBLP data—whether via portable media or cloud services—to any non-GHBLP system unless explicitly authorized as part of their regular duties. When sending GHBLP data externally, users must use email encryption or the External Sharing SharePoint drive, which requires multi-factor authentication (MFA) for external access.
- c. Users must remain vigilant against security threats (e.g. phishing, malware, ransomware) and are required to report any known or suspected issues to the IT Specialist immediately to help mitigate the risks and spread of malicious activities to other systems and data.

### **3. Internet, Email, Social Media and Instant Messaging (IM) Use**

- a. The internet, email, social media and instant messaging (IM) are valuable tools that support employees in performing their job duties. While their use is permitted to support business objectives, access is a privilege that requires adherence to company policies.
- b. All electronic communications conducted through GHBLP's IT systems and equipment are the property of GHBLP and should not be considered private. GHBLP reserves the right to monitor, examine, and regulate email, files, directories, internet usage, and IM activity. Employees should not expect privacy regarding data stored on or transmitted through GHBLP systems.
- c. Additionally, GHBLP may access an employee's computer, email, or network data as necessary to maintain business continuity when the employee is unavailable.
- d. Any information provided on a personal social networking site with regard to the GHBLP is expected to conform to established policies regarding access to and release of GHBLP information and communications procedures.
- e. Records can exist in a wide variety of formats for retention periods. Email is not to be considered the primary storage medium for retention purposes, but record retention schedules must be followed while using the email system.

### **4. Artificial Intelligence (AI)**

- a. Due to the inherent risk to GHBLP's proprietary and sensitive data, and concerns over the accuracy of content generated by AI tools, the following rules apply to the use of generative AI tools while performing work for GHBLP:
  - i. GHBLP accounts/log in credentials may not be linked to an account with any generative AI platform.
  - ii. No sensitive or confidential GHBLP data, including customer data, may be submitted (copied, typed, transferred, etc.) into these platforms.
  - iii. All AI-generated content must be reviewed for accuracy before relying on it for work purposes. If a reliable source cannot be found to verify factual information generated by the tool, that generated information may not be used for work purposes.

5. Bring Your Own Device (BYOD) and Guest Wi-Fi Use

- a. Employees may use personal smartphones and tablets on the GHBLP's guest Wi-Fi network with manager or supervisor approval. To connect, employees must agree to the terms outlined in this policy.
- b. The guest Wi-Fi network is separate and segmented from the internal corporate network and provides internet access only. It does not allow access to company resources, internal servers, or printers.
- c. For security, performance, and compliance, guest Wi-Fi duration is limited to two weeks, after which users must re-enter the guest password to reauthenticate. Bandwidth throttling or device blacklisting may be applied to prevent excessive usage, and content filtering will automatically block inappropriate or malicious websites. GHBLP reserves the right to monitor guest network activity and may retain activity logs (e.g., IP addresses, timestamps) for a fixed period for security purposes.
- d. Peer-to-peer (P2P) file sharing, torrenting, illegal or malicious activities, and using the network for personal gain or commercial purposes are strictly prohibited.

6. Acceptable Use

- a. This document outlines the acceptable use of technology at GHBLP to protect company data, ensure productivity, and prevent misuse of technological resources.
- b. Business Use
  - i. Employees are expected to use company technology resources for legitimate business purposes, including:
    - 1. Performing job-related duties using approved business applications, company systems, and files.
    - 2. Using approved communication tools (e.g., Outlook, ConnectUC, IP Phones) for business purposes.
    - 3. Engaging in work-related activities including training, research, or professional development.
- c. Limited Personal Use
  - i. Reasonable personal use is permitted, provided it does the following:
    - 1. Does not interfere with job responsibilities.
    - 2. Does not consume excessive bandwidth or system resources.
    - 3. Complies with firewall policies regarding content and behavior.
  - ii. Examples of Permitted Personal Use:
    - 1. Checking personal email or browsing news during breaks.
    - 2. Brief, non-disruptive personal communication.



## 7. Unacceptable Use

- a. GHBLP has a zero tolerance policy for texting or emailing while driving. Only hands free talking while driving is permitted (As enforced by Michigan distracted driving laws.)
- b. Employees are expressly prohibited from conducting any activity or behavior that violates company policies, legal regulations, or ethical standards while using the organization's technological resources, including computers, networks, email, and software. This includes, but is not limited to, the following:
  - i. Engaging in illegal activities – Using company systems to access, distribute, or store illegal content, violate copyright laws, engage in fraud, or conduct any activity that violates local, state, or federal laws.
  - ii. Participating in activities detrimental to the GHBLP's success – Any action that disrupts operations, reduces productivity, or undermines company interests, such as excessive personal use of company resources or unauthorized disclosures of sensitive information.
  - iii. Using company resources for personal gain or in ways that negatively impact business operations – Conducting outside business activities, excessive personal use of IT resources, or using company systems for non-work-related financial gain.
  - iv. Engaging in activities that could harm the GHBLP's reputation or are inappropriate for company association – Accessing, transmitting, or distributing offensive, discriminatory, or defamatory content; engaging in harassment; or participating in online discussions that misrepresent or harm the GHBLP's public image.
  - v. Attempting to bypass or compromise the GHBLP's IT security systems and protocols – Unauthorized access to restricted data, hacking, disabling security measures, using unapproved software, or sharing credentials that compromise the integrity of company systems.

## 8. Devices and Support

- a. Only GHBLP owned and provided computers, smartphones, and tablets are permitted to connect to the GHBLP corporate network.
- b. Personal electronic devices such as smartphones and tablets may only connect to the GHBLP-Guest wireless network. This is only after receiving proper approval from the employee's manager or supervisor and the IT Administrator and must follow the guidelines outlined in the Bring Your Own Device (BYOD) section.
- c. If a computer or mobile device is lost or stolen, it is the employee's responsibility to report the incident to the IT Specialist immediately. If they are unavailable, the Distribution & Engineering Manager must be contacted. Prompt reporting allows the IT Specialist to take swift action, such as disabling user/computer object to prevent unauthorized access to VPN or email systems.
- d. To prevent personal data loss during such an event, employees are strongly encouraged to regularly back up personal content (e.g., contacts, photos) to a personal computer or cloud storage service in case the device is lost, stolen, or needs to be reset.
- e. All devices must be presented to the IT Specialist for proper provisioning before being granted access to the GHBLP network. This includes the installation and configuration of standard applications such as browsers, standard or specialized software, and security software.

## 9. USB (Universal Serial Bus) Devices

- a. To maintain the security and integrity of GHBLP systems and data, the use of USB storage devices (such as flash drives, external hard drives, or any other portable media) is strictly prohibited unless explicitly approved by management. This policy is in place to reduce the risk

of data breaches, malware infections, and unauthorized data transfers. USB Ports on network computers are monitored and block mass storage attempts.

## 10. Software and App Installation

- a. The installation of software on GHBLP-owned devices is managed by the IT Specialist. Employees must notify IT if they require specific software for work purposes. IT is responsible for software evaluation, license tracking, and installation to ensure proper functionality and compliance.
- b. All GHBLP-owned devices will be equipped with the applications necessary for employees to perform their job duties. Likewise, any software or applications installed on employee-owned devices that access GHBLP data or email must run an operating system that is actively supported by the vendor. Devices with unsupported or end-of-life operating systems are not permitted, as they no longer receive critical security patches and pose a significant risk to network integrity.
- c. To maintain security, all devices with access to GHBLP systems/data/email must be configured to automatically check for and install operating system updates. Employees are expected to manually approve these updates as needed to apps or system software as they become available. Regular updates for platforms such as Android, iOS, Windows, and macOS often include important fixes to vulnerabilities, zero-days, and critical security updates. Delays in applying these updates can create vulnerabilities that may lead to serious security risks.
- d. GHBLP employees may only use licensed software—acquired through or approved by GHBLP—for business purposes on GHBLP-owned devices. All questions regarding software licensing must be directed to the IT Specialist.
- e. The use of unlicensed or illegally obtained software as outlined in unacceptable use—except public domain tools or software developed internally by GHBLP staff—is strictly prohibited. GHBLP is not responsible for any software licensing violations incurred through the use of unauthorized software. See Enforcement section below for GHBLP response steps.
- f. If you are unsure whether your device is properly configured, please contact the IT Specialist for review.

## 11. Passwords and Security

- a. Strong passwords are critical to protecting GHBLP systems and data. All employees, contractors, and vendors with access to GHBLP systems are responsible for creating and managing secure passwords.
- b. General Password Requirements
  - i. Network Passwords must be changed at least every 6 months (180 days).
  - ii. All devices accessing GHBLP data (email, documents, etc.) must require a password, passcode, or PIN.
  - iii. Devices must be configured to auto-lock after periods of inactivity as a basic security measure. (Windows devices are set to 30 minutes.) Users are required manually lock devices when not in use.
  - iv. Two-Factor Authentication (2FA) is required where ever possible.
- c. Password Standards
  - i. GHBLP network passwords must:
  - ii. Be at least 12 characters long.
  - iii. Include at least 3 of the following:
  - iv. Uppercase letters
  - v. Lowercase letters

- vi. Numbers
- vii. Special characters (e.g., @\$%^&\*)
- d. Avoid using:
  - i. Short passwords even when not enforced by vendor software
  - ii. Dictionary words or common terms
  - iii. Personal info (names, birthdays, addresses)
  - iv. Repeating or sequential patterns (e.g., 123321, qwerty)
  - v. Variations of "GHBLP" or "Grand Haven"
  - vi. Any of the above spelled backward or with added digits
- e. Longer passwords are always harder to crack. Consider using passphrase methodology for passwords.
- f. A Passphrase is a full sentence or phrase. These should still include mixed characters, make it long, and avoid predicable phrases, rather use a combination of random words, but something you can still remember.
- g. Password Best Practices
  - i. Use different passwords for all accounts.
  - ii. Never share your password—even with coworkers.
  - iii. Do not write down or store passwords unencrypted physically or digitally on the network.
  - iv. Avoid using the "Remember Password" feature in browsers and apps.
  - v. Never reveal passwords through email, chat, or phone. Delete emails that contain this information.
  - vi. If someone requests your password, refer them to IT. IT will never ask for your network password.
- h. If you suspect your account or password has been compromised, contact IT immediately.

## 12. Enforcement Steps

- a. To ensure compliance with the policy on unacceptable use of technology, GHBLP will take the following enforcement steps as needed:
  - i. Monitoring and Detection
    - 1. GHBLP reserves the right to monitor and log all activities on its IT systems, networks, and devices to identify potential violations. Monitoring may include reviewing internet usage, email correspondence, files, and other data stored on company systems.
  - ii. Investigation
    - 1. If a violation is suspected or observed, an investigation will be conducted by GHBLP. Employees may be asked to provide additional information or cooperate with the investigation.
  - iii. Verbal or Written Warning
    - 1. For first-time or minor offenses, employees may receive a verbal or written warning, outlining the nature of the violation and the consequences of further infractions.
  - iv. Suspension of Access
    - 1. In cases of serious violations or repeat offenses, disciplinary action may temporarily suspend access to the GHBLP's IT systems and networks. Depending on the severity of the violation, further disciplinary action may be taken up to and including termination of employment.
  - v. Reporting to Authorities

1. If the violation involves illegal activities, such as fraud, data theft, or hacking, GHBLP reserves the right to report the incident to law enforcement authorities or regulatory bodies as required by law, and pursue legal action
- vi. Review and Adjustment of Policies
  1. GHBLP will regularly review the effectiveness of the enforcement process and may adjust policies or procedures as necessary to address emerging risks or improve compliance efforts.