**JOPLIN CITY COUNCIL**
**INFORMAL MEETING**
**MONDAY, APRIL 15, 2024**
**5TH FLOOR COUNCIL CHAMBERS**
**602 S. MAIN ST.**
**5:30 PM**

---

This meeting can be livestreamed at http://www.joplinmo.org/182/Video-Multimedia

## AGENDA

1. Sales and Use Tax Update
2. RAVENII Update

Notice posted at 12:00 p.m. on this 11th day of April 2024. (RSMo 610.020)

The City of Joplin is committed to comply with the Americans with Disabilities Act. The Joplin City Council Chambers is wheelchair accessible. Request for reasonable special accommodations must be made 48 hours prior to the meeting. Please email the City Clerk's office at hnagy@joplinmo.org or call (417) 624-0820 ext. 1220 for assistance.

---

***Ad Omnia Parata***

# CITY OF JOPLIN, MISSOURI
## GENERAL MARIJUANA ADDTL SALES TAX - 100%
## ACCOUNT # 001-0000-400-0327
## HISTORICAL TAX RECEIPTS BY MONTH

| | FY 2024 | FY 2024 Y-T-D | % Change from FY 2023 | % Change from FY 2023 | Monthly Budget Remaining |
|---|---|---|---|---|---|
| November | - | - | 0.00% | 0.00% | 0.00% |
| December | 45,818.50 | 45,818.50 | 0.00% | 0.00% | 84.73% |
| January | 49,375.38 | 95,193.88 | 0.00% | 0.00% | 68.27% |
| February | 49,035.26 | 144,229.14 | 0.00% | 0.00% | 51.92% |
| March | 90,772.50 | 235,001.64 | 0.00% | 0.00% | 21.67% |
| April | 62,769.86 | 297,771.50 | 0.00% | 0.00% | 0.74% |
| May | - | - | 0.00% | 0.00% | 0.00% |
| June | - | - | 0.00% | 0.00% | 0.00% |
| July | - | - | 0.00% | 0.00% | 0.00% |
| August | - | - | 0.00% | 0.00% | 0.00% |
| September | - | - | 0.00% | 0.00% | 0.00% |
| October | - | - | 0.00% | 0.00% | 0.00% |
| YTD Totals | 297,771.50 | 297,771.50 | 0.00% | 0.00% | 0.74% |

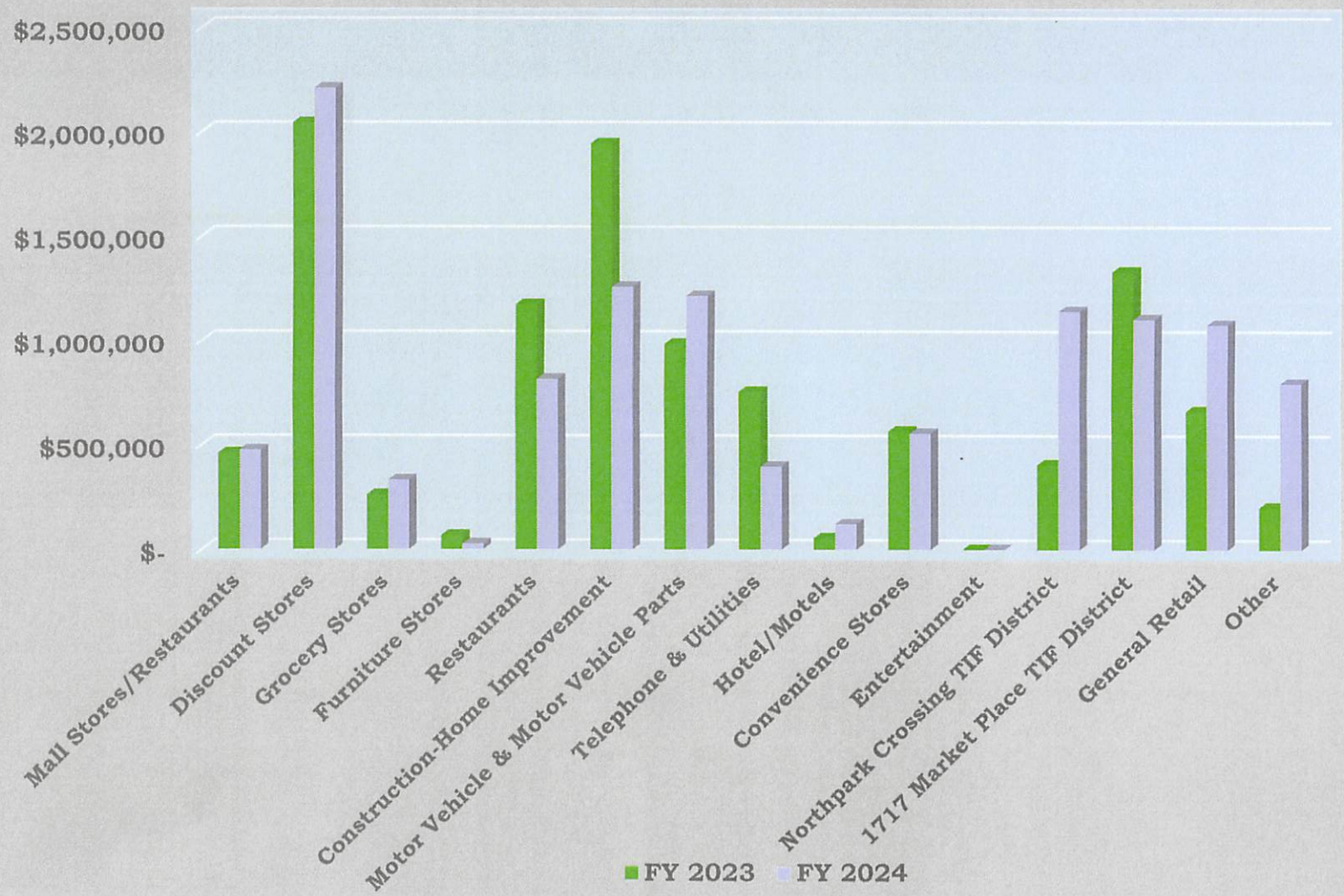
| | |
|---|---|
| Budgeted for FY 2024 | $ 300,000 |
| Y-T-D % Increase (Decrease) from FY 2023 | 0.00% |
| Actual % of FY 2024 Budget Remaining | 0.74% |
| % of Time Elapsed | 50.00% |

NOTE: Taxes are collected by the Department of Revenue approximately 30 days following the month in which taxable sales occur. Collections are remitted to the City by the 10th of each month for the prior months reported sales. Effective January 1, 2000, the State of Missouri Department of Revenue increased the threshold for monthly filing requirement from $250 to $500 for state tax collected.

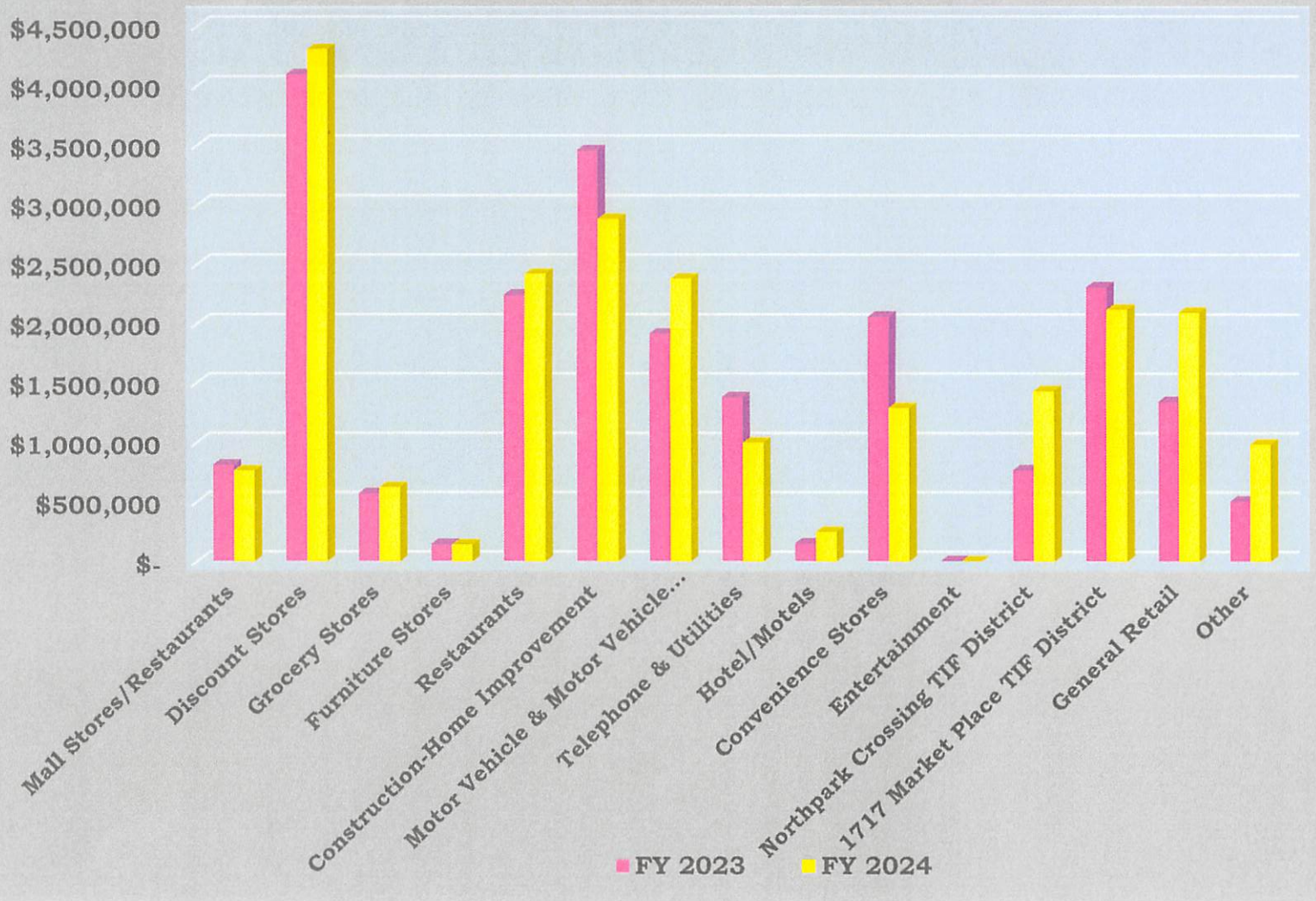
Actual budgeted increase is calculated by using the prior year actual collections compared to the budgeted amount.

This information is reported on a cash basis, while the accounting records are reported on an accrual basis.

# 2nd QUARTER (FEB-APRIL) SALES TAX COMPARISON BY CATEGORY (TOP 100 BUSINESSES)



# YEAR-TO-DATE SALES TAX COMPARISON BY CATEGORY (TOP 100 BUSINESSES)



# CITY OF JOPLIN, MISSOURI
## GENERAL SALES TAX --1%
## ACCOUNT # 001-0000-400-0301 (Tax Type Code 200)
## HISTORICAL TAX RECEIPTS BY MONTH

| | FY 2018 | FY 2019 | FY 2020 | FY 2021 | FY 2022 | FY 2023 | FY 2023 Y-T-D | FY 2024 | FY 2024 Y-T-D | Monthly % Change from FY 2023 | Y-T-D % Change from FY 2023 | Actual % of FY 2024 Budget Remaining |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| November | 864,840.99 | 1,018,673.84 | 1,090,430.38 | 1,075,827.30 | 1,171,792.22 | 1,321,687.86 | 1,321,687.86 | 1,301,114.54 | 1,301,114.54 | -1.56% | -1.56% | 92.86% |
| December | 1,724,313.47 | 1,232,874.05 | 1,355,281.81 | 1,403,354.16 | 1,486,673.02 | 1,497,611.46 | 2,819,299.32 | 1,540,275.51 | 2,841,390.05 | 2.85% | 0.78% | 84.42% |
| January | 1,012,860.10 | 1,450,849.53 | 1,353,568.92 | 1,358,290.69 | 1,431,020.07 | 1,516,095.13 | 4,335,394.45 | 1,599,960.33 | 4,441,350.38 | 5.53% | 2.44% | 75.64% |
| February | 1,342,971.47 | 1,271,096.61 | 1,335,166.72 | 1,360,530.09 | 1,549,497.19 | 1,554,171.79 | 5,889,566.24 | 1,614,588.32 | 6,055,938.70 | 3.89% | 2.82% | 66.79% |
| March | 1,345,240.66 | 1,361,552.45 | 1,322,254.82 | 1,433,507.48 | 1,286,337.08 | 1,370,941.79 | 7,260,508.03 | 1,304,966.35 | 7,360,905.05 | -4.81% | 1.38% | 59.63% |
| April | 1,103,641.48 | 1,193,015.26 | 1,071,421.25 | 1,314,220.00 | 1,517,799.15 | 1,495,565.91 | 8,756,073.94 | 1,496,303.00 | 8,857,208.05 | 0.05% | 1.16% | 51.43% |
| May | 1,073,466.90 | 1,122,187.32 | 1,092,586.90 | 1,291,986.62 | 1,189,442.30 | 1,212,145.50 | 9,968,219.44 | - | - | 0.00% | 0.00% | 0.00% |
| June | 1,219,876.57 | 1,264,770.32 | 1,237,244.91 | 1,596,922.41 | 1,449,457.40 | 1,591,492.88 | 11,559,712.32 | - | - | 0.00% | 0.00% | 0.00% |
| July | 1,470,035.68 | 1,279,316.91 | 1,292,888.47 | 1,640,598.95 | 1,476,731.63 | 1,439,436.05 | 12,999,148.37 | - | - | 0.00% | 0.00% | 0.00% |
| August | 1,070,687.96 | 1,074,123.80 | 1,249,324.51 | 1,293,211.15 | 1,660,582.30 | 1,486,908.52 | 14,486,056.89 | - | - | 0.00% | 0.00% | 0.00% |
| September | 1,302,353.26 | 1,433,627.20 | 1,442,892.53 | 1,930,630.77 | 1,558,365.34 | 1,558,525.00 | 16,044,581.89 | - | - | 0.00% | 0.00% | 0.00% |
| October | 1,066,250.29 | 1,254,497.04 | 1,322,546.86 | 1,360,047.71 | 1,587,849.77 | 1,343,428.39 | 17,388,010.28 | - | - | 0.00% | 0.00% | 0.00% |
| YTD Totals | 14,596,538.83 | 14,956,584.33 | 15,165,608.08 | 17,059,127.33 | 17,365,547.47 | 17,388,010.28 | 17,388,010.28 | 8,857,208.05 | 8,857,208.05 | 0.05% | 1.16% | 51.43% |
| **Annual % Change** | | **2.47%** | **1.40%** | **12.49%** | **1.80%** | **0.13%** | | | | | | |

| | |
|---|---|
| Budgeted for FY 2024 | $ 18,234,540 |
| Y-T-D % Increase (Decrease) from FY 2023 | 1.16% |
| Actual % of FY 2024 Budget Remaining | 51.43% |
| % of Time Elapsed | 50.00% |

NOTE: Taxes are collected by the Department of Revenue approximately 30 days following the month in which taxable sales occur. Collections are remitted to the City by the 10th of each month for the prior months reported sales. Effective January 1, 2000, the State of Missouri Department of Revenue increased the threshold for monthly filing requirement from $250 to $500 for state tax collected.

Sales tax figures include the TIF sales tax collections. 50% of the TIF sales tax collections have to be remitted by the City to the TIF developer after being received from the State.

Actual budgeted increase is calculated by using the prior year actual collections compared to the budgeted amount.

This information is reported on a cash basis, while the accounting records are reported on an accrual basis.

CITY OF JOPLIN, MISSOURI

**GENERAL SALES TAX --1%**

ACCOUNT # 001-0000-400-0301 (Tax Type Code 200)

HISTORICAL TAX RECEIPTS BY MONTH

| | FY 2019 | FY 2019 Y-T-D | FY 2020 | FY 2020 Y-T-D | FY 2021 | FY 2021 Y-T-D | FY 2022 | FY 2022 Y-T-D | FY 2023 | FY 2023 Y-T-D | FY 2024 | FY 2024 Y-T-D | Monthly % Change from FY 2023 | Y-T-D % Change from FY 2023 | Actual % of FY 2024 Budget Remaining |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| November | 1,018,673.84 | 1,018,673.84 | 1,090,430.38 | 1,090,430.38 | 1,075,827.30 | 1,075,827.30 | 1,171,792.22 | 1,171,792.22 | 1,321,687.86 | 1,321,687.86 | 1,301,114.54 | 1,301,114.54 | -1.56% | -1.56% | 92.86% |
| December | 1,232,874.05 | 2,251,547.89 | 1,355,281.81 | 2,445,712.19 | 1,403,354.16 | 2,479,181.46 | 1,486,673.02 | 2,658,465.24 | 1,497,611.46 | 2,819,299.32 | 1,540,275.51 | 2,841,390.05 | 2.85% | 0.78% | 84.42% |
| January | 1,450,849.53 | 3,702,397.42 | 1,353,568.92 | 3,799,281.11 | 1,358,290.69 | 3,837,472.15 | 1,431,020.07 | 4,089,485.31 | 1,516,095.13 | 4,335,394.45 | 1,599,960.33 | 4,441,350.38 | 5.53% | 2.44% | 75.64% |
| February | 1,271,096.61 | 4,973,494.03 | 1,335,166.72 | 5,134,447.83 | 1,360,530.09 | 5,198,002.24 | 1,549,497.19 | 5,638,982.50 | 1,554,171.79 | 5,889,566.24 | 1,614,588.32 | 6,055,938.70 | 3.89% | 2.82% | 66.79% |
| March | 1,361,552.45 | 6,335,046.48 | 1,322,254.82 | 6,456,702.65 | 1,433,507.48 | 6,631,509.72 | 1,286,337.08 | 6,925,319.58 | 1,370,923.57 | 7,260,489.81 | 1,304,966.35 | 7,360,905.05 | -4.81% | 1.38% | 59.63% |
| April | 1,193,015.26 | 7,528,061.74 | 1,071,421.25 | 7,528,123.90 | 1,314,220.00 | 7,945,729.72 | 1,517,799.15 | 8,443,118.73 | 1,495,565.10 | 8,756,054.91 | 1,496,303.00 | 8,857,208.05 | 0.05% | 1.16% | 51.43% |
| May | 1,122,187.32 | 8,650,249.06 | 1,092,586.90 | 8,620,710.80 | 1,291,986.62 | 9,237,716.34 | 1,189,442.30 | 9,632,561.03 | 1,212,145.50 | 9,968,200.41 | - | - | 0.00% | 0.00% | 0.00% |
| June | 1,264,770.32 | 9,915,019.38 | 1,237,244.91 | 9,857,955.71 | 1,596,922.41 | 10,834,638.75 | 1,449,457.40 | 11,082,018.43 | 1,591,492.88 | 11,559,693.29 | - | - | 0.00% | 0.00% | 0.00% |
| July | 1,279,316.91 | 11,194,336.29 | 1,292,888.47 | 11,150,844.18 | 1,640,598.95 | 12,475,237.70 | 1,476,731.63 | 12,558,750.06 | 1,439,436.05 | 12,999,129.34 | - | - | 0.00% | 0.00% | 0.00% |
| August | 1,074,123.80 | 12,268,460.09 | 1,249,324.51 | 12,400,168.69 | 1,293,211.15 | 13,768,448.85 | 1,660,582.30 | 14,219,332.36 | 1,486,908.52 | 14,486,037.86 | - | - | 0.00% | 0.00% | 0.00% |
| September | 1,433,627.20 | 13,702,087.29 | 1,442,892.53 | 13,843,061.22 | 1,930,630.77 | 15,699,079.62 | 1,558,365.34 | 15,777,697.70 | 1,558,525.00 | 16,044,562.86 | - | - | 0.00% | 0.00% | 0.00% |
| October | 1,254,497.04 | 14,956,584.33 | 1,322,546.86 | 15,165,608.08 | 1,360,047.71 | 17,059,127.33 | 1,587,849.77 | 17,365,547.47 | 1,343,428.39 | 17,387,991.25 | - | - | 0.00% | 0.00% | 0.00% |
| YTD Totals | 14,956,584.33 | 14,956,584.33 | 15,165,608.08 | 15,165,608.08 | 17,059,127.33 | 17,059,127.33 | 17,365,547.47 | 17,365,547.47 | 17,387,991.25 | 17,387,991.25 | 8,857,208.05 | 8,857,208.05 | 0.05% | 1.16% | 51.43% |
| **Annual % Change** | | | **1.40%** | | **12.49%** | | **1.80%** | | **0.13%** | | | | | | |

| | |
|---|---|
| Budgeted for FY 2024 | $ 18,234,540 |
| Y-T-D % Increase (Decrease) from FY 2023 | 1.16% |
| Actual % of FY 2024 Budget Remaining | 51.43% |
| % of Time Elapsed | 50.00% |

NOTE: Taxes are collected by the Department of Revenue approximately 30 days following the month in which taxable sales occur. Collections are remitted to the City by the 10th of each month for the prior months reported sales. Effective January 1, 2000, the State of Missouri Department of Revenue increased the threshold for monthly filing requirement from $250 to $500 for state tax collected.

Sales tax figures include the TIF sales tax collections. 50% of the TIF sales tax collections have to be remitted by the City to the TIF developer after being received from the State.

Actual budgeted increase is calculated by using the prior year actual collections compared to the budgeted amount.

This information is reported on a cash basis, while the accounting records are reported on an accrual basis.

# CITY OF JOPLIN, MISSOURI
## GENERAL SALES TAX - 1% (LESS TIF AMOUNT)
## ACCOUNT # 001-0000-400-0301
## HISTORICAL TAX RECEIPTS BY MONTH

| | FY 2017 | FY 2018 | FY 2019 | FY 2020 | FY 2021 | FY 2022 | FY 2023 | FY 2023 Y-T-D | FY2024 | FY 2024 Y-T-D | Monthly % Change from FY 2023 | Y-T-D % Change from FY 2023 | Actual % of FY 2024 Budget Remaining |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| November | 750,477.69 | 788,342.03 | 949,582.56 | 1,026,948.77 | 1,034,917.31 | 1,144,648.14 | 1,280,266.05 | 1,280,266.05 | 1,275,462.61 | 1,275,462.61 | -0.38% | -0.38% | 92.69% |
| December | 1,067,419.97 | 1,679,548.83 | 1,164,040.04 | 1,286,993.43 | 1,368,071.96 | 1,426,140.57 | 1,471,360.89 | 2,751,626.94 | 1,515,919.93 | 2,791,382.54 | 3.03% | 1.44% | 84.00% |
| January | 1,243,560.16 | 921,510.72 | 1,385,088.66 | 1,271,965.44 | 1,334,543.74 | 1,391,414.25 | 1,502,569.22 | 4,254,196.16 | 1,587,332.55 | 4,378,715.09 | 5.64% | 2.93% | 74.90% |
| February | 1,086,635.80 | 1,253,970.89 | 1,198,490.74 | 1,222,056.35 | 1,300,812.59 | 1,527,514.91 | 1,521,105.24 | 5,775,301.40 | 1,578,917.88 | 5,957,632.97 | 3.80% | 3.16% | 65.84% |
| March | 1,097,596.53 | 1,280,011.95 | 1,281,488.56 | 1,292,407.82 | 1,390,194.01 | 1,221,407.07 | 1,313,425.82 | 7,088,727.22 | 1,282,473.64 | 7,240,106.61 | -2.36% | 2.14% | 58.49% |
| April | 1,045,066.35 | 1,013,886.57 | 1,128,168.80 | 1,046,164.10 | 1,283,423.33 | 1,484,670.49 | 1,469,768.39 | 8,558,495.61 | | - | 0.00% | 0.00% | 0.00% |
| May | 892,413.93 | 996,145.89 | 1,035,008.39 | 1,052,938.24 | 1,242,602.83 | 1,156,115.45 | 1,184,701.24 | 9,743,196.85 | | - | 0.00% | 0.00% | 0.00% |
| June | 1,114,516.04 | 1,185,697.95 | 1,197,198.97 | 1,201,147.72 | 1,546,224.60 | 1,393,531.56 | 1,564,947.94 | 11,308,144.79 | | - | 0.00% | 0.00% | 0.00% |
| July | 1,338,119.60 | 1,385,070.74 | 1,202,352.28 | 1,262,763.88 | 1,640,598.95 | 1,434,891.95 | 1,405,132.46 | 12,713,277.25 | | - | 0.00% | 0.00% | 0.00% |
| August | 943,689.78 | 1,004,915.36 | 987,086.85 | 1,215,344.78 | 1,231,492.42 | 1,639,587.19 | 1,465,831.45 | 14,179,108.70 | | - | 0.00% | 0.00% | 0.00% |
| September | 1,175,277.19 | 1,222,254.64 | 1,363,784.87 | 1,398,544.20 | 1,873,564.48 | 1,524,385.73 | 1,525,827.23 | 15,704,935.93 | | - | 0.00% | 0.00% | 0.00% |
| October | 994,811.00 | 1,013,005.42 | 1,179,740.03 | 1,291,139.21 | 1,326,435.99 | 1,551,303.07 | 1,317,181.14 | 17,022,117.07 | | - | 0.00% | 0.00% | 0.00% |
| YTD Totals | 12,749,584.04 | 13,744,360.99 | 14,072,030.75 | 14,568,413.94 | 16,572,882.21 | 16,895,610.38 | 17,022,117.07 | 17,022,117.07 | 7,240,106.61 | 7,240,106.61 | -2.36% | 2.14% | 58.49% |

| | |
|---|---|
| Budgeted for FY 2023 | $ 17,442,000 |
| Y-T-D % Increase (Decrease) from FY 2022 | 2.14% |
| Actual % of FY 2023 Budget Remaining | 58.49% |
| % of Time Elapsed | 41.67% |

NOTE: Taxes are collected by the Department of Revenue approximately 30 days following the month in which taxable sales occur. Collections are remitted to the City by the 10th of each month for the prior months reported sales. Effective January 1, 2000, the State of Missouri Department of Revenue increased the threshold for monthly filing requirement from $250 to $500 for state tax collected.

Sales tax figures include the TIF sales tax collections. 50% of the TIF sales tax collections have to be remitted by the City to the TIF developer after being received from the State.

Actual budgeted increase is calculated by using the prior year actual collections compared to the budgeted amount.

This information is reported on a cash basis, while the accounting records are reported on an accrual basis.

CITY OF JOPLIN, MISSOURI

**GENERAL SALES TAX (38%)***

ACCOUNT # 001-9003-500-9805

SALES TAX REMITTANCES PER MONTH

| | FISCAL YEAR 2018 | | | | FISCAL YEAR 2019 | | | | FISCAL YEAR 2020 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developer | Admin. Fee** | Monthly Remittance | FY 2018 Y-T-D | Paid to TIF Developer | Admin. Fee** | Monthly Remittance | FY 2019 Y-T-D | Paid to TIF Developer | Admin. Fee** | Monthly Remittance | FY 2020 Y-T-D |
| November | 76,498.96 | 1,463.37 | 77,962.33 | 77,962.33 | 69,091.28 | 2,483.89 | 71,575.17 | 71,575.17 | 63,481.61 | 2,012.20 | 65,493.81 | 65,493.81 |
| December | 44,764.64 | 3,625.22 | 48,389.86 | 126,352.19 | 68,834.01 | 3,062.96 | 71,896.97 | 143,472.14 | 68,288.38 | 2,893.31 | 71,181.69 | 136,675.50 |
| January | 91,349.38 | 3,426.12 | 94,775.50 | 221,127.69 | 65,760.87 | 3,440.87 | 69,201.74 | 212,673.88 | 81,603.48 | 4,208.22 | 85,811.70 | 222,487.20 |
| February | 89,000.58 | 3,930.21 | 92,930.79 | 314,058.48 | 72,605.87 | 3,039.27 | 75,645.14 | 288,319.02 | 113,110.37 | 3,177.13 | 116,287.50 | 338,774.70 |
| March | 65,228.71 | 2,673.26 | 67,901.97 | 381,960.45 | 80,063.89 | 3,888.62 | 83,952.51 | 372,271.53 | 29,847.00 | 2,417.14 | 32,264.14 | 371,038.84 |
| April | 89,754.91 | 1,516.23 | 91,271.14 | 473,231.59 | 64,846.46 | 2,762.12 | 67,608.58 | 439,880.11 | 25,257.15 | 2,045.43 | 27,302.58 | 398,341.42 |
| May | 77,321.01 | 3,434.82 | 80,755.83 | 553,987.42 | 87,178.93 | 2,789.21 | 89,968.14 | 529,848.25 | 39,648.66 | 3,210.92 | 42,859.58 | 441,201.00 |
| June | 34,178.62 | 2,767.92 | 36,946.54 | 590,933.96 | 67,571.35 | 2,863.02 | 70,434.37 | 600,282.62 | 36,097.19 | 2,923.30 | 39,020.49 | 480,221.49 |
| July | 84,964.94 | 4,230.04 | 89,194.98 | 680,128.94 | 76,964.63 | 3,188.68 | 80,153.31 | 680,435.93 | 30,124.59 | 2,439.61 | 32,564.20 | 512,785.69 |
| August | 65,772.60 | 2,453.96 | 68,226.56 | 748,355.50 | 87,036.95 | 2,780.02 | 89,816.97 | 770,252.90 | 33,979.73 | 2,751.82 | 36,731.55 | 549,517.24 |
| September | 80,098.62 | 3,066.72 | 83,165.34 | 831,520.84 | 69,842.33 | 2,835.35 | 72,677.68 | 842,930.58 | 44,348.33 | 3,591.51 | 47,939.84 | 597,457.08 |
| October | 53,244.87 | 2,266.56 | 55,511.43 | 887,032.27 | 74,757.01 | 3,883.79 | 78,640.80 | 921,571.38 | 31,407.65 | 2,543.52 | 33,951.17 | 631,408.25 |
| YTD Totals | 852,177.84 | 34,854.43 | 887,032.27 | 887,032.27 | 884,553.58 | 37,017.80 | 921,571.38 | 921,571.38 | 597,194.14 | 34,214.11 | 631,408.25 | 631,408.25 |

| | FISCAL YEAR 2021 | | | | FISCAL YEAR 2022 | | | | FISCAL YEAR 2023 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developer | Admin. Fee** | Monthly Remittance | FY 2021 Y-T-D | Paid to TIF Developer | Admin. Fee** | Monthly Remittance | FY 2022 Y-T-D | Paid to TIF Developer | Admin. Fee** | Monthly Remittance | FY 2023 Y-T-D |
| November | 40,909.99 | 3,313.06 | 44,223.05 | 44,223.05 | 27,144.08 | 2,198.24 | 29,342.32 | 29,342.32 | 41,421.81 | 2,012.88 | 43,434.69 | 43,434.69 |
| December | 35,282.20 | 2,857.30 | 38,139.50 | 82,362.55 | 60,532.45 | 4,902.17 | 65,434.62 | 94,776.94 | 26,250.57 | 2,568.33 | 28,818.90 | 72,253.59 |
| January | 23,746.95 | 1,710.93 | 25,457.88 | 107,820.43 | 39,605.82 | 3,207.44 | 42,813.26 | 137,590.20 | 13,525.91 | 1,095.39 | 14,621.30 | 86,874.89 |
| February | 59,717.50 | 4,836.16 | 64,553.66 | 172,374.09 | 21,982.28 | 1,780.22 | 23,762.50 | 161,352.70 | 33,066.55 | 2,677.87 | 35,744.42 | 122,619.31 |
| March | 43,313.47 | 3,507.70 | 46,821.17 | 219,195.26 | 64,930.01 | 5,258.30 | 70,188.31 | 231,541.01 | 57,515.97 | 4,657.88 | 62,173.85 | 184,793.16 |
| April | 30,796.67 | 2,494.05 | 33,290.72 | 252,485.98 | 33,128.66 | 2,682.90 | 35,811.56 | 267,352.57 | 25,796.71 | 2,089.12 | 27,885.83 | 212,678.99 |
| May | 49,383.79 | 3,999.30 | 53,383.09 | 305,869.07 | 33,326.85 | 2,698.95 | 36,025.80 | 303,378.37 | 27,444.26 | 2,222.55 | 29,666.81 | 242,345.80 |
| June | 50,697.81 | 4,105.72 | 54,803.53 | 360,672.60 | 55,925.84 | 4,529.10 | 60,454.94 | 363,833.31 | 26,544.94 | 2,149.72 | 28,694.66 | 271,040.46 |
| July | - | - | - | 360,672.60 | 41,839.68 | 3,388.35 | 45,228.03 | 409,061.34 | 34,303.59 | 2,778.05 | 37,081.64 | 308,122.10 |
| August | 61,718.73 | 4,998.23 | 66,716.96 | 427,389.56 | 20,995.11 | 1,700.28 | 22,695.39 | 431,756.73 | 21,077.07 | 1,706.91 | 22,783.98 | 330,906.08 |
| September | 57,066.29 | 4,621.46 | 61,687.75 | 489,077.31 | 33,979.61 | 2,751.80 | 36,731.41 | 468,488.14 | 32,697.77 | 2,648.00 | 35,345.77 | 366,251.85 |
| October | 33,611.72 | 1,808.53 | 35,420.25 | 524,497.56 | 36,546.70 | 2,959.70 | 39,506.40 | 507,994.54 | 26,247.25 | 2,125.61 | 28,372.86 | 394,624.71 |
| YTD Totals | 486,245.12 | 38,252.44 | 524,497.56 | 524,497.56 | 469,937.09 | 38,057.45 | 507,994.54 | 507,994.54 | 365,892.40 | 28,732.31 | 394,624.71 | 366,251.85 |

| | FISCAL YEAR 2024 | | | | FISCAL YEAR 2025 | | | | FISCAL YEAR 2026 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developer | Admin. Fee** | Monthly Remittance | FY 2024 Y-T-D | Paid to TIF Developer | Admin. Fee** | Monthly Remittance | FY 2025 Y-T-D | Paid to TIF Developer | Admin. Fee** | Monthly Remittance | FY 2026 Y-T-D |
| November | 25,651.93 | $ 2,077.40 | 27,729.33 | 27,729.33 | | | - | - | | | - | - |
| December | 24,355.58 | 1,972.42 | 26,328.00 | 54,057.33 | | | - | - | | | - | - |
| January | 12,627.78 | 1,038.83 | 13,666.61 | 67,723.94 | | | - | - | | | - | - |
| February | 35,670.44 | 2,918.35 | 38,588.79 | 106,312.73 | | | - | - | | | - | - |
| March | 22,492.72 | 1,821.55 | 24,314.27 | 130,627.00 | | | - | - | | | - | - |
| April | | | - | - | | | - | - | | | - | - |
| May | | | - | - | | | - | - | | | - | - |
| June | | | - | - | | | - | - | | | - | - |
| July | | | - | - | | | - | - | | | - | - |
| August | | | - | - | | | - | - | | | - | - |
| September | | | - | - | | | - | - | | | - | - |
| October | | | - | - | | | - | - | | | - | - |
| YTD Totals | 120,798.45 | 9,828.55 | 130,627.00 | 130,627.00 | - | - | - | - | - | - | - | - |

*Percentage changed from 47% to 38% beginning with the June 2007 payment to the TIF developers due to the additional General Sales Tax for Police & Fire.

**A 5% fee is held out of the payment to the TIF developer as an administrative expense. The 5% fee goes into the General Fund as a revenue to the City. Administration fee dropped to 3% November 2007 (FY 2008).

**Note: Total collections are shown on the historical tax receipts report. The amounts above represent 50% of sales tax collections collected from the TIF districts. The above amounts have been remitted to the TIF developers and represent date paid to the developer and not the date collected from the state.**

CITY OF JOPLIN, MISSOURI

**GENERAL SALES TAX FOR POLICE & FIRE PENSION--1/2%***

ACCOUNT # 010-0000-400-0313 (Tax Type Code 202)

HISTORICAL TAX RECEIPTS BY MONTH

| | FY 2020 | FY 2021 | FY 2022 | FY 2023 | FY 2023 Y-T-D | FY 2024 | FY 2024 Y-T-D | Monthly % Change from FY 2023 | Y-T-D % Change from FY 2023 | Actual % of FY 2024 Budget Remaining |
|---|---|---|---|---|---|---|---|---|---|---|
| November | - | 535,663.79 | 580,270.98 | 656,529.03 | 656,529.03 | 648,756.08 | 648,756.08 | -1.18% | -1.18% | 92.88% |
| December | - | 703,796.64 | 736,011.96 | 747,012.77 | 1,403,541.80 | 767,589.51 | 1,416,345.59 | 2.75% | 0.91% | 84.47% |
| January | - | 675,387.57 | 713,539.63 | 754,804.01 | 2,158,345.81 | 798,044.72 | 2,214,390.31 | 5.73% | 2.60% | 75.71% |
| February | - | 677,662.13 | 767,231.31 | 776,092.19 | 2,934,438.00 | 807,096.00 | 3,021,486.31 | 3.99% | 2.97% | 66.86% |
| March | - | 712,434.09 | 640,626.10 | 682,348.71 | 3,616,786.71 | 649,890.06 | 3,671,376.37 | -4.76% | 1.51% | 59.73% |
| April | - | 651,616.53 | 755,818.69 | 738,946.93 | 4,355,733.64 | 745,688.33 | 4,417,064.70 | 0.91% | 1.41% | 51.55% |
| May | 27,005.46 | 642,760.86 | 592,095.29 | 603,407.92 | 4,959,141.56 | - | - | 0.00% | 0.00% | 0.00% |
| June | 409,843.94 | 798,423.11 | 718,799.57 | 794,497.13 | 5,753,638.69 | - | - | 0.00% | 0.00% | 0.00% |
| July | 609,949.85 | 817,504.98 | 734,530.23 | 717,731.00 | 6,471,369.69 | - | - | 0.00% | 0.00% | 0.00% |
| August | 618,667.76 | 640,539.32 | 825,343.77 | 741,280.05 | 7,212,649.74 | - | - | 0.00% | 0.00% | 0.00% |
| September | 708,995.63 | 964,438.81 | 777,202.19 | 778,075.94 | 7,990,725.68 | - | - | 0.00% | 0.00% | 0.00% |
| October | 650,705.81 | 677,729.93 | 791,033.10 | 670,213.13 | 8,660,938.81 | - | - | 0.00% | 0.00% | 0.00% |
| YTD Totals | 3,025,168.45 | 8,497,957.76 | 8,632,502.82 | 8,660,938.81 | 8,660,938.81 | 4,417,064.70 | 4,417,064.70 | 0.91% | 1.41% | 51.55% |

*Tax passed by voters November 2019. Tax effective April 1, 2020.

| | |
|---|---|
| Budgeted for FY 2024 | $ 9,117,270 |
| Y-T-D % Increase (Decrease) from FY 2023 | 1.41% |
| Actual % of FY 2024 Budget Remaining | 51.55% |
| % of Time Elapsed | 50.00% |

NOTE: Taxes are collected by the Department of Revenue approximately 30 days following the month in which taxable sales occur. Collections are remitted to the City by the 10th of each month for the prior months reported sales. Effective January 1, 2000, the State of Missouri Department of Revenue increased the threshold for monthly filing requirement from $250 to $500 for state tax collected.

Sales tax figures include the TIF sales tax collections. 50% of the TIF sales tax collections have to be remitted by the City to the TIF developer after being received from the State.

Actual budgeted increase is calculated by using the prior year actual collections compared to the budgeted amount.

This information is reported on a cash basis, while the accounting records are reported on an accrual basis.

CITY OF JOPLIN, MISSOURI

**GENERAL SALES TAX FOR POLICE & FIRE --1/2%***

ACCOUNT # 101-0000-400-0312 (Tax Type Code 201)

HISTORICAL TAX RECEIPTS BY MONTH

| | FY 2018 | FY 2019 | FY 2020 | FY 2021 | FY 2022 | FY 2023 | FY 2023 Y-T-D | FY 2024 | FY 2024 Y-T-D | Monthly % Change from FY 2023 | Y-T-D % Change from FY 2023 | Actual % of FY 2024 Budget Remaining |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| November | 432,457.56 | 509,064.16 | 544,700.84 | 537,750.61 | 583,839.02 | 659,342.89 | 659,342.89 | 649,379.73 | 649,379.73 | -1.51% | -1.51% | 92.88% |
| December | 861,997.66 | 615,680.31 | 677,338.25 | 701,509.00 | 742,051.14 | 748,000.30 | 1,407,343.19 | 768,595.42 | 1,417,975.15 | 2.75% | 0.76% | 84.45% |
| January | 506,398.03 | 723,740.71 | 676,631.41 | 678,821.35 | 715,479.02 | 755,646.03 | 2,162,989.22 | 798,276.85 | 2,216,252.00 | 5.64% | 2.46% | 75.69% |
| February | 670,561.05 | 633,762.08 | 667,542.37 | 680,236.65 | 773,898.05 | 776,506.34 | 2,939,495.56 | 805,833.24 | 3,022,085.24 | 3.78% | 2.81% | 66.85% |
| March | 671,873.58 | 680,020.06 | 660,377.56 | 716,239.81 | 641,422.41 | 684,313.08 | 3,623,808.64 | 650,742.12 | 3,672,827.36 | -4.91% | 1.35% | 59.72% |
| April | 551,626.62 | 595,796.46 | 534,740.95 | 657,053.60 | 758,115.03 | 746,720.95 | 4,370,529.59 | 745,621.16 | 4,418,448.52 | -0.15% | 1.10% | 51.54% |
| May | 536,268.63 | 560,936.61 | 545,959.21 | 645,967.55 | 592,875.30 | 605,190.91 | 4,975,720.50 | - | - | 0.00% | 0.00% | 0.00% |
| June | 608,968.16 | 631,632.40 | 618,450.70 | 798,139.28 | 722,595.07 | 795,094.46 | 5,770,814.96 | - | - | 0.00% | 0.00% | 0.00% |
| July | 734,615.78 | 639,169.79 | 646,310.78 | 820,183.62 | 735,812.47 | 718,430.80 | 6,489,245.76 | - | - | 0.00% | 0.00% | 0.00% |
| August | 534,861.93 | 536,592.93 | 624,237.41 | 645,647.41 | 826,975.17 | 742,864.62 | 7,232,110.38 | - | - | 0.00% | 0.00% | 0.00% |
| September | 650,774.69 | 716,033.23 | 721,198.53 | 964,756.17 | 776,085.56 | 778,707.67 | 8,010,818.05 | - | - | 0.00% | 0.00% | 0.00% |
| October | 532,915.48 | 627,014.08 | 660,951.69 | 679,354.50 | 792,614.64 | 670,633.14 | 8,681,451.19 | - | - | 0.00% | 0.00% | 0.00% |
| YTD Totals | 7,293,319.17 | 7,469,442.82 | 7,578,439.70 | 8,525,659.55 | 8,661,762.88 | 8,681,451.19 | 8,681,451.19 | 4,418,448.52 | 4,418,448.52 | -0.15% | 1.10% | 51.54% |

*Tax passed by voters November 2006. Tax effective April 1, 2007.

| | |
|---|---|
| Budgeted for FY 2024 | $ 9,117,270 |
| Y-T-D % Increase (Decrease) from FY 2023 | 1.10% |
| Actual % of FY 2024 Budget Remaining | 51.54% |
| % of Time Elapsed | 50.00% |

NOTE: Taxes are collected by the Department of Revenue approximately 30 days following the month in which taxable sales occur. Collections are remitted to the City by the 10th of each month for the prior months reported sales. Effective January 1, 2000, the State of Missouri Department of Revenue increased the threshold for monthly filing requirement from $250 to $500 for state tax collected.

Sales tax figures include the TIF sales tax collections. 50% of the TIF sales tax collections have to be remitted by the City to the TIF developer after being received from the State.

Actual budgeted increase is calculated by using the prior year actual collections compared to the budgeted amount.

This information is reported on a cash basis, while the accounting records are reported on an accrual basis.

CITY OF JOPLIN, MISSOURI

**GENERAL POLICE & FIRE SALES TAX (19%)**

ACCOUNT # 101-9003-500-9805

SALES TAX REMITTANCES PER MONTH

| | FISCAL YEAR 2015 | | FISCAL YEAR 2016 | | FISCAL YEAR 2017 | | FISCAL YEAR 2018 | |
|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developer | FY 2015 Y-T-D | Paid to TIF Developer | FY 2016 Y-T-D | Paid to TIF Developer | FY 2017 Y-T-D | Paid to TIF Developer | FY 2018 Y-T-D |
| November | 15,119.09 | 15,119.09 | 30,930.04 | 30,930.04 | 43,706.90 | 43,706.90 | 37,678.59 | 37,678.59 |
| December | 20,657.22 | 35,776.31 | 17,988.89 | 48,918.93 | 25,268.49 | 68,975.39 | 22,048.25 | 59,726.84 |
| January | 32,272.01 | 68,048.32 | 36,782.48 | 85,701.41 | 38,582.91 | 107,558.30 | 44,992.98 | 104,719.82 |
| February | 33,687.16 | 101,735.48 | 31,220.78 | 116,922.19 | 31,871.17 | 139,429.47 | 43,836.10 | 148,555.92 |
| March | 3,699.49 | 105,434.96 | 34,761.11 | 151,683.30 | 27,992.77 | 167,422.24 | 32,127.58 | 180,683.50 |
| April | 56,291.08 | 161,726.04 | 49,925.49 | 201,608.79 | 39,272.59 | 206,694.83 | 44,207.64 | 224,891.14 |
| May | 34,763.84 | 196,489.88 | 33,337.02 | 234,945.81 | 33,130.56 | 239,825.39 | 38,083.48 | 262,974.62 |
| June | 17,313.70 | 213,803.58 | 23,408.47 | 258,354.28 | 27,978.80 | 267,804.19 | 16,834.24 | 279,808.86 |
| July | 27,909.40 | 241,712.98 | 36,086.09 | 294,440.37 | 36,656.30 | 304,460.49 | 41,848.40 | 321,657.26 |
| August | 30,862.36 | 272,575.34 | 28,824.37 | 323,264.74 | 37,420.57 | 341,881.06 | 32,395.46 | 354,052.72 |
| September | 16,579.98 | 289,155.32 | 21,831.21 | 345,095.95 | 34,427.45 | 376,308.51 | 39,451.56 | 393,504.28 |
| October | 30,745.09 | 319,900.41 | 30,899.50 | 375,995.45 | 42,175.88 | 418,484.39 | 26,225.09 | 419,729.37 |
| **YTD Totals** | **319,900.41** | **319,900.41** | **375,995.45** | **375,995.45** | **418,484.39** | **418,484.39** | **419,729.37** | **419,729.37** |

| | FISCAL YEAR 2019 | | FISCAL YEAR 2020 | | FISCAL YEAR 2021 | | FISCAL YEAR 2022 | |
|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developer | FY 2019 Y-T-D | Paid to TIF Developer | FY 2020 Y-T-D | Paid to TIF Developer | FY 2021 Y-T-D | Paid to TIF Developer | FY 2022 Y-T-D |
| November | 34,030.03 | 34,030.03 | 31,267.06 | 31,267.06 | 20,149.70 | 20,149.70 | 13,369.47 | 13,369.47 |
| December | 33,903.32 | 67,933.35 | 33,634.58 | 64,901.64 | 17,377.80 | 37,527.50 | 29,814.49 | 43,183.96 |
| January | 32,389.68 | 100,323.03 | 40,192.76 | 105,094.40 | 11,696.26 | 49,223.76 | 19,507.35 | 62,691.31 |
| February | 35,761.10 | 136,084.13 | 55,711.08 | 160,805.48 | 29,413.10 | 78,636.86 | 10,827.09 | 73,518.40 |
| March | 39,434.45 | 175,518.58 | 14,700.76 | 175,506.24 | 21,333.50 | 99,970.36 | 31,980.45 | 105,498.85 |
| April | 31,939.30 | 207,457.88 | 12,440.09 | 187,946.33 | 15,168.51 | 115,138.87 | 16,317.10 | 121,815.95 |
| May | 42,938.87 | 250,396.75 | 19,528.44 | 207,474.77 | 24,323.36 | 139,462.23 | 16,414.72 | 138,230.67 |
| June | 33,281.41 | 283,678.16 | 17,779.21 | 225,253.98 | 24,970.56 | 164,432.79 | 27,545.56 | 165,776.23 |
| July | 37,907.95 | 321,586.11 | 14,837.48 | 240,091.46 | - | 164,432.79 | 20,607.60 | 186,383.83 |
| August | 42,868.95 | 364,455.06 | 16,736.29 | 256,827.75 | 30,398.78 | 194,831.57 | 10,340.87 | 196,724.70 |
| September | 34,399.95 | 398,855.01 | 21,843.21 | 278,670.96 | 28,107.28 | 222,938.85 | 16,736.22 | 213,460.92 |
| October | 36,820.61 | 435,675.62 | 15,469.44 | 294,140.40 | 16,555.03 | 239,493.88 | 18,000.61 | 231,461.53 |
| **YTD Totals** | **435,675.62** | **435,675.62** | **294,140.40** | **294,140.40** | **239,493.88** | **239,493.88** | **231,461.53** | **231,461.53** |

| | FISCAL YEAR 2023 | | FISCAL YEAR 2024 | | FISCAL YEAR 2025 | | FISCAL YEAR 2026 | |
|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developer | FY 2022 Y-T-D | Paid to TIF Developer | FY 2022 Y-T-D | Paid to TIF Developer | FY 2022 Y-T-D | Paid to TIF Developer | FY 2022 Y-T-D |
| November | 20,401.78 | 20,401.78 | 12,634.53 | 12,634.53 | - | - | - | - |
| December | 12,929.38 | 33,331.16 | 11,996.03 | 24,630.56 | - | - | - | - |
| January | 6,662.02 | 39,993.18 | 6,219.65 | 30,850.21 | - | - | - | - |
| February | 16,286.51 | 56,279.69 | 17,569.02 | 48,419.23 | - | - | - | - |
| March | 28,328.76 | 84,608.45 | 11,078.50 | 59,497.73 | - | - | - | - |
| April | 12,705.84 | 97,314.29 | - | - | - | - | - | - |
| May | 13,517.32 | 110,831.61 | - | - | - | - | - | - |
| June | 13,074.37 | 123,905.98 | - | - | - | - | - | - |
| July | 16,895.80 | 140,801.78 | - | - | - | - | - | - |
| August | 10,381.24 | 151,183.02 | - | - | - | - | - | - |
| September | 16,104.87 | 167,287.89 | - | - | - | - | - | - |
| October | 12,927.75 | 180,215.64 | - | - | - | - | - | - |
| **YTD Totals** | **180,215.64** | **180,215.64** | **59,497.73** | **59,497.73** | **-** | **-** | **-** | **-** |

Note: Total collections are shown on the historical tax receipts report. The amounts above represent 50% of sales tax collections collected from the TIF districts. The above amounts have been remitted to the TIF developers and represent date paid to the developer and not the date collected from the state.

CITY OF JOPLIN, MISSOURI

**PARKS & STORMWATER SALES TAX --1/4%**

ACCOUNT # 130-0000-400-0306 & 0307 (Tax Type Code 260)

HISTORICAL TAX RECEIPTS BY MONTH

| | FY 2018 | FY 2019 | FY 2020 | FY 2021 | FY 2022 | FY 2023 | FY 2023 Y-T-D | FY 2024 | FY 2024 Y-T-D | Monthly % Change from FY 2023 | Y-T-D % Change from FY 2023 | Actual % of FY 2024 Budget Remaining |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| November | 216,228.57 | 254,532.30 | 272,356.57 | 268,875.08 | 291,920.12 | 329,671.23 | 329,671.23 | 324,690.44 | 324,690.44 | -1.51% | -1.51% | 92.88% |
| December | 430,998.32 | 307,839.68 | 338,668.97 | 350,754.38 | 371,025.32 | 374,000.37 | 703,671.60 | 384,297.41 | 708,987.85 | 2.75% | 0.76% | 84.45% |
| January | 253,198.71 | 361,870.28 | 338,316.02 | 339,410.59 | 357,739.99 | 377,823.32 | 1,081,494.92 | 399,138.48 | 1,108,126.33 | 5.64% | 2.46% | 75.69% |
| February | 335,278.24 | 316,881.33 | 333,770.51 | 340,120.33 | 386,971.57 | 388,253.52 | 1,469,748.44 | 402,917.05 | 1,511,043.38 | 3.78% | 2.81% | 66.85% |
| March | 335,936.56 | 340,010.00 | 330,188.70 | 358,119.99 | 320,710.78 | 342,156.53 | 1,811,904.97 | 325,370.87 | 1,836,414.25 | -4.91% | 1.35% | 59.72% |
| April | 275,813.16 | 297,897.88 | 267,370.11 | 328,526.69 | 379,057.50 | 373,360.52 | 2,185,265.49 | 372,810.74 | 2,209,224.99 | -0.15% | 1.10% | 51.54% |
| May | 268,151.07 | 280,467.68 | 272,979.04 | 322,983.47 | 296,437.40 | 302,595.76 | 2,487,861.25 | - | - | 0.00% | 0.00% | 0.00% |
| June | 304,484.24 | 315,816.05 | 309,224.94 | 399,069.59 | 361,297.97 | 397,546.90 | 2,885,408.15 | - | - | 0.00% | 0.00% | 0.00% |
| July | 367,307.66 | 319,584.71 | 323,155.02 | 410,092.07 | 367,906.13 | 359,215.14 | 3,244,623.29 | - | - | 0.00% | 0.00% | 0.00% |
| August | 267,431.08 | 268,296.43 | 312,118.45 | 322,823.53 | 413,487.46 | 371,432.30 | 3,616,055.59 | - | - | 0.00% | 0.00% | 0.00% |
| September | 325,388.58 | 358,016.60 | 360,598.73 | 482,377.87 | 388,042.53 | 389,353.82 | 4,005,409.41 | - | - | 0.00% | 0.00% | 0.00% |
| October | 266,464.39 | 313,506.79 | 330,475.56 | 339,677.27 | 396,307.75 | 335,316.35 | 4,340,725.76 | - | - | 0.00% | 0.00% | 0.00% |
| YTD Totals | 3,646,680.58 | 3,734,719.73 | 3,789,222.62 | 4,262,830.86 | 4,330,904.52 | 4,340,725.76 | 4,340,725.76 | 2,209,224.99 | 2,209,224.99 | -0.15% | 1.10% | 51.54% |

| | |
|---|---|
| Budgeted for FY 2024 | $ 4,558,635 |
| Y-T-D % Increase (Decrease) from FY 2023 | 1.10% |
| Actual % of FY 2024 Budget Remaining | 51.54% |
| % of Time Elapsed | 50.00% |

NOTE: Taxes are collected by the Department of Revenue approximately 30 days following the month in which taxable sales occur. Collections are remitted to the City by the 10th of each month for the prior months reported sales. Effective January 1, 2000, the State of Missouri Department of Revenue increased the threshold for monthly filing requirement from $250 to $500 for state tax collected.

Sales tax figures include the TIF sales tax collections. 50% of the TIF sales tax collections have to be remitted by the City to the TIF developer after being received from the State.

Actual budgeted increase is calculated by using the prior year actual collections compared to the budgeted amount.

This information is reported on a cash basis, while the accounting records are reported on an accrual basis.

# CITY OF JOPLIN, MISSOURI
## PARKS & STORMWATER SALES TAX (10%)*
## ACCOUNT # 130-9003-530-9805 & 130-9003-560-9805
## SALES TAX REMITTANCES PER MONTH

| | FISCAL YEAR 2022 | | FISCAL YEAR 2023 | | FISCAL YEAR 2024 | | FISCAL YEAR 2025 | |
|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developers | FY 2022 Y-T-D | Paid to TIF Developers | FY 2023 Y-T-D | Paid to TIF Developers | FY 2024 Y-T-D | Paid to TIF Developers | FY 2025 Y-T-D |
| November | 7,107.64 | 7,107.64 | 10,846.24 | 10,846.24 | 6,716.92 | 6,716.92 | - | - |
| December | 15,850.34 | 22,957.98 | 6,873.68 | 17,719.92 | 6,377.48 | 13,094.40 | - | - |
| January | 10,370.73 | 33,328.71 | 3,541.74 | 21,261.66 | 3,306.57 | 16,400.97 | - | - |
| February | 5,756.03 | 39,084.74 | 8,658.43 | 21,261.66 | 9,340.26 | 25,741.23 | - | - |
| March | 17,001.84 | 56,086.58 | 15,060.48 | 44,980.57 | 5,889.69 | 31,630.92 | - | - |
| April | 8,674.70 | 64,761.28 | 6,754.84 | 51,735.41 | - | - | - | - |
| May | 8,726.59 | 73,487.87 | 7,186.24 | 58,921.65 | - | - | - | - |
| June | 14,644.11 | 88,131.98 | 6,950.76 | 65,872.41 | - | - | - | - |
| July | 10,955.66 | 99,087.64 | 8,982.35 | 74,854.76 | - | - | - | - |
| August | 5,497.54 | 104,585.18 | 5,519.00 | 80,373.76 | - | - | - | - |
| September | 8,897.51 | 113,482.69 | 8,561.87 | 88,935.63 | - | - | - | - |
| October | 9,569.70 | 123,052.39 | 6,872.81 | 95,808.44 | - | - | - | - |
| **YTD Totals** | **123,052.39** | **123,052.39** | **95,808.44** | **95,808.44** | **31,630.92** | **31,630.92** | **-** | **-** |

| | FISCAL YEAR 2026 | | FISCAL YEAR 2027 | | FISCAL YEAR 2028 | | FISCAL YEAR 2029 | |
|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developers | FY 2026 Y-T-D | Paid to TIF Developers | FY 2027 Y-T-D | Paid to TIF Developers | FY 2028 Y-T-D | Paid to TIF Developers | FY 2029 Y-T-D |
| November | - | - | - | - | - | - | - | - |
| December | - | - | - | - | - | - | - | - |
| January | - | - | - | - | - | - | - | - |
| February | - | - | - | - | - | - | - | - |
| March | - | - | - | - | - | - | - | - |
| April | - | - | - | - | - | - | - | - |
| May | - | - | - | - | - | - | - | - |
| June | - | - | - | - | - | - | - | - |
| July | - | - | - | - | - | - | - | - |
| August | - | - | - | - | - | - | - | - |
| September | - | - | - | - | - | - | - | - |
| October | - | - | - | - | - | - | - | - |
| **YTD Totals** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** |

*Percentage changed from 11.8% to10% beginning with the June 2007 payment to the TIF developers due to the additional General Sales Tax for Police & Fire.

**Note: Total collections are shown on the historical tax receipts report. The amounts above represent 50% of sales tax collections collected from the TIF districts. The above amounts have been remitted to the TIF developers and represent date paid to the developer and not the date collected from the state.**

# CITY OF JOPLIN, MISSOURI
## TRANSPORTATION SALES TAX --1/2%
## ACCOUNT # 140-0000-400-0302 (Tax Type Code 215)
## HISTORICAL TAX RECEIPTS BY MONTH

| | FY 2018 | FY 2019 | FY 2020 | FY 2021 | FY 2022 | FY 2023 | FY 2023 Y-T-D | FY 2024 | FY 2024 Y-T-D | Monthly % Change from FY 2023 | Y-T-D % Change from FY 2023 | Actual % of FY 2024 Budget Remaining |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| November | 432,420.42 | 509,336.78 | 545,214.59 | 537,913.56 | 585,895.96 | 660,844.34 | 660,844.34 | 650,557.20 | 650,557.20 | -1.56% | -1.56% | 92.86% |
| December | 862,156.43 | 616,437.35 | 677,641.12 | 701,677.42 | 743,336.54 | 748,805.87 | 1,409,650.21 | 770,137.90 | 1,420,695.10 | 2.85% | 0.78% | 84.42% |
| January | 506,429.50 | 725,424.74 | 676,784.92 | 679,145.12 | 715,510.08 | 758,047.31 | 2,167,697.52 | 799,980.33 | 2,220,675.43 | 5.53% | 2.44% | 75.64% |
| February | 671,486.26 | 635,548.13 | 667,583.59 | 680,265.13 | 774,747.92 | 777,085.98 | 2,944,783.50 | 807,294.06 | 3,027,969.49 | 3.89% | 2.82% | 66.79% |
| March | 672,620.42 | 680,776.00 | 661,127.22 | 716,754.43 | 643,169.09 | 685,471.01 | 3,630,254.51 | 652,483.09 | 3,680,452.58 | -4.81% | 1.38% | 59.63% |
| April | 551,820.80 | 596,506.99 | 535,710.72 | 657,109.71 | 758,899.67 | 747,782.92 | 4,378,037.43 | 748,151.49 | 4,428,604.07 | 0.05% | 1.16% | 51.43% |
| May | 536,733.66 | 561,093.96 | 546,293.73 | 645,993.43 | 594,721.89 | 606,072.45 | 4,984,109.88 | - | - | 0.00% | 0.00% | 0.00% |
| June | 609,938.18 | 632,385.22 | 618,622.76 | 798,460.76 | 724,728.50 | 795,746.57 | 5,779,856.45 | - | - | 0.00% | 0.00% | 0.00% |
| July | 735,017.79 | 639,659.01 | 646,444.54 | 820,298.96 | 738,365.35 | 719,717.57 | 6,499,574.02 | - | - | 0.00% | 0.00% | 0.00% |
| August | 535,343.84 | 537,061.77 | 624,662.11 | 646,605.79 | 830,290.87 | 743,454.31 | 7,243,028.33 | - | - | 0.00% | 0.00% | 0.00% |
| September | 651,176.48 | 716,813.63 | 721,446.39 | 965,315.43 | 779,183.12 | 779,262.58 | 8,022,290.91 | - | - | 0.00% | 0.00% | 0.00% |
| October | 533,127.91 | 627,248.75 | 661,273.59 | 680,027.76 | 793,924.62 | 671,714.45 | 8,694,005.36 | - | - | 0.00% | 0.00% | 0.00% |
| YTD Totals | 7,298,271.69 | 7,478,292.33 | 7,582,805.28 | 8,529,567.50 | 8,682,773.61 | 8,694,005.36 | 8,694,005.36 | 4,428,604.07 | 4,428,604.07 | 0.05% | 1.16% | 51.43% |

| | |
|---|---|
| Budgeted for FY 2024 | $ 9,117,270 |
| Y-T-D % Increase (Decrease) from FY 2023 | 1.16% |
| Actual % of FY 2024 Budget Remaining | 51.43% |
| % of Time Elapsed | 50.00% |

NOTE: Taxes are collected by the Department of Revenue approximately 30 days following the month in which taxable sales occur. Collections are remitted to the City by the 10th of each month for the prior months reported sales. Effective January 1, 2000, the State of Missouri Department of Revenue increased the threshold for monthly filing requirement from $250 to $500 for state tax collected.

Sales tax figures include the TIF sales tax collections. 50% of the TIF sales tax collections have to be remitted by the City to the TIF developer after being received from the State.

Actual budgeted increase is calculated by using the prior year actual collections compared to the budgeted amount.

This information is reported on a cash basis, while the accounting records are reported on an accrual basis.

# CITY OF JOPLIN, MISSOURI
## TRANSPORTATION SALES TAX (19%)*
## ACCOUNT # 140-9003-530-9805
## SALES TAX REMITTANCES PER MONTH

| | FISCAL YEAR 2022 | | FISCAL YEAR 2023 | | FISCAL YEAR 2024 | | FISCAL YEAR 2025 | |
|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developers | FY 2022 Y-T-D | Paid to TIF Developers | FY 2023 Y-T-D | Paid to TIF Developers | FY 2024 Y-T-D | Paid to TIF Developers | FY 2025 Y-T-D |
| November | 13,504.52 | 13,504.52 | 20,607.86 | 20,607.86 | 12,762.15 | 12,762.15 | - | - |
| December | 30,115.65 | 43,620.17 | 13,059.98 | 33,667.84 | 12,117.20 | 24,879.35 | - | - |
| January | 19,704.39 | 63,324.56 | 6,729.31 | 40,397.15 | 6,282.48 | 31,161.83 | - | - |
| February | 10,936.46 | 74,261.02 | 16,451.02 | 56,848.17 | 17,746.49 | 48,908.32 | - | - |
| March | 32,303.49 | 106,564.51 | 28,614.91 | 85,463.08 | 11,190.40 | 60,098.72 | - | - |
| April | 16,481.92 | 123,046.43 | 12,834.19 | 98,297.27 | - | - | - | - |
| May | 16,580.52 | 139,626.95 | 13,653.86 | 111,951.13 | - | - | - | - |
| June | 27,823.80 | 167,450.75 | 13,206.44 | 125,157.57 | - | - | - | - |
| July | 20,815.76 | 188,266.51 | 17,066.47 | 142,224.04 | - | - | - | - |
| August | 10,445.33 | 198,711.84 | 10,486.11 | 152,710.15 | - | - | - | - |
| September | 16,905.28 | 215,617.12 | 16,267.55 | 168,977.70 | - | - | - | - |
| October | 18,182.44 | 233,799.56 | 13,058.33 | 182,036.03 | - | - | - | - |
| **YTD Totals** | **233,799.56** | **233,799.56** | **182,036.03** | **182,036.03** | **60,098.72** | **60,098.72** | - | - |

| | FISCAL YEAR 2026 | | FISCAL YEAR 2027 | | FISCAL YEAR 2028 | | FISCAL YEAR 2029 | |
|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developers | FY 2026 Y-T-D | Paid to TIF Developers | FY 2027 Y-T-D | Paid to TIF Developers | FY 2028 Y-T-D | Paid to TIF Developers | FY 2029 Y-T-D |
| November | - | - | - | - | - | - | - | - |
| December | - | - | - | - | - | - | - | - |
| January | - | - | - | - | - | - | - | - |
| February | - | - | - | - | - | - | - | - |
| March | - | - | - | - | - | - | - | - |
| April | - | - | - | - | - | - | - | - |
| May | - | - | - | - | - | - | - | - |
| June | - | - | - | - | - | - | - | - |
| July | - | - | - | - | - | - | - | - |
| August | - | - | - | - | - | - | - | - |
| September | - | - | - | - | - | - | - | - |
| October | - | - | - | - | - | - | - | - |
| **YTD Totals** | - | - | - | - | - | - | - | - |

*Percentage changed from 11.8% to10% beginning with the June 2007 payment to the TIF developers due to the additional General Sales Tax for Police & Fire.

**Note: Total collections are shown on the historical tax receipts report. The amounts above represent 50% of sales tax collections collected from the TIF districts. The above amounts have been remitted to the TIF developers and represent date paid to the developer and not the date collected from the state.**

CITY OF JOPLIN, MISSOURI

**CAPITAL IMPROVEMENT SALES TAX --3/8%**

ACCOUNT # 145-0000-400-0308 (Tax Type Code 210)

HISTORICAL TAX RECEIPTS BY MONTH

| | FY 2018 | FY 2019 | FY 2020 | FY 2021 | FY 2022 | FY 2023 | FY 2023 Y-T-D | FY 2024 | FY 2024 Y-T-D | Monthly % Change from FY 2023 | Y-T-D % Change from FY 2023 | Actual % of FY 2024 Budget Remaining |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| November | 324,343.25 | 381,798.45 | 408,534.06 | 403,312.57 | 437,879.01 | 494,506.85 | 494,506.85 | 487,034.93 | 487,034.93 | -1.51% | -1.51% | 92.88% |
| December | 646,497.65 | 461,760.49 | 508,003.66 | 526,131.61 | 556,538.25 | 560,999.69 | 1,055,506.54 | 576,446.62 | 1,063,481.55 | 2.75% | 0.76% | 84.45% |
| January | 379,798.62 | 542,805.76 | 507,473.32 | 509,116.02 | 536,609.68 | 566,734.92 | 1,622,241.46 | 598,707.50 | 1,662,189.05 | 5.64% | 2.46% | 75.69% |
| February | 502,917.97 | 475,321.60 | 500,656.25 | 510,180.01 | 580,457.12 | 582,379.95 | 2,204,621.41 | 604,375.28 | 2,266,564.33 | 3.78% | 2.81% | 66.85% |
| March | 503,904.91 | 510,014.83 | 495,283.25 | 537,179.60 | 481,066.36 | 513,235.18 | 2,717,856.59 | 488,056.56 | 2,754,620.89 | -4.91% | 1.35% | 59.72% |
| April | 413,719.82 | 446,847.84 | 401,055.54 | 492,790.62 | 568,586.34 | 560,041.29 | 3,277,897.88 | 559,215.97 | 3,313,836.86 | -0.15% | 1.10% | 51.54% |
| May | 402,200.92 | 420,701.61 | 409,469.18 | 484,475.40 | 444,656.09 | 453,893.08 | 3,731,790.96 | - | - | 0.00% | 0.00% | 0.00% |
| June | 456,726.03 | 473,724.29 | 463,837.55 | 598,604.66 | 541,946.50 | 596,320.02 | 4,328,110.98 | - | - | 0.00% | 0.00% | 0.00% |
| July | 550,961.84 | 479,377.25 | 484,732.73 | 615,137.76 | 551,859.31 | 538,823.12 | 4,866,934.10 | - | - | 0.00% | 0.00% | 0.00% |
| August | 401,146.37 | 402,444.81 | 468,178.34 | 484,234.79 | 620,231.49 | 557,148.62 | 5,424,082.72 | - | - | 0.00% | 0.00% | 0.00% |
| September | 488,080.89 | 537,025.17 | 540,898.55 | 723,566.66 | 582,064.06 | 584,031.44 | 6,008,114.16 | - | - | 0.00% | 0.00% | 0.00% |
| October | 399,702.28 | 470,260.48 | 495,713.98 | 509,515.75 | 594,460.89 | 502,974.39 | 6,511,088.55 | - | - | 0.00% | 0.00% | 0.00% |
| YTD Totals | 5,470,000.55 | 5,602,082.58 | 5,683,836.41 | 6,394,245.45 | 6,496,355.10 | 6,511,088.55 | 6,511,088.55 | 3,313,836.86 | 3,313,836.86 | -0.15% | 1.10% | 51.54% |

| | |
|---|---|
| Budgeted for FY 2024 | $ 6,837,953 |
| Y-T-D % Increase (Decrease) from FY 2023 | 1.10% |
| Actual % of FY 2024 Budget Remaining | 51.54% |
| % of Time Elapsed | 50.00% |

NOTE: Taxes are collected by the Department of Revenue approximately 30 days following the month in which taxable sales occur. Collections are remitted to the City by the 10th of each month for the prior months reported sales. Effective January 1, 2000, the State of Missouri Department of Revenue increased the threshold for monthly filing requirement from $250 to $500 for state tax collected.

Sales tax figures include the TIF sales tax collections. 50% of the TIF sales tax collections have to be remitted by the City to the TIF developer after being received from the State.

Actual budgeted increase is calculated by using the prior year actual collections compared to the budgeted amount.

This information is reported on a cash basis, while the accounting records are reported on an accrual basis.

# CITY OF JOPLIN, MISSOURI
## CAPITAL IMPROVEMENT SALES TAX (14%)*
## ACCOUNT # 145-9003-520-9805
## SALES TAX REMITTANCES PER MONTH

| | FISCAL YEAR 2022 | | FISCAL YEAR 2023 | | FISCAL YEAR 2024 | | FISCAL YEAR 2025 | |
|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developers | FY 2022 Y-T-D | Paid to TIF Developers | FY 2023 Y-T-D | Paid to TIF Developers | FY 2024 Y-T-D | Paid to TIF Developers | FY 2025 Y-T-D |
| November | 9,950.70 | 9,950.70 | 15,184.74 | 15,184.74 | 9,403.69 | 9,403.69 | - | - |
| December | 22,190.48 | 32,141.18 | 9,623.15 | 24,807.89 | 8,928.47 | 18,332.16 | - | - |
| January | 14,519.02 | 46,660.20 | 4,958.44 | 29,766.33 | 4,629.19 | 22,961.35 | - | - |
| February | 8,058.44 | 54,718.64 | 12,121.80 | 41,888.13 | 13,076.36 | 36,037.71 | - | - |
| March | 23,802.57 | 78,521.21 | 21,084.67 | 62,972.80 | 8,245.56 | 44,283.27 | - | - |
| April | 12,144.57 | 90,665.78 | 9,456.77 | 72,429.57 | - | - | - | - |
| May | 12,217.23 | 102,883.01 | 10,060.74 | 82,490.31 | - | - | - | - |
| June | 20,501.75 | 123,384.76 | 9,731.06 | 92,221.37 | - | - | - | - |
| July | 15,337.93 | 138,722.69 | 12,575.29 | 104,796.66 | - | - | - | - |
| August | 7,696.56 | 146,419.25 | 7,726.60 | 112,523.26 | - | - | - | - |
| September | 12,456.52 | 158,875.77 | 11,986.61 | 124,509.87 | - | - | - | - |
| October | 13,397.59 | 172,273.36 | 9,621.93 | 134,131.80 | - | - | - | - |
| **YTD Totals** | **172,273.36** | **172,273.36** | **134,131.80** | **134,131.80** | **44,283.27** | **44,283.27** | - | - |

| | FISCAL YEAR 2026 | | FISCAL YEAR 2027 | | FISCAL YEAR 2028 | | FISCAL YEAR 2029 | |
|---|---|---|---|---|---|---|---|---|
| | Paid to TIF Developers | FY 2026 Y-T-D | Paid to TIF Developers | FY 2027 Y-T-D | Paid to TIF Developers | FY 2028 Y-T-D | Paid to TIF Developers | FY 2029 Y-T-D |
| November | - | - | - | - | - | - | - | - |
| December | - | - | - | - | - | - | - | - |
| January | - | - | - | - | - | - | - | - |
| February | - | - | - | - | - | - | - | - |
| March | - | - | - | - | - | - | - | - |
| April | - | - | - | - | - | - | - | - |
| May | - | - | - | - | - | - | - | - |
| June | - | - | - | - | - | - | - | - |
| July | - | - | - | - | - | - | - | - |
| August | - | - | - | - | - | - | - | - |
| September | - | - | - | - | - | - | - | - |
| October | - | - | - | - | - | - | - | - |
| **YTD Totals** | - | - | - | - | - | - | - | - |

*Percentage changed from 11.8% to10% beginning with the June 2007 payment to the TIF developers due to the additional General Sales Tax for Police & Fire.

**Note: Total collections are shown on the historical tax receipts report. The amounts above represent 50% of sales tax collections collected from the TIF districts. The above amounts have been remitted to the TIF developers and represent date paid to the developer and not the date collected from the state.**

CITY OF JOPLIN
TOTAL USE TAX COMPARISON
8-Apr-24

| MONTH | FY 2022 | FY 2022 Y-T-D | FY 2023 | FY 2023 Y-T-D | FY 2024 | FY 2024 Y-T-D | MONTHLY % CHANGE FROM FY 2023 | Y-T-D % CHANGE FROM FY 2023 |
|---|---|---|---|---|---|---|---|---|
| November | $ - | $ - | $ 429,310 | $ 429,310 | $ 402,700 | $ 402,700 | -6.2% | -6.2% |
| December | $ - | $ - | $ 424,027 | $ 853,337 | $ 595,155 | $ 997,856 | 40.4% | 16.9% |
| January | $ - | $ - | $ 314,605 | $1,167,942 | $ 505,044 | $1,502,900 | 60.5% | 28.7% |
| February | $ - | $ - | $ 530,679 | $1,698,621 | $ 694,536 | $2,197,436 | 30.9% | 29.4% |
| March | $ 92,787 | $ 92,787 | $ 443,132 | $2,141,753 | $ 526,522 | $2,723,958 | 18.8% | 27.2% |
| April | $ 171,530 | $ 264,317 | $ 394,395 | $2,536,148 | $ 623,222 | $3,347,180 | 58.0% | 32.0% |
| May | $ 433,065 | $ 697,382 | $ 340,376 | $2,876,524 | | | | |
| June | $ 323,803 | $1,021,185 | $ 364,178 | $3,240,702 | | | | |
| July | $ 279,350 | $1,300,535 | $ 508,888 | $3,749,590 | | | | |
| August | $ 600,073 | $1,900,608 | $ 802,615 | $4,552,206 | | | | |
| September | $ 419,693 | $2,320,301 | $ 467,084 | $5,019,290 | | | | |
| October | $ 311,492 | $2,631,793 | $ 497,430 | $5,516,720 | | | | |
| YTD Totals | $2,631,793 | $2,631,793 | $5,516,720 | $5,516,720 | $3,347,180 | $3,347,180 | | 32.0% |
| **Annual % Change** | | | | | | | | |

CITY OF JOPLIN
USE TAX COLLECTIONS SUMMARY
8-Apr-24

| MONTH COLLECTED | MONTH OF SALES | GENERAL-1% | PUBLIC SAFETY-1/2% | PENSION 1/2% | PARKS & SW-1/4% | TST-1/2% | CIP-3/8% | GRAND TOTAL |
|---|---|---|---|---|---|---|---|---|
| March-22 | Jan-22 | 29,692 | 14,846 | 14,846 | 7,423 | 14,846 | 11,134 | 92,787 |
| Apr-22 | Feb-22 | 54,890 | 27,445 | 27,445 | 13,722 | 27,445 | 20,584 | 171,530 |
| May-22 | Mar-22 | 138,581 | 69,290 | 69,290 | 34,645 | 69,290 | 51,968 | 433,065 |
| Jun-22 | Apr-22 | 103,617 | 51,808 | 51,808 | 25,904 | 51,808 | 38,856 | 323,803 |
| Jul-22 | May-22 | 89,392 | 44,696 | 44,696 | 22,348 | 44,696 | 33,522 | 279,350 |
| Aug-22 | Jun-22 | 192,023 | 96,012 | 96,012 | 48,006 | 96,012 | 72,009 | 600,073 |
| Sep-22 | Jul-22 | 134,302 | 67,151 | 67,151 | 33,575 | 67,151 | 50,363 | 419,693 |
| Oct-22 | Aug-22 | 99,677 | 49,839 | 49,839 | 24,919 | 49,839 | 37,379 | 311,492 |
| **FY 2022 TOTAL** | | **842,174** | **421,087** | **421,087** | **210,543** | **421,087** | **315,815** | **2,631,793** |
| Nov-22 | Sep-22 | 137,379 | 68,690 | 68,690 | 34,345 | 68,690 | 51,517 | 429,310 |
| Dec-22 | Oct-22 | 135,689 | 67,844 | 67,844 | 33,922 | 67,844 | 50,883 | 424,027 |
| Jan-23 | Nov-22 | 100,674 | 50,337 | 50,337 | 25,168 | 50,337 | 37,753 | 314,606 |
| Feb-23 | Dec-22 | 169,817 | 84,909 | 84,909 | 42,454 | 84,909 | 63,682 | 530,679 |
| Mar-23 | Jan-23 | 141,802 | 70,901 | 70,901 | 35,451 | 70,901 | 53,176 | 443,132 |
| Apr-23 | Feb-23 | 126,206 | 63,103 | 63,103 | 31,552 | 63,103 | 47,327 | 394,395 |
| May-23 | Mar-23 | 108,920 | 54,460 | 54,460 | 27,230 | 54,460 | 40,845 | 340,375 |
| Jun-23 | Apr-23 | 116,537 | 58,269 | 58,269 | 29,134 | 58,269 | 43,701 | 364,178 |
| Jul-23 | May-23 | 162,844 | 81,422 | 81,422 | 40,711 | 81,422 | 61,067 | 508,888 |
| Aug-23 | Jun-23 | 256,837 | 128,418 | 128,418 | 64,209 | 128,418 | 96,314 | 802,615 |
| Sep-23 | Jul-23 | 149,467 | 74,733 | 74,733 | 37,367 | 74,733 | 56,050 | 467,084 |
| Oct-23 | Aug-23 | 159,178 | 79,589 | 79,589 | 39,794 | 79,589 | 59,692 | 497,430 |
| **FY 2023 TOTAL** | | **1,765,351** | **882,675** | **882,675** | **441,337** | **882,675** | **662,007** | **5,516,719** |

CITY OF JOPLIN
USE TAX COLLECTIONS SUMMARY
8-Apr-24

| MONTH COLLECTED | MONTH OF SALES | GENERAL-1% | PUBLIC SAFETY-1/2% | PENSION 1/2% | PARKS & SW-1/4% | TST-1/2% | CIP-3/8% | GRAND TOTAL |
|---|---|---|---|---|---|---|---|---|
| Nov-23 | Sep-23 | 128,864 | 64,432 | 64,432 | 32,216 | 64,432 | 48,324 | 402,700 |
| Dec-23 | Oct-23 | 190,450 | 95,225 | 95,225 | 47,612 | 95,225 | 71,419 | 595,155 |
| Jan-24 | Nov-23 | 161,614 | 80,807 | 80,807 | 40,404 | 80,807 | 60,605 | 505,044 |
| Feb-24 | Dec-23 | 222,252 | 111,126 | 111,126 | 55,563 | 111,126 | 83,344 | 694,536 |
| Mar-24 | Jan-24 | 168,487 | 84,243 | 84,243 | 42,122 | 84,243 | 63,183 | 526,522 |
| Apr-24 | Feb-24 | 199,431 | 99,716 | 99,716 | 49,858 | 99,716 | 74,787 | 623,222 |
| May-24 | Mar-24 | - | - | - | - | - | - | - |
| Jun-24 | Apr-24 | - | - | - | - | - | - | - |
| Jul-24 | May-24 | - | - | - | - | - | - | - |
| Aug-24 | Jun-24 | - | - | - | - | - | - | - |
| Sep-24 | Jul-24 | - | - | - | - | - | - | - |
| Oct-24 | Aug-24 | - | - | - | - | - | - | - |
| **FY 2024 TOTAL** | | **1,071,097** | **535,549** | **535,549** | **267,775** | **535,549** | **401,661** | **3,347,180** |
| **LIFE-TO-DATE TOTAL** | | **3,678,622** | **1,839,310** | **1,839,310** | **919,655** | **1,839,310** | **1,379,484** | **11,495,692** |

# Executive Maturity Summary Report

Prepared for City of Joplin

April 2024

# Progress on Initiative

## Recap of Previous Quarters Initiatives

- Incident Response Plan Documented
- 35 Laptop Computers and Supplies
- Policies Formally Approved
  - Acceptable Use
  - Password
  - Antivirus
  - Training and Awareness

# Incident Response Plan (Page 1)

## City of Joplin Incident Response Plan

### 1. INTRODUCTION & OBJECTIVES

#### 1.1.Introduction

The Incident Response Plan (IRP) is designed to provide a systematic approach to handling cybersecurity incidents effectively within the City of Joplin. It outlines the steps and responsibilities necessary to detect, respond to, and recover from security incidents.

[Provide a brief introduction to the incident response plan and its purpose.]

#### 1.2.Objectives

- Minimize downtime and service disruptions.
- Safeguard sensitive data and company information.
- Ensure organization continuity during and after incidents.
- Identify the root cause of incidents and implement measures to prevent their recurrence.

[Define the main objectives of the plan, such as minimizing downtime, safeguarding customer data, and ensuring business continuity.]

### 2. INCIDENT RESPONSE TEAM

#### 2.1.Incident Response Team Members

- **IT Director (CISO)** – Mark A Morris, mmorris@joplinmo.org , +1 (417) 439-7877)
- **Security Operations Center (SOC) Manager** – RAVENii, LLC., support@raveniisupport.zendesk.com , +1 (844) 317-0944 or +1 (316)-655-8109
- **NW Administrator**- Lane Starchman, lstarchm@joplinmo.org +1 (417) 540-9941
- **Legal Counsel** – Peter Edwards, pedwards@joplinmo.org +1 (417) 624-0820 ext. 1225
- **PIO**– Lynn Onstot, lonstot@joplinmo.org , +1 (417) 624-0820 ext. 1204

[List key personnel involved in incident response and their roles. Include contact information for each member.]

| Insurance Contact(s) | Office | Mobile |
|---|---|---|
| (Name and Title) | | |
| | | |

#### 2.2.Roles and Responsibilities

# Incident Response Plan (Page 2)

Incident Response Team members are responsible for promptly reporting and responding to incidents within their respective areas of the organization.

**2.IT Director (CISO)**

**2.2.1.1. Definition**

The CISO is a senior-level executive responsible for overseeing the organization's information security and cybersecurity strategy.

**2.2.1.2. Responsibilities**

- Approve and maintain the Incident Response Plan (IRP).
- Ensure the IRP aligns with the organization's risk management and business continuity strategies.
- Declare and authorize the escalation of incidents to higher management levels when necessary.
- Coordinate with other senior executives to allocate necessary resources for incident response and recovery.
- Review incident reports and lead post-incident analysis to identify areas for improvement.

**2.Security Operations Center (SOC) Manager**

**2.2.2.1. Definition**

The SOC Manager is responsible for overseeing the day-to-day operations of the Security Operations Center, which monitors and responds to cybersecurity incidents.

**2.2.2.2. Responsibilities**

- Supervise the SOC team and ensure their readiness to respond to incidents promptly.
- Review and analyze security alerts and incidents.
- Determine the severity and impact of incidents and assign appropriate response actions.
- Ensure timely communication with the Incident Response Team and other stakeholders during incidents.
- Oversee the collection and preservation of digital evidence during investigations.

**2.Network Administrator**

**2.2.3.1. Definition**

The NW Administrator is responsible for the overall management of the organization's IT infrastructure and systems.

**2.2.3.2. Responsibilities**

- Collaborate with the Incident Response Team to implement incident containment and eradication actions.

RAVENii
CYBER SECURITY

# Incident Response Plan (Page 3)

- Coordinate system recovery efforts and verify the restoration of services to normal operation.
- Implement measures to prevent similar incidents from occurring in the future.
- Ensure that system backups are regularly performed and securely stored.

**2.Legal Counsel**

**2.2.4.1. Definition**

Legal Counsel refers to an attorney or legal representative with expertise in cybersecurity and data privacy.

**2.2.4.2. Responsibilities**

- Advise the Incident Response Team on legal implications and regulatory requirements related to incidents.
- Determine if incidents warrant reporting to law enforcement or regulatory bodies.
- Assist in evaluating potential legal liabilities and risks associated with incidents.
- Review incident-related communications before they are released externally.

**2.PIO-Public Information Officer**

**2.2.5.1. Definition**

The PIO-Public Information Officer oversees the organization's public relations and external communications.

**2.2.5.2. Responsibilities**

- Coordinate external communications during and after incidents to maintain transparency with citizens, partners, and the public.
- Craft clear and consistent incident-related messages for various stakeholders.
- Work with Legal Counsel to ensure compliance with data breach notification laws and regulations.
- Monitor media coverage and manage the organization's reputation during incidents.

[Define the responsibilities of different teams and individuals during incident response.]
[Clarify decision-making authority and delegation of tasks.]

## 3. INCIDENT CLASSIFICATION & SEVERITY LEVELS

**3.1. Incident Categories**

- Unauthorized Access

RAVENii CYBER SECURITY

# Incident Response Plan (Page 4)

- Malware and Ransomware
- Denial of Service (DoS) or Distributed Denial of Service (DDoS)
- Data Breach
- Insider Threat

3.2. **Physical Security Incident Severity Levels**

- Low: Incidents with minimal impact on services or data.
- Medium: Incidents with moderate impact on services or data.

**3.3.Incident Impact Matrix**

| Impact Category | Description |
|---|---|
| High | - A large number of staff/users/citizens are affected. - Hefty Financial impact, causing considerable damage to the operation of the company or its clients |
| Moderate | - A moderate number of staff/users/citizens are affected. - Considerable financial impact. - Caused moderate damage to company operation or business reputation |
| Low | - A small number of staff/users/citizens are affected. - Minimal financial impact - Caused minimal damage to company operations or business reputation |

3.4. **Urgency of Incident Matrix**

| Urgency Category | Description |
|---|---|
| High | - The damage caused by the incident is rapidly increasing - Users are unable to use the services properly - The staff cannot perform highly time-sensitive work - A minor incident that can become a major incident if not resolved immediately - A minor incident that can be resolved without investing much time or many resources |

RAVENii
CYBER SECURITY

# Incident Response Plan (Page 5)

| | |
|---|---|
| Moderate | - The damage caused by the incident is increasing considerably - A small number of staff/users/citizens are affected |
| Low | - The damage caused by the incident increased marginally over time - A handful of staff/users/citizens are affected - The resources required may be difficult to procure compared to other priorities |

**3.5. Incident Priority Levels**

| Priority Level | Description | Target Response Time |
|---|---|---|
| 1 | Critical | Immediate |
| 2 | High | 10 Minutes |
| 3 | Medium | 1 Hour |
| 4 | Low | 24 Hours |
| 5 | Very Low | Up to 7 Days |

[Define the different incident categories and their corresponding severity levels. Specify the criteria for classifying incidents based on impact and urgency.]

## 4. INCIDENT REPORTING & DOCUMENTATION

**4.1.Incident Reporting**

4.Employees should report suspected or confirmed incidents to the IT department or the designated Incident Response Team contact.

4.Incident reports are to be validated by way of a preliminary review to confirm relevancy.

4.The Incident Response Team contact information shall be prominently displayed in employee training materials and on the company's intranet.

4.If an employee is unable to reach the designated contact, they should escalate to their immediate supervisor or manager.

**4.2.Incident Documentation**

4.Upon detection, the Incident Response Team shall create an incident report detailing the date, time, and nature of the incident.

4.All actions taken during incident response, including containment, eradication, and recovery, shall be thoroughly documented.

4.Preserve digital evidence and document the chain of custody to maintain the integrity of evidence for potential legal proceedings.

[Explain the process for reporting incidents and documenting relevant details.]

RAVENii CYBER SECURITY

# Incident Response Plan (Page 6)

[Specify the tools or systems to be used for incident tracking and documentation.]

## 5. INCIDENT RESPONSE PROCEDURES

### 5.1. Logging

Logging of information is critical in situations that may eventually involve federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for all security incidents that are under investigation. The information should be logged in a location that cannot be altered by others. Manually written logs are preferable since on-line logs can be altered or deleted. The types of information that should be logged are:

- Dates and times of incident-related phone calls.
- Dates and times when incident-related events were discovered or occurred.
- Amount of time spent working on incident-related tasks.
- People you have contacted or have contacted you.
- Names of systems, programs or networks that have been affected.

### 5.2. Incident Detection and Assessment

Incident detection is completed through SIEM alerts, intrusion detection systems, and employee reporting. Assess the nature and scope of the incident promptly upon detection.

[Outline the process for identifying and detecting potential incidents.]
[Describe how incidents will be assessed to determine their severity and impact.]

### 5.3. Identify Critical Systems

Critical systems are those that are vital to the organization's operations and the protection of sensitive data. The IT department, in collaboration with business units, shall identify and prioritize critical systems.

[Identification of critical systems should be based on an in-depth risk assessment and business impact analysis.]

### 5.4. Incident Declaration

The CISO or the designated Incident Response Team leader has the authority to declare an incident based on its severity and impact. Once declared, the Incident Response Plan shall be activated immediately.

[Outline the declaration process including the threshold criteria.]

### 5.5. Escalation Process

If an incident exceeds the Incident Response Team's ability to handle it effectively, it shall be escalated to the CISO. The CISO shall assess the situation and determine

RAVENii CYBER SECURITY

# Incident Response Plan (Page 7)

whether further escalation is required, such as involving executive management, legal counsel, or government agencies.

[Outline the process for escalating incidents to higher management levels when necessary.]
[Specify communication channels and the criteria for escalating incidents.]

## 6. INCIDENT RESPONSE PHASES

### 6.1.Incident Containment

- Isolate affected systems and networks to prevent further spread.
- Review other potential targets to determine the magnitude of the incident.
- The NW Administrator and the SOC Manager shall work together to isolate affected systems from the network to prevent further spread of the incident.
- Quarantine infected devices and disconnect them from the network until they are deemed safe for reconnection.

[Provide step-by-step instructions for containing and containing incidents.]

### 6.2.Incident Eradication

- Conduct a thorough investigation to identify the root cause of the incident.
- Analyze the evidence collected during the incident response process to determine how the incident occurred and how it spread through the network.
- If the incident involves malware or malicious software, deploy antivirus and antimalware tools to identify and remove the malicious code from affected systems.
- Cleanse the systems to ensure there are no remnants of the malware left behind.
- Identify any vulnerabilities that were exploited to carry out the incident.
- Apply appropriate patches or security updates to fix these vulnerabilities in affected systems and prevent future exploitation.
- Review and modify access controls and user privileges to prevent unauthorized access to critical systems and data.
- Implement the principle of least privilege to limit user access to only what is necessary for their roles.
- Reset passwords for compromised accounts and enforce stronger password policies.
- If the incident involved lateral movement across the network, review and enhance network segmentation to isolate critical systems and limit the potential spread of future incidents.
- Verify the integrity of critical system files and configurations to ensure they have not been tampered with during the incident.
- Consider using file integrity monitoring tools to detect unauthorized changes in real-time.
- Conduct thorough testing and verification to ensure that the incident has been completely eradicated.

RAVENii
CYBER SECURITY

# Incident Response Plan (Page 8)

- Validate that the affected systems are functioning as expected and without any abnormalities.
- Implement continuous monitoring and intrusion detection measures to promptly detect and respond to any signs of recurring or new incidents.

[Provide step-by-step instructions for containing and eradicating incidents.]

**6.3.Incident Recovery**

- Prioritize the recovery of critical systems and data based on the organization's business impact analysis and the results of the post-incident assessment.
- Develop a detailed recovery plan with specific tasks, timelines, and responsible parties for each critical system or service, that details when recovery should be initiated.
- Restore data from backups to affected systems, ensuring the integrity and security of the data.
- Verify the validity of backups and perform data consistency checks.
- Rebuild affected systems using clean images or configurations from trusted sources.
- Apply all necessary security patches and updates to ensure the systems are protected from known vulnerabilities.
- Verify that the configurations of recovered systems align with the organization's security standards.
- Perform vulnerability scans on recovered systems to identify any remaining vulnerabilities or potential attack vectors.
- Communicate with users and stakeholders about the progress of the recovery efforts.
- Inform them about any temporary changes in service availability or operational procedures during the recovery process.
- Implement continuous monitoring and additional security measures to ensure that recovered systems remain secure.
- Monitor for any signs of recurring incidents or potential indicators of compromise.
- Gradually restore normal operations as systems are confirmed to be secure and fully functional.
- Continuously monitor systems and services after recovery to detect any anomalies or issues that may arise.

[Explain the procedures for recovering affected systems and data.]

**6.4.Evidence Handling**

6. Designate a qualified team member to handle evidence collection and preservation.
6. Use digital forensic tools to acquire and analyze evidence following chain-of-custody procedures to preserve the integrity of evidence thought the investigation process.

[Describe the process for collecting, preserving, and analyzing digital evidence.]
[Ensure compliance with legal and chain-of-custody requirements.]

RAVENii
CYBER SECURITY

# Incident Response Plan (Page 9)

A. **INCIDENT SPECIFIC PROCEDURES**
   a. This section discusses the procedure for handling virus, worm and hacker/cracker incidents.
   b. **VIRUS AND WORM INCIDENTS**
      i. Although virus and worm incidents are very different, the procedures for handling each are very similar aside from the initial isolation of the system and the time criticality. Viruses are not self-replicating and, thus, incidents of this nature are not as time critical as worm or hacker incidents. Worms are self-replicating and can spread to hundreds of machines in a matter of minutes, thus, time is a critical factor when dealing with a worm attack. If you are not sure of the type of attack, then proceed as if the attack was worm related.
      ii. **Isolate the System**
         1. Isolate infected system(s) from the remaining City of Joplin network as soon as possible. If a worm is suspected, then a decision must be made to disconnect the City of Joplin from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since the City of Joplin will be disconnected from sites which may have patches. The City of Joplin CISO must authorize the isolation of the network from the outside world.

      iii. **Log all actions.**
         1. Do not power off or reboot systems that may be infected. There are some viruses that will destroy disk data if the system is power-cycled or rebooted. Also, rebooting a system could destroy needed information or evidence.
      iv. **Notify Appropriate People**

B. Notify the City of Joplin SOC Manager as soon as possible. If unable to reach him/her within 10 minutes, contact the backup person. The City of Joplin SOC Manager will then be responsible for notifying other appropriate personnel. *** **NOTE** - Below, different times are given for suspected worm attack and for a suspected virus attack.

C. - The City of Joplin NW Administrator or SOC Manager will notify the City of Joplin CISO within two hours (one hour for a worm attack). The City of Joplin CISO will escalate to higher level management if necessary.

D. - The control room or City of Joplin SOC Manager should notify all involved LSAs within four hours (two hours for a worm attack).
      i. **Identify the Problem**
         1. Try to identify and isolate the suspected virus or worm-related files and processes. Prior to removing any files or killing any processes, a snapshot

RAVENii CYBER SECURITY

# Incident Response Plan (Page 17)

1. Regularly review logs, access logs, and audit trails to identify any suspicious activity, unauthorized access, or data modifications.

v. *Response*

vi. **Containment**
   1. Quickly contain the breach by isolating affected systems and revoking unauthorized access.
   2. Limit lateral movement of attackers within the network to prevent further damage.

vii. **Investigation**
   1. Conduct a thorough investigation to determine the extent of the data breach. Identify what data was accessed, how it was accessed, and who was responsible.
   2. Assess the potential damage and impact of the breach.

viii. **Vulnerability Patching**
   1. Identify and patch the vulnerabilities that allowed the breach to occur in the first place.
   2. Implement security enhancements, such as multi-factor authentication and encryption, to improve data protection.

ix. **Communication**
   1. Notify affected citizens and regulatory authorities as per data breach notification laws. Provide detailed information about the breach, its scope, and the steps taken for remediation.
   2. Maintain open communication channels with affected parties.

x. **Legal Cooperation**
   1. Cooperate with law enforcement agencies to support potential investigations and evidence collection.
   2. Preserve evidence and logs for legal and regulatory purposes.

xi. **Security Enhancement**
   1. Enhance security controls, including access controls, network segmentation, and data encryption, to prevent future data breaches.

## 7. COMMUNICATION & NOTIFICATION

### 7.1.Internal Communication

7.1.1.1. Incident Response Team members shall communicate through a dedicated incident response channel on the company's collaboration platform, Microsoft TEAMS.

7.1.1.2. Escalate incidents to higher management levels as per the predefined escalation process.

[Specify how incidents will be reported within the organization.]

RAVENii
CYBER SECURITY

# Incident Response Plan (Page 18)

[Define the communication channels and stakeholders to be informed.]

7.2. **External Communication**

7.2.1.1. Notify citizens, partners, and regulatory authorities in accordance with legal requirements and data breach notification laws.

7.2.1.2. Communications shall be coordinated by the Communications Manager.

[Outline the process for notifying relevant external parties, such as citizens, partners, and regulatory authorities.]
[Ensure consistent and timely communication.]

## 8. TRAINING & AWARENESS

8.1. All employees shall receive regular cybersecurity awareness training to recognize and report potential security incidents. The Incident Response Team shall conduct simulated incident response exercises at least once a year to test the organization's preparedness and identify areas for improvement.

[Detail the importance of regular training for employees on incident response procedures.] [Consider conducting simulated exercises to test the effectiveness of the plan.]

## 9. CONTINUOUS IMPROVEMENT

9.1. The Incident Response Team shall conduct post-incident reviews to evaluate the root cause, identify lessons learned, and overall effectiveness of the response. Based on the review findings, updates to the Incident Response Plan and related processes shall be made to enhance incident response capabilities.

[Describe how the incident response plan will be regularly reviewed, updated, and tested.] [Define metrics for evaluating the plan's effectiveness and making necessary improvements.]

## 10. LEGAL REGULATORY CONCIDERATIONS

10.1. Legal Counsel shall be responsible for staying up to date with relevant cybersecurity laws and regulations. The Incident Response Team shall collaborate with Legal Counsel to ensure compliance with data breach notification laws and other legal requirements.

[Address any legal or regulatory requirements specific to your organization's industry.]
[Ensure compliance with data protection and privacy regulations.]

## 11. PLAN DISTRIBUTION

RAVENii
CYBER SECURITY

# (March) Security Operations Center Report – Vulnerability Management

## Mitigation Summary – Vulnerabilities by Severity

| | Total Mitigated | Mitigated <10d | Mitigated 10-30d | Mitigated >30d | Total Unmitigated | Exploitable | Patch Available >30d | Exploitable Hosts |
|---|---|---|---|---|---|---|---|---|
| Total Vulnerabilties | 1,039 | 57% | 30% | 13% | 2,723 | 16% | 34% | 277 |
| Critical | 16 | 38% | 0% | 63% | 192 | 24% | 85% | 12 |
| High | 228 | 63% | 32% | 5% | 582 | 23% | 45% | 75 |
| Medium | 748 | 57% | 30% | 13% | 1,700 | 15% | 20% | 230 |
| Low | 47 | 34% | 34% | 32% | 249 | 5% | 0% | 13 |

- Total Vulnerabilities Mitigated this month: 27.62%, down 14.81% from last month.
- Critical Vulnerabilities Mitigated this month: 7.69%, up 0.75% from last month.
- High Vulnerabilities Mitigated this month: 28.15%, down 6.31% from last month.
- Medium Vulnerabilities Mitigated this month: 30.56%, down 19.18% from last month.
- Low Vulnerabilities Mitigated this month: 15.88%, down 9.83% from last month.

IPs scanned: 874

RAVENii
CYBER SECURITY

# (April) Security Operations Center Report – Vulnerability Management

## Mitigation Summary – Vulnerabilities by Severity

| | Total Mitigated | Mitigated <10d | Mitigated 10-30d | Mitigated >30d | Total Unmitigated | Exploitable | Patch Available >30d | Exploitable Hosts |
|---|---|---|---|---|---|---|---|---|
| Total Vulnerabilities | 1,087 | 59% | 27% | 15% | 1,971 | 17% | 21% | 266 |
| Critical | 17 | 35% | 0% | 65% | 54 | 9% | 100% | 5 |
| High | 249 | 62% | 27% | 11% | 314 | 27% | 23% | 61 |
| Medium | 771 | 59% | 27% | 13% | 1,418 | 17% | 20% | 222 |
| Low | 50 | 38% | 28% | 34% | 185 | 3% | 0% | 6 |

- Total Vulnerabilities Mitigated this month: 35.55%, up 7.93% from last month.
- Critical Vulnerabilities Mitigated this month: 23.94%, up 16.25% from last month.
- High Vulnerabilities Mitigated this month: 44.23%, up 16.08% from last month.
- Medium Vulnerabilities Mitigated this month: 35.22%, up 4.66% from last month.
- Low Vulnerabilities Mitigated this month: 21.28%, up 5.40% from last month.

IPs scanned: 812

RAVENii
CYBER SECURITY

# Security Operations Center Report – Vulnerability Management

## Risk Reduction Recommendations (VPR: 5-10)

| Solution | Risk R... | Hosts A... | Vulnera... | CVEs | MS |
|---|---|---|---|---|---|
| Contact the vendor or consult product documentation to disable CBC mode cipher en... | 4.90% | 17 | 17 | 51 | 0 |
| Contact the vendor for an update with the strict key exchange countermeasures or di... | 3.11% | 26 | 36 | 54 | 0 |
| Upgrade to VMware vCenter Server 7.0U3o, or 8.0U2 or later. | 2.31% | 1 | 2 | 6 | 0 |
| Upgrade to IBM Spectrum Protect 8.1.15.000 or later. | 2.31% | 2 | 2 | 4 | 0 |
| Update to Dropbear version 2016.74.0 or later. | 1.15% | 1 | 1 | 4 | 0 |
| Apply updates in accordance with the vendor advisory. | 1.15% | 1 | 1 | 1 | 0 |
| Fix Netatalk OpenSession Remote Code Execution | 1.15% | 1 | 1 | 1 | 0 |
| Upgrade to JQuery version 3.5.0 or later. | 0.52% | 3 | 6 | 6 | 0 |
| Fix SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) | 0.17% | 6 | 6 | 6 | 0 |

RAVENii
CYBER SECURITY

# Firewall Management

## Joplin SonicWall

## Registered January 14 2022-2024

## SonicOS 7.0.1-5119 - (Current)

TOP APPLICATIONS BY TOTAL DATA TRANSFERRED

| APPLICATIONS NAME | TOTAL DATA TRANSFERR... | PERCENTAGE |
|---|---|---|
| SSL/TLS Protocol | 12.62 TB | 45.65% |
| Encrypted Key Exchange | 3.82 TB | 13.9% |
| Netflix | 1.05 TB | 3.79% |
| Windows Update Delivery Optimiz... | 0.92 TB | 3.31% |
| Unknown | 797.03 GB | 2.79% |
| Apple Inc | 635.34 GB | 2.24% |
| TikTok | 563.95 GB | 1.99% |
| Microsoft Office 365 | 459.20 GB | 1.62% |
| Outlook.com (Hotmail) | 350.93 GB | 1.24% |
| Adobe | 239.46 GB | 0.84% |

TOP INTRUSIONS BY BLOCKED

| INTRUSIONS NAME | BLOCKED | PERCENTAGE |
|---|---|---|
| HTTPS Response with Punycode String | 17.54K | 45.54% |
| Absolute Computrace Server Response | 11.24K | 29.19% |
| Squid DNS Replies Memory Corruption 1 | 9.01K | 23.4% |
| SSLv2.0 Client Hello 2 | 554 | 1.44% |
| OpenSSL Heartbeat 1 | 115 | 0.3% |
| SSLv2.0 Client Hello | 36 | 0.09% |
| Web Robots Activity 2 | 14 | 0.04% |
| VML File Download (HTTP) 4 | 4 | 0.01% |
| Obfuscated VBScript/JavaScript Code 11 | 2 | 0.01% |
| Obfuscated VBScript/JavaScript Code 27 | 2 | 0.01% |

TOP BLOCKED BY CONNECTIONS

| BLOCKED NAME | CONNECTIONS | PERCENTAGE |
|---|---|---|
| Firewall Rule | 749.31M | 99.4% |
| Geo-IP Filter | 4.24M | 0.56% |
| Content Filter | 244.14K | 0.03% |
| Threat | 49.05K | 0.01% |
| Botnet Filter | 106 | 0% |

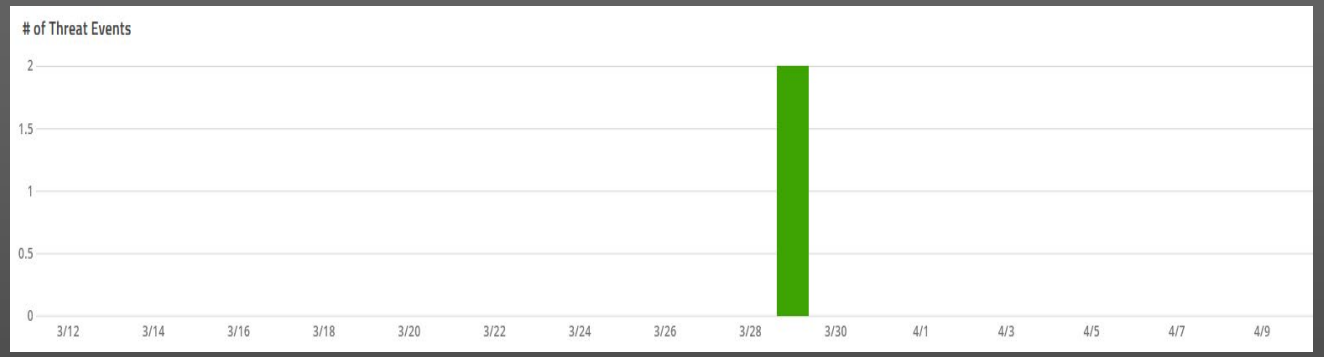
RAVENii CYBER SECURITY

# Endpoint

## Possible threats found last 30 days : 2 (pups)

- 2 trash chrome files

## Endpoint Status




- Installed on 479 devices
- Secondary policy in place for memory actions that are too aggressive

Total Files Analyzed
91,990,106

RAVENii
CYBER SECURITY

# Backup

## Jobs Operating Normally

Storage Capacity
Joplin: 98 TB
Error with SVR-NETMOTION
SVR-PSJAPP missing

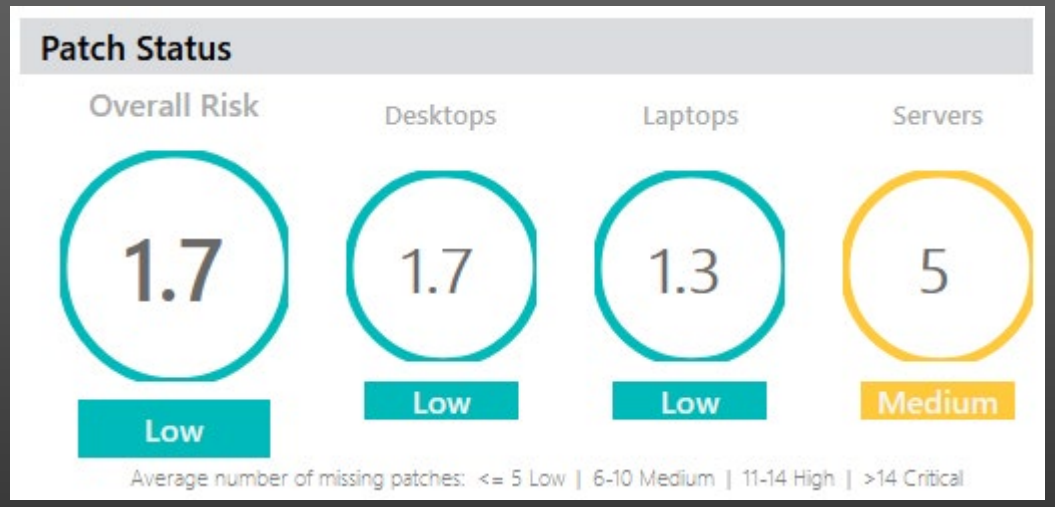



| OS | Computer Name ↑ | April, | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | JOPLINVIDEO-NEW<br>Joplin * jsupport | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Files Backup Plan JoplinVideo-new | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | → | ✓ | ✓ | ✓ | ◷ | | | | |
| | SVR-BLUETEAM<br>Joplin * jsupport | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Backup Image Based / System State | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◷ | | | | |
| | SVR-COURTNEW<br>Joplin * jsupport | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Backup Image Based / System State | | | ✓ | | | | ✓ | | | ✓ | | | | ◷ | |
| | Consistency check plan for Joplin Backups | | | | | | | | | | | | | | | |
| | CourtFiles | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◷ | | | | |
| | SVR-FIREHOUSE<br>Joplin * jsupport | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Firehouse | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◷ | | | | |
| | SVR-INTEGRA2<br>Joplin * jsupport | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Consistency check plan for Joplin Backups | | | | | | | | | | | | | | | |
| | Svr-Integra2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◷ | | | | |
| | SVR-NETMOTION<br>Joplin * jsupport | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Backup VMware on 11/1/2021 10:07:15 AM | | | | | | ✗ | ✗ | | | | | | | ◷ | |
| | SVR-ROUTEMATCH<br>Joplin * jsupport | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Routematch | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◷ | | | | |
| | SVR-WEBGIS<br>Joplin * jsupport | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Files Backup plan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◷ | | | | |
| | Svr-webgis(Files) legacy | | | | | | | | | | | | | | | |

– Deleted – Failed – Missed Run – Warning – Running – Success – Scheduled

# Patching

March-April




Device Count:
  - Currently at 438
- A device scan for patches was setup on weekly basis
- Non Critical servers are restarting middle of the night (Friday-Saturday)
- Patches are approved once investigated as they come out.
  - restart window for endpoints set as well (after 10pm)

- 67 devices offline

RAVENii
CYBER SECURITY

# Current Initiatives

## Initiatives In Progress

- Sandbox Server
- Admin Level Multi-Factor Authentication
- In-Person Training
    - Policy Review with Employee Groups
- Continued Patching/Backups
- Continued Network/Dark Web Monitoring
- Continued Endpoint Management

JOPLIN
MISSOURI

# Thank You for Your Attention!

RAVENii
CYBER SECURITY

Powered by
MixMode

# City of Joplin Incident Response Plan

## 1. INTRODUCTION & OBJECTIVES

### 1.1. Introduction

The Incident Response Plan (IRP) is designed to provide a systematic approach to handling cybersecurity incidents effectively within the City of Joplin. It outlines the steps and responsibilities necessary to detect, respond to, and recover from security incidents.

[Provide a brief introduction to the incident response plan and its purpose.]

### 1.2. Objectives

- Minimize downtime and service disruptions.
- Safeguard sensitive data and company information.
- Ensure organization continuity during and after incidents.
- Identify the root cause of incidents and implement measures to prevent their recurrence.

[Define the main objectives of the plan, such as minimizing downtime, safeguarding customer data, and ensuring business continuity.]

## 2. INCIDENT RESPONSE TEAM

### 2.1. Incident Response Team Members

- **IT Director (CISO)** – Mark A Morris, mmorris@joplinmo.org , +1 (417) 439-7877)
- **Security Operations Center (SOC) Manager** – RAVENii, LLC., support@raveniisupport.zendesk.com , +1 (844) 317-0944 or +1 (316)-655-8109
- **NW Administrator**- Lane Starchman, lstarchm@joplinmo.org +1 (417) 540-9941
- **Legal Counsel** – Peter Edwards, pedwards@joplinmo.org +1 (417) 624-0820 ext. 1225
- **PIO**– Lynn Onstot, lonstot@joplinmo.org , +1 (417) 624-0820 ext. 1204

[List key personnel involved in incident response and their roles. Include contact information for each member.]

| **Insurance Contact(s)** | **Office** | **Mobile** |
|---|---|---|
| **(Name and Title)** | | |
| | | |

### 2.2. Roles and Responsibilities

Incident Response Team members are responsible for promptly reporting and responding to incidents within their respective areas of the organization.

**2. IT Director (CISO)**

**2.2.1.1. Definition**

The CISO is a senior-level executive responsible for overseeing the organization's information security and cybersecurity strategy.

**2.2.1.2. Responsibilities**

- Approve and maintain the Incident Response Plan (IRP).
- Ensure the IRP aligns with the organization's risk management and business continuity strategies.
- Declare and authorize the escalation of incidents to higher management levels when necessary.
- Coordinate with other senior executives to allocate necessary resources for incident response and recovery.
- Review incident reports and lead post-incident analysis to identify areas for improvement.

**2. Security Operations Center (SOC) Manager**

**2.2.2.1. Definition**

The SOC Manager is responsible for overseeing the day-to-day operations of the Security Operations Center, which monitors and responds to cybersecurity incidents.

**2.2.2.2. Responsibilities**

- Supervise the SOC team and ensure their readiness to respond to incidents promptly.
- Review and analyze security alerts and incidents.
- Determine the severity and impact of incidents and assign appropriate response actions.
- Ensure timely communication with the Incident Response Team and other stakeholders during incidents.
- Oversee the collection and preservation of digital evidence during investigations.

**2. Network Administrator**

**2.2.3.1. Definition**

The NW Administrator is responsible for the overall management of the organization's IT infrastructure and systems.

**2.2.3.2. Responsibilities**

- Collaborate with the Incident Response Team to implement incident containment and eradication actions.
- Coordinate system recovery efforts and verify the restoration of services to normal operation.
- Implement measures to prevent similar incidents from occurring in the future.

- Ensure that system backups are regularly performed and securely stored.

**2. Legal Counsel**

**2.2.4.1. Definition**

Legal Counsel refers to an attorney or legal representative with expertise in cybersecurity and data privacy.

**2.2.4.2. Responsibilities**

- Advise the Incident Response Team on legal implications and regulatory requirements related to incidents.
- Determine if incidents warrant reporting to law enforcement or regulatory bodies.
- Assist in evaluating potential legal liabilities and risks associated with incidents.
- Review incident-related communications before they are released externally.

**2. PIO-Public Information Officer**

**2.2.5.1. Definition**

The PIO-Public Information Officer oversees the organization's public relations and external communications.

**2.2.5.2. Responsibilities**

- Coordinate external communications during and after incidents to maintain transparency with citizens, partners, and the public.
- Craft clear and consistent incident-related messages for various stakeholders.
- Work with Legal Counsel to ensure compliance with data breach notification laws and regulations.
- Monitor media coverage and manage the organization's reputation during incidents.

[Define the responsibilities of different teams and individuals during incident response.]
[Clarify decision-making authority and delegation of tasks.]

# 3. INCIDENT CLASSIFICATION & SEVERITY LEVELS

**3.1. Incident Categories**

- Unauthorized Access
- Malware and Ransomware
- Denial of Service (DoS) or Distributed Denial of Service (DDoS)
- Data Breach
- Insider Threat

3.2. **Physical Security Incident Severity Levels**

- Low: Incidents with minimal impact on services or data.
- Medium: Incidents with moderate impact on services or data.

### 3.3. Incident Impact Matrix

| Impact Category | Description |
|---|---|
| High | - A large number of staff/users/citizens are affected. - Hefty Financial impact, causing considerable damage to the operation of the company or its clients |
| Moderate | - A moderate number of staff/users/citizens are affected. - Considerable financial impact. - Caused moderate damage to company operation or business reputation |
| Low | - A small number of staff/users/citizens are affected. - Minimal financial impact - Caused minimal damage to company operations or business reputation |

### 3.4. Urgency of Incident Matrix

| Urgency Category | Description |
|---|---|
| High | - The damage caused by the incident is rapidly increasing - Users are unable to use the services properly - The staff cannot perform highly time-sensitive work - A minor incident that can become a major incident if not resolved immediately - A minor incident that can be resolved without investing much time or many resources |
| Moderate | - The damage caused by the incident is increasing considerably - A small number of staff/users/citizens are affected |
| Low | - The damage caused by the incident increased marginally over time - A handful of staff/users/citizens are affected - The resources required may be difficult to procure compared to other priorities |

| | |
|---|---|
| | |

### 3.5. Incident Priority Levels

| Priority Level | Description | Target Response Time |
|---|---|---|
| 1 | Critical | Immediate |
| 2 | High | 10 Minutes |
| 3 | Medium | 1 Hour |
| 4 | Low | 24 Hours |
| 5 | Very Low | Up to 7 Days |

[Define the different incident categories and their corresponding severity levels. Specify the criteria for classifying incidents based on impact and urgency.]

# 4. INCIDENT REPORTING & DOCUMENTATION

### 4.1. Incident Reporting

4. Employees should report suspected or confirmed incidents to the IT department or the designated Incident Response Team contact.
4. Incident reports are to be validated by way of a preliminary review to confirm relevancy.
4. The Incident Response Team contact information shall be prominently displayed in employee training materials and on the company's intranet.
4. If an employee is unable to reach the designated contact, they should escalate to their immediate supervisor or manager.

### 4.2. Incident Documentation

4. Upon detection, the Incident Response Team shall create an incident report detailing the date, time, and nature of the incident.
4. All actions taken during incident response, including containment, eradication, and recovery, shall be thoroughly documented.
4. Preserve digital evidence and document the chain of custody to maintain the integrity of evidence for potential legal proceedings.

[Explain the process for reporting incidents and documenting relevant details.]
[Specify the tools or systems to be used for incident tracking and documentation.]

# 5. INCIDENT RESPONSE PROCEDURES

### 5.1. Logging

Logging of information is critical in situations that may eventually involve federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for all security incidents that are under investigation. The information should be logged in a location that cannot be altered by others. Manually written logs are preferable since on-line logs can be altered or deleted. The types of information that should be logged are:

- Dates and times of incident-related phone calls.
- Dates and times when incident-related events were discovered or occurred.
- Amount of time spent working on incident-related tasks.
- People you have contacted or have contacted you.
- Names of systems, programs or networks that have been affected.

### 5.2. Incident Detection and Assessment

Incident detection is completed through SIEM alerts, intrusion detection systems, and employee reporting. Assess the nature and scope of the incident promptly upon detection.

[Outline the process for identifying and detecting potential incidents.]
[Describe how incidents will be assessed to determine their severity and impact.]

### 5.3. Identify Critical Systems

Critical systems are those that are vital to the organization's operations and the protection of sensitive data. The IT department, in collaboration with business units, shall identify and prioritize critical systems.

[Identification of critical systems should be based on an in-depth risk assessment and business impact analysis.]

### 5.4. Incident Declaration

The CISO or the designated Incident Response Team leader has the authority to declare an incident based on its severity and impact. Once declared, the Incident Response Plan shall be activated immediately.

[Outline the declaration process including the threshold criteria.]

### 5.5. Escalation Process

If an incident exceeds the Incident Response Team's ability to handle it effectively, it shall be escalated to the CISO. The CISO shall assess the situation and determine whether further escalation is required, such as involving executive management, legal counsel, or government agencies.

[Outline the process for escalating incidents to higher management levels when necessary.]
[Specify communication channels and the criteria for escalating incidents.]

## 6. INCIDENT RESPONSE PHASES

### 6.1. Incident Containment

- Isolate affected systems and networks to prevent further spread.
- Review other potential targets to determine the magnitude of the incident.
- The NW Administrator and the SOC Manager shall work together to isolate affected systems from the network to prevent further spread of the incident.
- Quarantine infected devices and disconnect them from the network until they are deemed safe for reconnection.

[Provide step-by-step instructions for containing and containing incidents.]

### 6.2. Incident Eradication

- Conduct a thorough investigation to identify the root cause of the incident.
- Analyze the evidence collected during the incident response process to determine how the incident occurred and how it spread through the network.
- If the incident involves malware or malicious software, deploy antivirus and antimalware tools to identify and remove the malicious code from affected systems.
- Cleanse the systems to ensure there are no remnants of the malware left behind.
- Identify any vulnerabilities that were exploited to carry out the incident.
- Apply appropriate patches or security updates to fix these vulnerabilities in affected systems and prevent future exploitation.
- Review and modify access controls and user privileges to prevent unauthorized access to critical systems and data.
- Implement the principle of least privilege to limit user access to only what is necessary for their roles.
- Reset passwords for compromised accounts and enforce stronger password policies.
- If the incident involved lateral movement across the network, review and enhance network segmentation to isolate critical systems and limit the potential spread of future incidents.
- Verify the integrity of critical system files and configurations to ensure they have not been tampered with during the incident.
- Consider using file integrity monitoring tools to detect unauthorized changes in real-time.
- Conduct thorough testing and verification to ensure that the incident has been completely eradicated.
- Validate that the affected systems are functioning as expected and without any abnormalities.
- Implement continuous monitoring and intrusion detection measures to promptly detect and respond to any signs of recurring or new incidents.

[Provide step-by-step instructions for containing and eradicating incidents.]

### 6.3. Incident Recovery

- Prioritize the recovery of critical systems and data based on the organization's business impact analysis and the results of the post-incident assessment.
- Develop a detailed recovery plan with specific tasks, timelines, and responsible parties for each critical system or service, that details when recovery should be initiated.
- Restore data from backups to affected systems, ensuring the integrity and security of the data.
- Verify the validity of backups and perform data consistency checks.
- Rebuild affected systems using clean images or configurations from trusted sources.
- Apply all necessary security patches and updates to ensure the systems are protected from known vulnerabilities.
- Verify that the configurations of recovered systems align with the organization's security standards.

- Perform vulnerability scans on recovered systems to identify any remaining vulnerabilities or potential attack vectors.
- Communicate with users and stakeholders about the progress of the recovery efforts.
- Inform them about any temporary changes in service availability or operational procedures during the recovery process.
- Implement continuous monitoring and additional security measures to ensure that recovered systems remain secure.
- Monitor for any signs of recurring incidents or potential indicators of compromise.
- Gradually restore normal operations as systems are confirmed to be secure and fully functional.
- Continuously monitor systems and services after recovery to detect any anomalies or issues that may arise.

[Explain the procedures for recovering affected systems and data.]

**6.4. Evidence Handling**

6. Designate a qualified team member to handle evidence collection and preservation.
6. Use digital forensic tools to acquire and analyze evidence following chain-of-custody procedures to preserve the integrity of evidence thought the investigation process.

[Describe the process for collecting, preserving, and analyzing digital evidence.]
[Ensure compliance with legal and chain-of-custody requirements.]

# A. INCIDENT SPECIFIC PROCEDURES

**a.** This section discusses the procedure for handling virus, worm and hacker/cracker incidents.

b. **VIRUS AND WORM INCIDENTS**

**i.** Although virus and worm incidents are very different, the procedures for handling each are very similar aside from the initial isolation of the system and the time criticality. Viruses are not self-replicating and, thus, incidents of this nature are not as time critical as worm or hacker incidents. Worms are self-replicating and can spread to hundreds of machines in a matter of minutes, thus, time is a critical factor when dealing with a worm attack. If you are not sure of the type of attack, then proceed as if the attack was worm related.

ii. **Isolate the System**

**1.** Isolate infected system(s) from the remaining City of Joplin network as soon as possible. If a worm is suspected, then a decision must be made to disconnect the City of Joplin from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since the City of Joplin will be disconnected from sites which may have patches. The City of Joplin CISO must authorize the isolation of the network from the outside world.

**iii. Log all actions.**

1. Do not power off or reboot systems that may be infected. There are some viruses that will destroy disk data if the system is power-cycled or rebooted. Also, rebooting a system could destroy needed information or evidence.

**iv. Notify Appropriate People**

B. Notify the City of Joplin SOC Manager as soon as possible. If unable to reach him/her within 10 minutes, contact the backup person. The City of Joplin SOC Manager will then be responsible for notifying other appropriate personnel. ***** NOTE -** Below, different times are given for suspected worm attack and for a suspected virus attack.

C. - The City of Joplin NW Administrator or SOC Manager will notify the City of Joplin CISO within two hours (one hour for a worm attack). The City of Joplin CISO will escalate to higher level management if necessary.

D. - The control room or City of Joplin SOC Manager should notify all involved LSAs within four hours (two hours for a worm attack).

**i. Identify the Problem**

1. Try to identify and isolate the suspected virus or worm-related files and processes. Prior to removing any files or killing any processes, a snapshot of the system should be taken and saved. Below is a list of tasks to make a snapshot of the system:

E. 1) Save a copy of all system log files. The log files are usually located in /usr/adm.

F. 2) Save a copy of the root history file, */.history*.

G. 3) Save copies of the */etc/utmp* and */etc/wtmp* files. Sometimes these files are found in the */usr/adm* directory.

H. 4). Capture all process status information in a file using the command ps -awwxl > file name for BSD systems and ps -efl > file name for SYSV systems.

1. If specific files that contain virus or worm code can be identified, then move those files to a safe place or archive them to tape and then remove the infected files. Also, get a listing of all active network connections. A control room analyst can provide assistance in obtaining snap-shot information on the system.
2. Run the cop's security checker on the infected system(s) to identify other possible problems such as altered system files, new suid programs or hidden special files. It may be necessary to install a clean version of cops from tape.
3. If other sites have been involved at this point, they may have helpful information on the problem and possible short-term solutions. Also, any helpful information gained about the virus or worm should be passed along to Internet CERT sites, after approval by City of Joplin CISO. Log all actions.

**ii. Contain the virus or worm**

1. All suspicious processes should now be halted and removed from the system. Make a full dump of the system and store it in a safe place. The tapes should be carefully labeled so they will not be used by unsuspecting people in the future. Then remove all suspected infected files or worm code. In the case of a worm attack, it may be necessary to keep the system(s) isolated from the outside world until all City of Joplin systems have been inoculated and/or the other internet sites have been cleaned up and inoculated. **Log all actions.**

**iii. Inoculate the System(s)**

1. Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been analyzed, then the task of assessing the damage is not very difficult. However, if the offending code has not been analyzed, then it may be necessary to restore the system from backup tapes. Once the system is brought back into a safe mode, then any patches or fixes should be implemented and tested. If possible, the virus or worm should be let loose on an isolated system that has been inoculated to ensure the system(s) are no longer vulnerable. **Log all actions.**

**iv. Return to a Normal Operating Mode**

1. Prior to bringing the systems back into full operation mode, you should notify the same group of people who were notified in stage one. The users should also be notified that the systems are returning to a fully operational state. It may be wise to request all users to change their passwords. Before restoring connectivity to the outside world, verify that all affected parties have successfully eradicated the problem and inoculated their systems. **Log all actions.**

**v. Follow-up Analysis**

1. After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up
postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All parties involved (or a representative from each group) should meet and discuss actions that were taken, and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s). If applicable, a set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by the City of Joplin CISO and distributed to all appropriate personnel.

**b. HACKER/CRACKER INCIDENTS**

i. Responding to hacker/cracker incidents is somewhat different than responding to a worm or virus incident. Some hackers are very sophisticated and will go to

great depths to avoid detection. Others are naive young students looking for a thrill. A hacker can also be someone on the inside engaging in illicit system activity (i.e., password cracking). Any hacker/cracker incident needs to be addressed as a real threat to the NPSN.

ii. Hacker incidents can be divided into three types: attempts to gain access to a system, an active session on a system, or events which have been discovered after the fact. Of the three, an active hacker/cracker session is the most severe and must be dealt with as soon as possible.

iii. There are two methods for dealing with an active hacker/cracker incident. The first method is to immediately lock the person out of the system and restore the system to a safe state. The second method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to an identification and possible criminal conviction. The method used to handle a cracker/hacker incident will be determined by the level of understanding of the risks involved.

**iv. Attempted Probes into a NPSN System**

1. Incidents of this type would include repeated login attempts, repeated ftp, telnet or rsh commands, and repeated dial-back attempts.

**v. Identify Problem**

**1.** Identify source of attack(s) by looking at system log files and active network connections. Make copies of all audit trail information such a system logs files, the root history file, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. **Log all actions.**

**vi. Notify City of Joplin SOC Manager**

1. Notify the City of Joplin SOC Manager within 30 minutes. If the City of Joplin SOC manager cannot be reached, then notify the City of Joplin NW Administrator or the City of Joplin SOC Manager backup person. The City of Joplin SOC Manager or their backup person will be responsible for notifying other levels of management.

**vii. Identify Hacker/Cracker**

**1.** If the source of the attacks can be identified, then the City of Joplin SOC Manager (or a designated person) will contact the system administrator or security analyst for that site and attempt to obtain the identity of the hacker/cracker. The NIC may be one source for obtaining the name and phone number of the site administrator of the remote site. If the hacker/cracker can be identified, the information should be provided to the City of Joplin SOC Manager or CISO. The City of Joplin IT Manager or CISO will provide directions on how to proceed, if necessary. **Log all actions.**

**viii. Notify CERT**

**1.** If the source of the attacks cannot be identified, then the City of Joplin CISO will contact the Internet CIRT and CIAC teams and provide them

with information concerning the attack. ***NOTE - Release of information must be approved by the City of Joplin CISO or someone he designates. **Log all actions.**

**ix. Follow-up**

1. After the investigation, a short report describing the incident and actions that were taken should be written by the City of Joplin SOC Manager or CISO and distributed to the appropriate people. After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All parties involved (or a representative from each group) should meet and discuss actions that were taken, and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s).

**x. Active Hacker/Cracker Activity**

1. Incidents of this type would include any active session or command by an unauthorized person. Some examples would include an active login or telnet session, an active ftp session, or a successful dial-back attempt. In the case of active hacker/cracker activity, a decision must be made whether to allow the activity to continue while you gather evidence or to get the hacker/cracker off the system and then lock the person out. Since a hacker can do damage and be off the system in a matter of minutes, time is critical when responding to active hacker attacks. This decision must be made by the City of Joplin CISO or someone he designates (i.e., the City of Joplin SOC Manager). The decision will be based on the availability of qualified personnel to monitor and observe the hacker/cracker and the level of risk involved.

**xi. Notify Appropriate People**

I. Notify the City of Joplin SOC Manager as soon as possible. If unable to reach him/her within 5 minutes, contact the backup person. The SOC Manager will then be responsible for notifying other appropriate personnel. The City of Joplin SOC Manager, with possible help from the involved LSA, will be responsible for trying to assess what the hacker/cracker is after, and the risks involved in letting the hacker/cracker continue his/her activity.

J. The City of Joplin SOC Manager will notify the City of Joplin CISO as soon as possible. If unable to reach him within ten minutes, his backup person should be contacted. The City of Joplin CISO can make the decision to allow the hacker to continue or to lock him out of the system.

K. The City of Joplin SOC Manager or CISO will notify the City of Joplin City Manager within 30 minutes. The City of Joplin City Manager will escalate to higher level management if necessary.

**i. Removal of Hacker/Cracker from the System, Snapshot the System**

1. Make copies of all audit trail information such as system logs files, the root history files, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Any suspicious files should be moved to a safe place or archived to tape and then removed from the system. Also, get a listing of all active network connections. A control room analyst can provide assistance in obtaining snap-shot information on the system. **Log all actions.**

**ii. Lock Out the Hacker**

1. Kill all active processes for the hacker/cracker and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the hacker/cracker. At this stage, the hacker/cracker should be locked out of the system. **Log all actions.**

**iii. Restore the System**

1. Restore the system to a normal state. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Inform the appropriate people. All actions taken to restore the system to a normal state should be documented in the logbook for this incident. **Log all actions.**

**iv. Notify Other Agencies**

1. Report the incident to the Ames CNSRT, the Internet CIRT and to CIAC. ***NOTE- Release of information must be approved by the City of Joplin CISO or someone he designates. **Log all actions**.

**v. Follow-up**

1. After the investigation, a short report describing the incident and actions that were taken should be written by the City of Joplin SOC Manager or CISO and distributed to the appropriate people. After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All parties involved (or a representative from each group) should meet and discuss actions that
were taken, and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-
line copies of infected files, worm code, etc., should be removed from the system(s).

**vi. Monitoring of Hacker/Cracker Activity**

1. There are no set procedures for monitoring the activity of a hacker. Each incident will be dealt with on a case-by-case basis. The City of Joplin CISO or the person authorizing the monitoring activity should provide directions to those doing the monitoring. Once the decision has been made to cease monitoring the hacker's activities and have him removed from the system(s).

**b. DDoS (Distributed Denial of Service) Attack**

*i. Detection*

**ii. Traffic Analysis**

1. Use network traffic analysis tools such as intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic. Look for unusual traffic patterns, high request rates, or traffic from suspicious sources.
2. Implement flow data analysis tools like NetFlow to track traffic volume and patterns.

**iii. Pattern Recognition**

1. Configure your monitoring tools to recognize patterns indicative of DDoS attacks, such as a sudden spike in incoming requests.
2. Set up thresholds and alerts that trigger when traffic anomalies are detected.

**iv. Alerting**

1. Establish alerting mechanisms to notify the incident response team in real-time when unusual traffic patterns are detected.
2. These alerts can be configured to include information about the type and magnitude of the attack, allowing for a quicker response.

*v. Response*

**vi. DDoS Mitigation**

1. Employ dedicated DDoS mitigation solutions to filter out malicious traffic and reduce the impact of the attack.
2. Work with upstream providers to implement traffic filtering and rate limiting measures.
3. Divert traffic through cloud-based DDoS protection services that can absorb the attack's impact.

**vii. Communication**

1. Maintain open lines of communication with affected citizens to keep them informed about the situation, the measures being taken, and estimated resolution times.
2. Consider a public-facing status page to provide updates on service availability to citizens.

**viii. Logging**

1. Create detailed logs of the DDoS attack, including the attack vector, source IPs, duration, and response measures taken.
2. These logs are valuable for post-incident analysis, reporting, and legal purposes.

**c. Malware Infection**

*i. Detection*

**ii. Antivirus and IDS**

1. Utilize antivirus software on endpoints and intrusion detection systems (IDS) on network segments to identify and alert malware presence.

2. Set up regular signature and behavior-based scans to detect known and unknown threats.

**iii. File Scanning**

1. Implement file scanning on incoming and outgoing email attachments, downloaded files, and shared documents to detect potential malware.
2. Use sandboxing to isolate and analyze suspicious files safely.

**iv. Traffic Analysis**

1. Monitor outbound network traffic to detect unusual patterns that may be indicative of a compromised system attempting to communicate with a command-and-control server.

*v. Response*

**vi. Isolation**

1. Isolate affected systems from the network to prevent the spread of malware and protect other devices from infection.
2. Disable or disconnect the compromised devices to ensure they do not pose a threat to the network.

**vii. Malware Analysis**

1. Analyze the malware to determine its type, behavior, and the entry point through which it entered the network. This analysis can help identify potential vulnerabilities that allowed the infection.

**viii. Removal and Patching**

1. Remove the malware from infected devices using antivirus tools and manual remediation methods.
2. Identify and patch the vulnerabilities that the malware exploited to prevent re-infection.

**ix. Communication**

1. If customer data or privacy is affected, notify the affected citizens and provide information on the steps taken to remediate the malware infection.

**x. Post-Incident Scanning**

1. After removing the malware, perform a thorough post-incident scan to ensure that no traces of the malware remain.

**d. Data Breach**

*i. Detection*

**ii. Monitoring**

1. Continuously monitor logs and access control lists for any signs of unauthorized access or changes to sensitive data.
2. Set up real-time alerts for suspicious activities, such as multiple failed login attempts or access from unusual locations.

**iii. Intrusion Detection**

1. Utilize intrusion detection and prevention systems to detect unusual user activity and access patterns, especially in critical systems and data repositories.

**iv. Log Analysis**

1. Regularly review logs, access logs, and audit trails to identify any suspicious activity, unauthorized access, or data modifications.

v. *Response*

vi. **Containment**

1. Quickly contain the breach by isolating affected systems and revoking unauthorized access.
2. Limit lateral movement of attackers within the network to prevent further damage.

vii. **Investigation**

1. Conduct a thorough investigation to determine the extent of the data breach. Identify what data was accessed, how it was accessed, and who was responsible.
2. Assess the potential damage and impact of the breach.

viii. **Vulnerability Patching**

1. Identify and patch the vulnerabilities that allowed the breach to occur in the first place.
2. Implement security enhancements, such as multi-factor authentication and encryption, to improve data protection.

ix. **Communication**

1. Notify affected citizens and regulatory authorities as per data breach notification laws. Provide detailed information about the breach, its scope, and the steps taken for remediation.
2. Maintain open communication channels with affected parties.

x. **Legal Cooperation**

1. Cooperate with law enforcement agencies to support potential investigations and evidence collection.
2. Preserve evidence and logs for legal and regulatory purposes.

xi. **Security Enhancement**

1. Enhance security controls, including access controls, network segmentation, and data encryption, to prevent future data breaches.

# 7. COMMUNICATION & NOTIFICATION

## 7.1. Internal Communication

7.1.1.1. Incident Response Team members shall communicate through a dedicated incident response channel on the company's collaboration platform, Microsoft TEAMS.

7.1.1.2. Escalate incidents to higher management levels as per the predefined escalation process.

[Specify how incidents will be reported within the organization.]
[Define the communication channels and stakeholders to be informed.]

## 7.2. External Communication

7.2.1.1. Notify citizens, partners, and regulatory authorities in accordance with legal requirements and data breach notification laws.

7.2.1.2. Communications shall be coordinated by the Communications Manager.

[Outline the process for notifying relevant external parties, such as citizens, partners, and regulatory authorities.]

[Ensure consistent and timely communication.]

## 8. TRAINING & AWARENESS

8.1. All employees shall receive regular cybersecurity awareness training to recognize and report potential security incidents. The Incident Response Team shall conduct simulated incident response exercises at least once a year to test the organization's preparedness and identify areas for improvement.

[Detail the importance of regular training for employees on incident response procedures.] [Consider conducting simulated exercises to test the effectiveness of the plan.]

## 9. CONTINUOUS IMPROVEMENT

9.1. The Incident Response Team shall conduct post-incident reviews to evaluate the root cause, identify lessons learned, and overall effectiveness of the response. Based on the review findings, updates to the Incident Response Plan and related processes shall be made to enhance incident response capabilities.

[Describe how the incident response plan will be regularly reviewed, updated, and tested.] [Define metrics for evaluating the plan's effectiveness and making necessary improvements.]

## 10. LEGAL REGULATORY CONCIDERATIONS

10.1. Legal Counsel shall be responsible for staying up to date with relevant cybersecurity laws and regulations. The Incident Response Team shall collaborate with Legal Counsel to ensure compliance with data breach notification laws and other legal requirements.

[Address any legal or regulatory requirements specific to your organization's industry.]

[Ensure compliance with data protection and privacy regulations.]

## 11. PLAN DISTRIBUTION

11.1. Once approved, the Incident Response Plan shall be distributed to all members of the Incident Response Team and other relevant stakeholders.

11.2. The plan shall be easily accessible to employees through the company's intranet or a designated shared drive.

[List the individuals or entities responsible for distributing the plan to relevant stakeholders.]

## 12. EMPLOYEE AUDIT PLAN REVISION HISTORY

| Version | | Date | Author(s) | Changes Made |
|---|---|---|---|---|
| **1.0** | | 1/1/2000 | (Consulting Company) | Initial |
| | | | | |
| | | | | |

# Executive Approval Signature

| | | |
|---|---|---|
| _____ | | _____ |
| **Print Name** | **IT Director (CISO) Signature** | **Date** |
| _____ | | _____ |
| **Print Name** | **City Manager Signature** | **Date** |

**Version: [1.0]**
**Effective Date: [1/1/2000]**