TOWNSHIP OF MULLICA
COMMITTEE AGENDA
MAY 25, 2021
7:00 P.M.

CALL TO ORDER

SUNSHINE LAW

FLAG SALUTE

ROLL CALL

APPROVAL OF MINUTES: 04 / 08 / 2021

PUBLIC DISCUSSION RELATING TO AGENDA ITEMS

Resolution #122-2021 / Authorizing Local Examination and CFO Certification

HEARING: 2021 MUNICIPAL BUDGET

FIRST READING: Ordinance #7-2021 / Amend Chapter 144-123A / Accessory Structures

Ordinance #8-2021 / Amending Chapter 192 / Smoking

COMMITTEE REPORTS

CORRESPONDENCE

OLD BUSINESS:

NEW BUSINESS:

A. Accept Resignation Municipal Alliance / Laura Engelmann
B. Resolution #123-2021 / Thank You Municipal Alliance Member / Laura Engelmann
C. Resolution #124-2021 / Adopt Information Technology Practice Policy
D. Resolution #125-2021 / Refund Taxes – Block 11023, Lot 11 / Cape Atlantic Title

PAYMENT OF BILLS

PUBLIC DISCUSSION

ADJOURN

MEETING INFORMATION:

Join Zoom Meeting
https://zoom.us/j/6579457427?pwd=dEtEQk5jUFhXbUwrT01idUlySGNtQT09

Meeting ID: 657 945 7427
Passcode: 0117
One tap mobile
+13126266799,,6579457427# US (Chicago)
+16465588656,,6579457427# US (New York)

Dial by your location

+1 312 626 6799 US (Chicago)
+1 646 558 8656 US (New York)
+1 301 715 8592 US (Washington D.C)
+1 346 248 7799 US (Houston)
+1 669 900 9128 US (San Jose)
+1 253 215 8782 US (Tacoma)

Meeting ID: 657 945 7427
Find your local number: https://zoom.us/u/a0XfMYEff

Questions or public comments concerning meetings may be submitted in advanced via e-mail to the Township Clerk: kjohnson@mullicatownship.org and/ or alupinetti@mullicatownship.org or mailed to Kimberly Johnson, RMC; Township of Mullica; P.O. Box 317; 4528 White Horse Pike; Elwood, NJ 08217. (***Must be received prior to 4:00 p.m. on the day of the meeting.)***

TOWNSHIP OF MULLICA
RESOLUTION NO. 122-2021

SELF-EXAMINATION OF BUDGET

WHEREAS, N.J.S.A. 40A:4-78b has authorized the Local Finance Board to adopt rules that permit municipalities in sound fiscal condition to assume the responsibility, normally granted to the Director of the Division of Local Government Services, of conducting the annual budget examination; and

WHEREAS, N.J.A.C. 5:30-7 was adopted by the Local Finance Board on February 11, 1997; and

WHEREAS, pursuant to N.J.A.C. 5:30-7.2 through 7.5, the Township of Mullica has been declared eligible to participate in the program by the Division of Local Government Services, and the Chief Financial Officer has determined that the local government meets the necessary conditions to participate in the program for the 2017 budget year.

NOW, THEREFORE, BE ITS RESOLVED, by the governing body of the Township of Mullica that in accordance with N.J.A.C. 5:30-7.6a & 7.6b and based upon the Chief Financial Officer's certification, the governing body has found the budget has met the following requirements:

1. That with reference to the following items, the amounts have been calculated pursuant to law and appropriated as such in the budget.

    a. Payments of interest and debt redemption charges
    b. Deferred charges and statutory expenditures
    c. Cash deficit of preceding year
    d. Reserve for uncollected taxes
    e. Other reserves and non-disbursement items
    f. Any inclusions of amounts required for school purposes

2. That the provisions relating to limitation on increases of appropriations pursuant to N.J.S.A. 40A:4-45.2 and appropriations for exceptions to limits on appropriations found at N.J.S.A. 40A:4-45.3 et seq., are fully met (complies with CAP law).

3. That the budget is in such form, arrangement, and content as required by the Local Budget Law and N.J.A.C. 5:30-4 and 5:30-5.

4. That pursuant to the Local Budget Law:

    a. All estimates of revenue are reasonable, accurate, and correctly stated,
    b. Items of appropriation are properly set forth
    c. In itemization, form, arrangement and content, the budget will permit the exercise of the comptroller function within the municipality.

5. The budget and associated amendments have been introduced and publicly advertised in accordance with the relevant provisions of the Local Budget Law,

except that failure to meet the deadlines of N.J.S.A. 40A:4-5 shall not prevent such certification.

6. That all other applicable statutory requirements have been fulfilled.

BE IT FURTHER RESOLVED that a copy of this resolution will be forwarded to the Director of the Division of Local Government Services upon adoption.

Adopted: May 25, 2021

_____
KRISTI HANSELMANN, MAYOR

_____
KIMBERLY JOHNSON
TOWNSHIP CLERK

MULLICA TOWNSHIP
ATLANTIC COUNTY, NEW JERSEY

CERTIFICATION OF APPROVED BUDGET

It is hereby certified that the Approved Budget complies with the requirements of law and approval is given pursuant to N.J.S.A. 40A:4-78(b) and N.J.A.C. 5:30-7.

It is further certified that the municipality has met the eligibility requirements of N.J.A.C. 5:30-7.4 and 7.5, and that I, as Chief Financial Officer, have completed the local examination in compliance with N.J.A.C. 5:30-7.6.

By: _____

Dawn Stollenwerk
Chief Financial Officer

Date: May 25, 2021

2021 Introduced Budget 4/27/21

	% Change	$ Change	Budgeted 2021	Adopted Budget 2020	Amended by Transfers/Emerg	Amended Budget 2020	Actual 2020	Difference 2020
APPROPRIATIONS								
Township Committee S & W	0.00%	-	15,000.00	15,000.00	-	15,000.00	15,000.00	-
Township Committte O/E	48.57%	1,700.00	5,200.00	3,500.00		3,500.00	2,230.50	1,269.50
Clerk S & W	3.14%	4,000.00	131,500.00	127,500.00		127,500.00	125,058.91	2,441.09
Clerk O/E	0.00%	-	20,000.00	20,000.00	-	20,000.00	19,448.98	551.02
Finance S & W	3.65%	2,500.00	71,000.00	68,500.00		68,500.00	68,368.04	131.96
Finance O/E	0.00%	-	18,000.00	16,000.00	2,000.00	18,000.00	17,424.50	575.50
Audit O/E	10.20%	2,500.00	27,000.00	24,500.00		24,500.00	24,400.00	100.00
Prosector O/E	-7.69%	(1,000.00)	12,000.00	13,000.00		13,000.00	12,000.00	1,000.00
Public Defender O/E	0.00%	-	7,150.00	7,150.00		7,150.00	6,600.00	550.00
Collector S & W	4.05%	3,350.00	86,100.00	82,750.00		82,750.00	82,735.38	14.62
Collector O/E	27.50%	2,200.00	10,200.00	8,000.00		8,000.00	7,568.72	431.28
Assessor S & W	3.72%	1,495.00	41,700.00	40,205.00		40,205.00	40,005.94	199.06
Assessor O/E	-0.14%	(10.00)	7,050.00	6,060.00	1,000.00	7,060.00	6,253.93	806.07
Workman's Compensation	1.30%	1,568.00	122,000.00	124,000.00	(3,568.00)	120,432.00	120,432.00	-
Employee Group Insurance	3.55%	25,000.00	730,000.00	725,000.00	(20,000.00)	705,000.00	704,955.24	44.76
General Liability	0.00%	-	53,000.00	53,000.00		53,000.00	53,000.00	-
Health Benefits Waiver	116.59%	3,499.00	6,500.00	1.00	3,000.00	3,001.00	1,261.52	1,739.48
Legal O/E	-15.54%	(23,000.00)	125,000.00	115,000.00	33,000.00	148,000.00	147,779.94	220.06
Court S & W	4.99%	4,800.00	101,000.00	96,200.00		96,200.00	84,843.52	11,356.48
Court O/E	0.00%	-	7,450.00	7,450.00		7,450.00	4,693.15	2,756.85
Planning Board S & W	0.00%	-	5,000.00	5,000.00		5,000.00	4,587.93	412.07
Planning Board O/E	86.96%	10,000.00	21,500.00	11,500.00		11,500.00	9,653.75	1,846.25
Engineering O/E	40.00%	10,000.00	35,000.00	25,000.00		25,000.00	24,581.58	418.42
Historical Society O/E	0.00%	-	5,000.00	5,000.00		5,000.00	5,000.00	-
Senior Citizen Advisory	0.00%	-	1,000.00	1,000.00		1,000.00	1,000.00	-
Police S & W	-0.25%	(3,000.00)	1,212,000.00	1,235,000.00	(20,000.00)	1,215,000.00	1,115,641.64	99,358.36
Police O/E	11.22%	13,065.00	129,500.00	116,435.00		116,435.00	105,618.13	10,816.87
Emergency Mgmt S & W	0.00%	-	4,500.00	4,500.00		4,500.00	2,865.27	1,634.73
Emergency Mgmt O/E	0.00%	-	1,000.00	1,000.00		1,000.00	17.40	982.60
Aid to Volunteer Fire Companies	0.00%	-	69,000.00	69,000.00		69,000.00	69,000.00	-
Emergency Medical Services	-100.00%	(1.00)	-	1.00		1.00	-	1.00
Public Works S/W	2.54%	4,250.00	171,750.00	152,500.00	15,000.00	167,500.00	159,933.42	7,566.58
Public Works O/E	55.56%	25,000.00	70,000.00	70,000.00	(25,000.00)	45,000.00	36,085.91	8,914.09
Reserve for Storm Recovery	-99.99%	(10,000.00)	1.00	1.00	10,000.00	10,001.00	10,000.00	1.00
Vehicle Maintenance O/E	16.00%	12,000.00	87,000.00	75,000.00		75,000.00	70,140.03	4,859.97
Solid Waste Contracts	-100.00%	(151,000.00)	-	151,000.00		151,000.00	130,089.76	20,910.24
Buildings & Grounds O/E	1.84%	910.00	50,250.00	46,000.00	3,340.00	49,340.00	46,985.73	2,354.27
Landfill & Solid Waste Disposal	-19.73%	(36,500.00)	148,500.00	185,000.00		185,000.00	161,169.43	23,830.57
Dog Regulation	0.00%	-	8,000.00	8,000.00		8,000.00	5,500.00	2,500.00
Environmental Commission	0.00%	-	200.00	200.00		200.00	-	200.00
Recreation Services & Programs	0.00%		5,000.00	5,000.00		5,000.00	5,000.00	-
Maintenance of Parks	0.00%		25,000.00	23,000.00		23,000.00	13,243.32	9,756.68
Construction Official S & W	-15.61%	(15,300.00)	82,700.00	98,000.00		98,000.00	96,438.39	1,561.61
Construction Official O/E	33.33%	1,000.00	4,000.00	3,000.00		3,000.00	2,594.68	405.32
Other Code EnforcementS & W	82.61%	9,500.00	21,000.00	16,500.00	(5,000.00)	11,500.00	8,092.15	3,407.85
Other Code Enforcement O/E	0.00%	-	2,500.00	2,500.00		2,500.00	92.17	2,407.83
Electricity & Natural Gas	0.00%	-	80,000.00	80,000.00		80,000.00	69,034.61	10,965.39
Telecommunications	13.73%	3,500.00	29,000.00	24,000.00	1,500.00	25,500.00	23,972.88	1,527.12
Petroleum Products	4.84%	3,000.00	65,000.00	65,000.00	(3,000.00)	62,000.00	61,070.31	929.69
Accumulated Absence	0.00%	-	500.00	500.00		500.00	500.00	
Settlement Award		-	-	-	-	-		
Sub-total apppropriations in CAPS	-2.36%	(94,974.00)	3,930,751.00	4,031,453.00	(7,728.00)	4,023,725.00	3,781,968.76	241,756.24
						-		
PERS	19.50%	15,414.00	94,463.00	79,049.00		79,049.00	79,049.00	-
Social Security	8.67%	13,000.00	163,000.00	150,000.00		150,000.00	137,576.72	12,423.28
PFRS	14.42%	39,483.00	313,354.00	266,143.00	7,728.00	273,871.00	273,870.87	0.13
Unemployment	0.00%	-	10,000.00	10,000.00		10,000.00	7,654.50	2,345.50
DCRP	0.00%	-	4,500.00	4,500.00		4,500.00	2,815.71	1,684.29
Deferred Charges & Statutory Expe	13.12%	67,897.00	585,317.00	509,692.00	7,728.00	517,420.00	500,966.80	16,453.20
						-		-
Salaries & Wages inside CAP	0.60%	11,595.00	1,949,750.00	1,941,656.00	(7,000.00)	1,934,656.00		##########
Other Expenses inside CAP	-1.48%	(38,672.00)	2,566,318.00	2,599,489.00	7,000.00	2,606,489.00		##########

	% Change	$ Change	Budgeted 2021	Adopted Budget 2020	Amended by Transfers/Emerg	Amended Budget 2020	Actual 2020	Difference 2020
REVENUE								
Surplus	28.43%	183,000.00	826,600.00	643,600.00		643,600.00	643,600.00	0.0192
Alcoholic Beverages	0.00%	-	4,500.00	4,500.00		4,500.00	4,500.00	-
Fines & Costs-Court	-54.55%	(60,000.00)	50,000.00	110,000.00		110,000.00	78,890.43	(31,109.57)
Interest & Costs on Taxes	20.00%	15,000.00	90,000.00	75,000.00		75,000.00	96,933.36	21,933.36
Interest on Investments	38.89%	7,000.00	25,000.00	18,000.00		18,000.00	31,179.46	13,179.46
Trailer Pad Fees	0.00%	-	40,000.00	40,000.00		40,000.00	44,528.00	4,528.00
Cell Tower Revenues	-2.50%	(1,000.00)	39,000.00	40,000.00		40,000.00	39,781.18	(218.82)
Sub-Total Local Revenues	-13.57%	(39,000.00)	248,500.00	287,500.00		287,500.00	295,812.43	8,312.43
								-
UCC Fees	0.00%	-	85,000.00	85,000.00		85,000.00	96,719.00	11,719.00
								-
Consolidated Prop Tax Relief	0.00%	-	17,432.00	17,432.00		17,432.00	17,432.00	-
Energy Receipts	0.00%		434,344.00	434,344.00		434,344.00	434,344.00	-
Garden State Trust	-35.17%	(22,484.00)	41,440.00	63,924.00		63,924.00	41,440.00	(22,484.00)
Sub-Total State Aid	-4.36%	(22,484.00)	493,216.00	515,700.00		515,700.00	493,216.00	(22,484.00)
								-
Interlocal Agreement - SRO	0.00%	-	75,000.00	75,000.00		75,000.00	57,068.60	(17,931.40)
Interlocal Agreement - Contruction			58,125.00	-		-	-	-
Sub-Total Interlocals	0.00%	-	133,125.00	75,000.00		75,000.00	57,068.60	(17,931.40)
								-
NJ Transportation Trust Fund	78.81%	72,316.00	164,076.00	91,760.00		91,760.00	91,760.00	-
Drunk Driving Enforcement	-62.17%	(5,747.17)	3,497.74	9,244.91		9,244.91	9,244.91	-
Clean Communities	-100.00%	(20,687.53)			20,687.53	20,687.53	20,687.53	-
Recycling Tonnage Grant	5.85%	229.50	4,152.78	3,923.28		3,923.28	3,923.28	-
Municipal Alliance	-30.30%	(2,632.48)	6,054.52	8,687.00		8,687.00	8,687.00	-
Safe & Secure		16,604.00	16,604.00	-		-	-	
Community Dev Block Grant		-				-	-	
Distracted Driving Grant		6,000.00	6,000.00	-		-	-	
Body Armor Grant	-14.55%	(231.55)	1,359.60	1,591.15		1,591.15	1,591.15	-
USRDA SEARCH Grant	-100.00%	(30,000.00)	-	30,000.00		30,000.00	30,000.00	-
Drive Sober or Get Pulled Over	-100.00%	(6,000.00)			6,000.00	6,000.00	6,000.00	-
Click It or Ticket		-		-		-	-	
US DOJ Body Armor Grant		1,798.00	1,798.00	-	-	-	-	-
Sub-Total Grants	18.41%	31,648.77	203,542.64	145,206.34	26,687.53	171,893.87	171,893.87	-
Capital Fund Surplus		-	-	-		-		-
Sub-Total Revenues with Consent		-	-	-		-	-	
								-
Receipts from Delinquent Taxes	20.51%	80,000.00	470,000.00	390,000.00		390,000.00	460,744.20	70,744.20
								-
Sub-Total General Revenues	13.43%	291,289.77	2,459,983.64	2,142,006.34		2,168,693.87	2,219,054.10	50,360.23
								-
Amount to be Raised by Taxation	2.26%	90,099.48	4,084,843.85	3,994,744.37		3,994,744.37	4,087,013.85	92,269.48
								-
TOTAL REVENUES	6.19%	381,389.25	6,544,827.49	6,136,750.71		6,163,438.24	6,306,067.95	142,629.71

	% Change	$ Change	Budgeted 2021	Adopted Budget 2020	Amended by Transfers/Emerg	Amended Budget 2020	Actual 2020	Difference 2020
Appropriations Excluded From CAI						-		
						-		
Health Insurance		-	-	-		-	-	-
NJDEP Stormwater Management	0.00%	-	12,000.00	12,000.00		12,000.00	500.00	11,500.00
Delcared Emergency - Corona Virus		(40,000.00)	-	40,000.00		40,000.00	0.10	39,999.90
						-		-
Interlocal Agreement - Dispatch	1.81%	4,000.00	225,000.00	221,000.00		221,000.00	221,000.00	-
Interlocal Agreement - Solid Waste		299,000.00	299,000.00	-		-	-	-
Interlocal Agreement - SRO	0.00%	-	75,000.00	75,000.00		75,000.00	35,429.50	39,570.50
Interlocal Agreement - Construction		58,125.00	58,125.00			-		-
Interlocal Agreement - Court		19,000.00	19,000.00			-		-
Interlocal Agreement - IT	11.01%	992.00	10,000.00	9,008.00		9,008.00	9,008.00	-
Sub-Total Interlocals	**124.95%**	**381,117.00**	**686,125.00**	**305,008.00**	**-**	**305,008.00**	**265,437.50**	**39,570.50**
						-		-
						-		-
Drunk Driving Enforcement	-62.17%	(5,747.17)	3,497.74	9,244.91		9,244.91	9,244.91	-
Clean Communities	-100.00%	(20,687.53)			20,687.53	20,687.53	20,687.53	-
Recycling Tonnage Grant	5.85%	229.50	4,152.78	3,923.28		3,923.28	3,923.28	-
Municipal Alliance	-30.30%	(2,632.48)	6,054.52	8,687.00		8,687.00	8,687.00	-
Municipal Alliance - Match	-30.30%	(658.12)	1,513.63	2,171.75		2,171.75	2,171.75	-
Community Dev Block Grant		-				-	-	-
USRDA SEARCH Grant	-100.00%	(30,000.00)	-	30,000.00		30,000.00	30,000.00	-
Safe & Secure Grant		52,903.00	52,903.00			-	-	-
Body Armor Grant	-14.57%	(231.79)	1,359.36	1,591.15		1,591.15	1,591.15	-
Drive Sober or Get Pulled Over	-100.00%	(6,000.00)			6,000.00	6,000.00	6,000.00	-
Distracted Driving Grant		6,000.00	6,000.00	-		-	-	-
Match for Fire Grant		23,000.00	23,000.00	-		-	-	-
US DOJ Body Armor Grant		1,798.00	1,798.00	-		-	-	-
Sub-Total Grants	**21.84%**	**17,973.41**	**100,279.03**	**55,618.09**	**26,687.53**	**82,305.62**	**82,305.62**	**-**
						-		
Total Operations Excluded From CA	**84.68%**	**372,013.41**	**798,404.03**	**412,626.09**	**26,687.53**	**439,313.62**	**348,243.22**	**91,070.40**
						-		-
Total S/W Excluded from CAPS	**52.25%**	**47,155.83**	**137,400.74**	**84,244.91**	**6,000.00**	**90,244.91**	**50,674.41**	**39,570.50**
Total O/E Excluded from CAPS	**93.06%**	**324,857.58**	**661,003.29**	**328,381.18**	**20,687.53**	**349,068.71**	**297,568.81**	**51,499.90**
NJ Transporation Trust Fund		72,316.00	164,076.00	91,760.00		91,760.00	91,760.00	-
Capital Improvement Fund	950.00%	95,000.00	105,000.00	10,000.00		10,000.00	10,000.00	-
Info Technology Equip & Supplies	100.00%	25,000.00	50,000.00	25,000.00		25,000.00	10,716.85	14,283.15
Road Improvements		-	-	-		-	-	-
Facility Improvements		-	-	-		-	-	-
Sub-Total Capital Improvements	**151.72%**	**192,316.00**	**319,076.00**	**126,760.00**	**-**	**126,760.00**	**112,476.85**	**14,283.15**
						-		-
Bond Principal	3.13%	5,000.00	165,000.00	160,000.00		160,000.00	160,000.00	-
BAN Payment	-100.00%	(136,500.00)	-	136,500.00		136,500.00	136,500.00	-
Interest on Bonds	-16.00%	(6,400.00)	33,600.00	40,000.00		40,000.00	40,000.00	-
Interest on Notes	-61.82%	(13,600.00)	8,400.00	22,000.00	-	22,000.00	20,570.94	-
Sub-Total Debt Service	**-42.26%**	**(151,500.00)**	**207,000.00**	**358,500.00**	**-**	**358,500.00**	**357,070.94**	**-**
						-		
Emergency Authorizations		-	-	-		-	-	
Special Emergency - Tax Map Update		-	-	-		-	-	-
Special Emergency - Revaluation	0.00%	-	50,000.00	50,000.00	-	50,000.00	50,000.00	-
Sub-Total Deferred Charges	**0.00%**	**-**	**50,000.00**	**50,000.00**	**-**	**50,000.00**	**50,000.00**	**-**
						-		-
General Appropriations	**6.99%**	**385,752.41**	**5,890,548.03**	**5,489,031.09**	**26,687.53**	**5,515,718.62**	**5,150,726.57**	**364,992.05**
						-		
Reserve for Uncollected Taxes	**1.01%**	**6,559.84**	**654,279.46**	**647,719.62**		**647,719.62**	**647,719.62**	**-**
						-		-
Total General Appropriations	**6.19%**	**381,389.25**	**6,544,827.49**	**6,136,750.71**	**26,687.53**	**6,163,438.24**	**5,798,446.19**	**364,992.05**

CAP Information

		appropriation	levy	levy w/bank
Total Available		4,653,664.90	4,276,388.55	$4,417,702.55
Total Appropriated		4,516,068.00	4,084,843.85	4,084,843.85
Remaining (Excess)		137,596.90	191,544.70	332,858.70
Difference between 2.5% & 3.5%	109,753.63		Cap Bank $	141,314.00

TAX

TAX RATE	2021 CURRENT	2020 PRIOR	CHANGE	
LOCAL	0.8984	0.8792	0.0192	2.18%
TOTAL	3.270	3.190	0.080	2.51%
TOTAL LOCAL LEVY	4,084,843.85	3,994,744.37	90,099.48	2.26%
NET VALUATION TAX	454,695,800	454,359,100	336,700.00	0.07%

TOTAL BUDGET

	CURRENT	PRIOR	CHANGE	
TOTAL REVENUE	6,544,827.49	6,163,438.24	381,389.25	6.19%
TOTAL APPROPRIATI	6,544,827.49	6,163,438.24	381,389.25	6.19%

SURPLUS

	AVAILABLE	BUDGETED	BALANCE	% used
CURRENT	1,237,139.34	826,600.00	410,539.34	66.82%
Prior Year	1,404,760.84	643,600.00	761,160.84	45.82%
Difference	(167,621.50)	183,000.00	(350,621.50)	

Cash Surplus Available $ 1,143,383.89

BUDGET ANALYSIS

	2021 BUDGET YEAR	2020 PRIOR YEAR	CHANGE	
REVENUE				
Surplus	826,600.00	643,600.00	183,000.00	28.43%
Local	466,625.00	447,500.00	19,125.00	4.27%
State Aid	493,216.00	515,700.00	(22,484.00)	-4.36%
Grants	203,542.64	171,893.87	31,648.77	18.41%
Delinquent Tax	470,000.00	390,000.00	80,000.00	20.51%
Local Tax	4,084,843.85	3,994,744.37	90,099.48	2.26%
TOTAL REVENUE	6,544,827.49	6,163,438.24	381,389.25	6.19%
APPROPRIATIONS				
Salaries and Wages	2,087,150.74	2,024,900.91	62,249.83	3.07%
OE & Statutory	3,127,042.26	2,873,252.09	253,790.17	8.83%
Grants	100,279.03	82,305.62	17,973.41	21.84%
Deferred Charges	50,000.00	50,000.00	-	0.00%
Capital	319,076.00	126,760.00	192,316.00	151.72%
Debt Service	207,000.00	358,500.00	(151,500.00)	-42.26%
Library Tax	-	-	-	
Reserve for Uncollect	654,279.46	647,719.62	6,559.84	1.01%
TOTAL APPROPRIATI	6,544,827.49	6,163,438.24	381,389.25	6.19%
	-	-	(0.00)	

% OF COLLECTION

	MAXIMUM	USED	UNUSED
%	95.80%	95.60%	0.20%
$	623,235.65	654,279.46	31,043.82
2019 rate	96.46%	96.00%	-0.66%

TOWNSHIP OF MULLICA
ORDINANCE NO. 7-2021

AN ORDINANCE AMENDING CHAPTER 144-123, LAND DEVELOPMENT, OF THE CODE OF THE TOWNSHIP OF MULLICA, COUNTY OF ATLANTIC AND STATE OF NEW JERSEY

WHEREAS, the Township Committee of the Township of Mullica having considered the amendments presented by the Planning Board wishes to amend Chapter 144-123 A., of the Code of the Township of Mullica; and

WHEREAS, the Planning Board and the Governing Body having determined that the proposed amendments contained herein would be in the best interests of the Township of Mullica and are consistent with the intent and purpose of the Mullica Township Master Plan; and

WHEREAS, the purpose of amendments is in response to recommendations made by a sub-committee of the Planning Board due to numerous variance applications.

NOW, THEREFORE, BE IT ORDAINED BY THE TOWNSHIP COMMITTEE OF THE TOWNSHIP OF MULLICA THAT, that the following amendments to be made:

Section I. Chapter 144, "Land Development", Article XII, Zoning Districts and Permitted Uses, §144-123 A. Accessory structures, is hereby amended by adding:

(5) Maximum square footage for a residential accessory building will be as follows:

Under two (2) acres: 850 square feet

Two (2) to five (5) acres: 1,250 square feet

Over five (5) acres: 1,500 square feet

(7) Sanitary facilities are restricted.

Section 2. This Ordinance shall take effect upon adoption, publication as provided by law.

Section 3. A certified copy of this Ordinance shall be forwarded to the Pinelands Commission for certification

First Reading: May 25, 2021

Adopted: June 8, 2021

Attest: _____ KRISTI HANSELMANN, MAYOR

_____

KIMBERLY JOHNSON, TOWNSHIP CLERK

TOWNSHIP OF MULLICA
ORDINANCE NO. 8-2021

An Ordinance Supplementing and Amending Chapter 192 of the Municipal Code of the Township of Mullica Governing Smoking on Municipal Property; and Repealing All Ordinances Heretofore Adopted the Provisions of Which Are Inconsistent Herewith.

WHEREAS, by Ordinance Number 4 of 2020 the Township Committee amended the Municipal Code to Add Chapter 192 SMOKING which, in Code Section 192.3, prohibits smoking in all property within the Township of Mullica as set forth therein; and

WHEREAS, in 2020 New Jersey voters approved Public Question No. 1, which amended the New Jersey Constitution to allow for the legalization of a controlled form of marijuana called "cannabis" for adults at least 21 years of age; and

WHEREAS, on February 22, 2021, Governor Murphy signed into law P.L. 2021, c. 16, known as the "New Jersey Cannabis Regulatory, Enforcement Assistance, and Marketplace Modernization Act" (the "Act"), which legalizes the recreational use of marijuana by adults 21 years of age or older, and establishes a comprehensive regulatory and licensing scheme for commercial recreational (adult use) cannabis operations, use and possession; and

WHEREAS, to avoid any confusion and prevent any inconsistency in enforcement, it is the intent of this governing body to expand the definition of Smoking to include the smoking of cannabis products.

NOW, THEREFORE, IT IS HEREBY ORDAINED, by the Township Committee of the Township of Mullica, County of Atlantic, and State of New Jersey:

SECTION 1:
Section 192.1 'Definitions" in the Mullica Township Municipal Code is amended to include cannabis within the definition of SMOKING.

SMOKING
The inhaling, exhaling, burning or possession of any lighted cigar, cigarette, pipe, or other combustible tobacco product in any manner or in any form. This shall include e-cigarettes or any other type of artificial cigarettes that produce emissions; and shall also include cannabis smoking products.

SECTION 3. Repealer Clause
All Ordinances or parts of Ordinances inconsistent with this Ordinance are hereby repealed to the extent of such inconsistencies.

SECTION 4. Savings Clause

All other provisions of any other Chapter of the Mullica Township Administrative Code which are not affected by this Amendment shall remain in full force and effect.

SECTION 5. Severability
If any portion of this Article is adjudged unconstitutional or invalid by a court of competent jurisdiction, such judgment shall not affect or invalidate the remainder of this article but shall be confined in its effect to the provision directly involved in the controversy in which such judgment shall have been rendered.

SECTION 6. Effective Date.
This Ordinance shall take effect upon final passage and publication in accordance with New Jersey law.

First Reading: May 25, 2021

Adopted: June 8, 2021

_____
: KRISTI HANSELMANN, MAYOR

ATTEST:

_____
KIMBERLY JOHNSON, TOWNSHIP CLERK

TOWNSHIP OF MULLICA
RESOLUTION NO. 123-2021

THANK YOU LAURA ENGELMANN

WHEREAS, Laura Engelmann has tendered her resignation as a member of Mullica Township's Municipal Alliance; and

WHEREAS, the Governing Body of the Township of Mullica expresses their appreciation to Laura Engelmann for voluntary service to the community.

NOW, THEREFORE, BE IT RESOLVED, the Governing Body of the Township of Mullica extend to Laura Engelmann their best wishes for many years of happiness during her new endeavors.

Adopted: May 25, 2021

_____
KRISTI HANSELMANN
MAYOR

ATTEST:

_____
KIMBERLY JOHNSON
TOWN SHIP CLERK

TOWNSHIP OF MULLICA
RESOLUTION NO. 124-2021

INFORMATION TECHNOLOGY POLICY

WHEREAS, The Township of Mullica is a member of the Atlantic County Municipal Joint Insurance Fund (JIF) and the Municipal Excess Liability Joint Insurance Fund (MEL); and

WHEREAS, the Township of Mullica wishes to comply with various practices suggested by the JIF and MEL in regards to their cyber insurance policy; and

WHEREAS, by adopting such practices will enable the municipality to a claim reimbursement or a paid insurance deductible in the event there is a claim; and

WHEREAS, the Township of Mullica through the JIF will provide Township employees annual training in email and website malware identification, password construction, identifying security incidents and social engineering attacks.

WHEREAS, the Township of Mullica adopted the Cyber Incident Response Plan by Resolution No. 92-2018 and wishes to amend said

NOW, THEREOFRE, BE IT RSOLVED, the Governing Body of the Township of Mullica hereby adopts the attached Master Technology Practice Policy and implements the attached cybersecurity incident response plan.

BE IT FURTHER RESOLVED, the attached policies will be filed in the Office of the Township Clerk and a certified copy shall be forwarded to the JIF.

Adopted: May 25, 2021

_____
KRISTI HANSELMANN
MAYOR

ATTEST:

_____
KIMBERLY JOHNSON
TOWNSHIP CLERK

Township of Mullica

Master
Technology Policy

Version 2.2

MEL Cyber Risk Management Program

Adopted: May 25, 2021

P

1. Policy Statement

The Technology Policy defines the technology security practices necessary to ensure the security of the member's technology systems and the information it stores, processes, and/or transmits.

2. Reason for the Policy

We act as the custodian of a wealth of sensitive information relating to the services we provide and the constituents we serve. We also rely on technology for much of our daily operations. Accordingly, an appropriate set of security measures must be implemented to guard against unauthorized access to, alteration, disclosure, or destruction of this information and/or the technology systems that store, process, or transmit the information.

This policy affirms our commitment to technology security by specifying the policies and standards necessary to achieve our security objectives, including compliance with all Federal and State requirements, as well as the Municipal Excess Liability Joint Insurance Fund's (MEL) Minimum Technology Proficiency Standards.

3. Scope

All technology systems and users are expected to comply with this policy.

4. Tier 1 Operational Policies

The member shall implement practices and policies that meet or exceed the MEL's requirements at a minimum.

4.1. Information Backup Policy

Objective:

The objective of the Information Backup Policy is to ensure all data is regularly "backed up" and available when needed in the event of an incident (e.g., ransomware, flood, fire, etc.). If the network is virtual, meaning no local data is stored on devices, the requirement to backup devices does not apply.

Requirements:

a) Use of standardized system images or virtualized desktops
b) A back-up of applications, operating systems and network configuration software must always be available
c) Daily incremental backups with a minimum of 14 days of versioning on off-network device of all data
d) Weekly, off-network, full back-up of all data
e) All backups are spot-checked monthly
f) Third-party and cloud-based application data must also be backed-up to the same standards

4.2. Patch Management Policy

Objective:

The objective of the Patch Management Policy is to ensure all systems and applications are patched on a timely basis. Outdated and/or unsupported operating systems/applications shall not be used.

Requirements:

Patch all operating systems, applications, and infrastructure equipment with latest versions.

a. Use automatic updating where practicable, particularly as related to security patches.

b. All security and critical updates and patches are installed as soon as possible following release. Following are examples:

- Microsoft products (Windows, Desktops, Servers, Office, SQL Data Bases, Outlook, etc.)
- Search engines (Google, Firefox, Microsoft Edge, Bing, etc.)
- Technical infrastructure equipment that requires regular security updates (switches, firewalls, routers, etc.)
- Third-Party applications (finance, animal license, construction, code enforcement, etc.)

c. Annually review all non-standard applications for possible replacement/upgrade

4.3. Defensive Software Policy

Objective:

The objective of the Defensive Software Policy is to ensure all systems are protected by software that minimizes the likelihood of an attack by malicious individuals and/or malware that can compromise the confidentiality, integrity and availability of that system or information.

Requirements:

a. Antivirus and firewalls are enabled for all desktops and laptops
b. Antispam and antivirus filters are enabled for all email servers
c. Firewalls, switches, routers, and any interconnecting devices must ensure unused or non-active ports are closed
d. Antivirus and antimalware must be enabled for network servers that connect to the internet
e. Firewall rules and policies need to be reviewed at least twice per year
f. All Microsoft Office applications automatically open all downloaded files in "Protected Mode"

4.4. Security Awareness Training Policy

Objective:

The objective of the Security Awareness Training Policy is to ensure all personnel with access to the member's technology assets receive appropriate cyber awareness education to reduce the likelihood of a cyber incident by understanding potential cyber threats.

Requirements:

All personnel with access to the member's technology assets shall receive annual training of at least one hour that includes malware identification (email and websites), password construction, identifying security incidents, and social engineering.

4.5. Password Policy

Objective:

The objective of the Password Policy is to ensure that users construct passwords that minimize the likelihood of unauthorized access to the member's data and technology systems.

Requirements:

There are two options for compliance: 1) Follow the set of standards below; or 2) Follow the NIST Password Standards 800-63B (03/02/2020 Updates).

Option 1

1- **Change Frequency**
   a. Network users' passwords are updated every three (3) months.
2- **Construction**
   b. Passwords must be unique from passwords used on all other programs, websites, devices, etc., both personal and work.
   c. Passwords must be a minimum of ten (10) characters.
   d. Sequential or repetitive characters of more than two in succession are not to be permitted.
      - Example: "123", "AAA", etc.
   e. Commonly used passwords are not to be permitted.
      - Example, "password", "123456789", "qwerty", "abc123", etc.
      - Full lists of commonly used passwords can be found in various cybersecurity reports.
   f. Context-specific words are not to be permitted.
      - Example, the name of the application or website being logged into.
3- **Previously Breached Passwords**
   The member shall implement a process for identifying breaches containing user email addresses and utilize a breach corpus search for breached passwords, and such passwords shall be updated and not used again.
4- **Failed Login Lockout**
   The user account shall be locked out after five (5) failed attempts for a period of no less than 30 minutes. In lieu of a timed lockout, the member may utilize a positive identification process to unlock the account.

Option 2 (NIST)

1- **Failed Login Lockout**
   a. Limit the number of failed authentication attempts
2- **Password**
   a. Suggest users use "memorized secrets" instead of passwords

b. Memorized Secrets are secret values intended to be chosen and memorized by the user; something you know

3- **Length**
   a. 8 characters minimum to at least 64 characters maximum
4- **Change**
   a. Only change if there is evidence of compromise
5- **Screening**
   a. Screen passwords against a list of known compromised passwords
6- **Hints**
   a. Disable password hints and knowledge-based security questions
7- **Composition Minimums**
   a. Skip character composition rules
8- **Composition Restrictions**
   a. Do not allow
      i. Dictionary words
      ii. Repetitive or sequential characters
      iii. Context-specific words (i.e. service name or username)
9- **Copy & Paste**
   a. Allow copying and pasting passwords from a password manager
10- **Other Characters**
   a. Allow ASCII and UNICODE, including emojis

4.6. Email Warning Policy

Objective:

The objective of the Email Warning Policy is to reduce spoofing emails and social engineering emails by identifying when emails are coming from outside the organization.

Requirements:

Example of email warning label:

> **CAUTION:**
>
> **This email originated from outside of our email domain. Do not click on links or open attachments unless you recognize the sender and know the content is safe. If unsure, do not reply to this email and call the sender directly.**

4.7. Cyber Incident Response Plan

Objective:

The objective of the Incident Response Plan is to define the methods for identifying, tracking, and responding to technology security incidents.

Requirements:

Please refer to the Incident Response Plan. V2.1

4.8. Technology Practice Policy

Objective:

The objective of the Technology Practice Policy is to ensure management/governing bodies adopt a Technology Practices Policy that includes all the subject items outlined in the MEL Cyber Risk Management Program.

Requirements:

This document shall serve as the Technology Practice Policy.

4.9. Government Cybersecurity Membership Policy

Objective:

The objective of the Government Cybersecurity Membership policy is to ensure the member stays current with cyber threat notifications and relevant information. Both required below are FREE.

Requirements:

The member shall register and become a member of New Jersey Cybersecurity Communications Integration Cell (NJCCIC) and Multi-State Information Sharing and Analysis Center (MS-ISAC).

New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) - https://www.cyber.nj.gov/

The New Jersey Cybersecurity and Communications Integration Cell is the state's one-stop shop for cybersecurity information sharing, threat intelligence, and incident reporting. Acting in a cyber fusion center capacity, the NJCCIC is a component organization within the New Jersey Office of Homeland Security and Preparedness.

The NJCCIC works to make New Jersey more resilient to cyberattacks by promoting statewide awareness of cyber threats and widespread adoption of best practices. We provide a wide array of cybersecurity services, including the development and distribution of cyber alerts and advisories, cyber tips, and best practices for effectively managing cyber risk. Other services include threat briefings, risk assessments, incident response support, and training.

Multi-State Information Sharing & Analysis Center (MS-ISAC) - https://www.cisecurity.org/ms-isac/

The mission of MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal, and territorial governments through focused cyber threat prevention, protection, response, and recovery.

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing technology systems and data. We lead a global community of technology professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

5. Tier 2 Operational Policies

5.1. Server Security Policy

Objective:

The objective of the Server Security Policy is to prevent unauthorized physical access, damage, and interference to the member's server(s) and network equipment.

Requirements:

The member's servers and network equipment shall be protected by physical barriers with restricted access controls and must not be in common public areas. The servers and network equipment may be stored in an enclosed cabinet, data closet, or office with secure entries.

5.2. Access Privilege Controls Policy

Objective:

The objective of the Access Privilege Control Policy is to control access to all technology digital assets. Access to all technology shall be controlled by role-based access controls.

Requirements:

a. System and Network administrative rights are to be limited to those who are authorized to make changes to the systems, computers, and network.
b. Network and system access to file and folders are granted based on the individual's job function and level of responsibility.
c. Access rights need to be reviewed and updated upon any personnel change. Exiting employees' access must be revoked immediately upon separation.
d. A review process is to be implemented to ensure access rights are up to date. Minimal review frequency is six (6) months.

5.3. Technology Support Policy

Objective:

The objective of the Technology Support Policy is to ensure the member has the technical support expertise and structure in place to effectively mitigate and triage technology and cyber related issues.

Requirements:

Technical support can be provided by a qualified and experienced employee or vendor.

5.4. System and Event Logging Policy

Objective:

The objective of the Logging Policy is to ensure system activities, information security events, and system utilization and performance are captured.

Requirements:

The member shall use the following Microsoft logs (or similar for other operating systems) to monitor system activities, information security events, and system utilization and performance.

a- System
b- Application
c- Security

Note: There are numerous free and for-cost log management tools on the market.

5.5. Protected Information Policy

Objective:

The objective of the Protected Information Policy is to ensure all digital files and data containing sensitive information, Personally Identifiable Information (PII), and Protected Health Information (PHI) are protected in accordance with statutory, regulatory, and contractual requirements.

Requirements:

All digital documents containing Personally Identifiable Information (PII), Protected Health Information (PHI) and documents deemed by the member as sensitive shall be encrypted.

5.6. Remote Access Policy

Objective:

The purpose of Remote Access Policy is to secure remote access connectivity into the member's network using a Virtual Private Network (VPN).

Requirements:

The member shall deploy a Virtual Private Network (VPN) for those who need to remotely access the member's network. Only approved users, third-parties, vendors, and contractors may utilize the VPN service to connect to the member's network. VPN profiles shall be created upon request from the relevant

department head, approving authorities, or designated sponsor.

Using Personal Devices:

The following requirements only apply to those approved users, third-party, vendor or contractors who use their personal devices to access the member's network.

- All personal devices must be up to date with all applicable operating systems, security patches and virus/malware protection software.
- Users with remote access privileges shall ensure their remote access connection is used explicitly for member work and used in a manner consistent with their on-site connection to the member's network.
- Personal equipment shall not be used to connect to the member network unless authorized and approved in writing by someone in senior management charged with approving cybersecurity changes.
- VPN users are automatically disconnected from the member network after thirty (30) minutes of inactivity. The user must then logon again to re-authenticate in order to reconnect to the network.
- All personal devices are required to use a password to protect from tampering using the same standards and requirements as the member's equipment.
- The member shall not allow remote users to save any data to their personal devices (i.e. member can utilize Content Access Controls or a Cloud Access Security Broker).

5.7. Leadership Expertise Policy

Objective:

The objective of the Leadership Expertise Policy is to ensure the member's senior management has access to resources with expertise in their respective fields to support technology decision making, such as risk assessments, planning, budgeting, etc.

Requirements:

The member's senior management shall have access to resources with expertise in their respective fields leveraging their technology support and the JIF's or MEL's available resources.

5.8. Technology Business Continuity Plan Policy

Objective:

The objective of the Technology Business Continuity Plan Policy is to ensure the member is prepared and can effectively recover from a disruption in service, including cyber breaches, denial of service or ransomware attacks, and be able to restore continuity of operations.

Requirements:

The Emergency Management/Continuity of Government (CoG) plan shall include a Technology Business Continuity Plan as part of its Disaster Recovery section.

When developing a Technology Business Continuity Plan the member shall consider the following:

Recovery Strategies

5.1. Identify all operational functions

5.2. Identify key support personnel and communications plan

5.3. Prioritize based on Recovery Time Objectives (RTOs)

5.4. Consider and accommodate the following impacts:

- ✓ Loss of Computing (Systems and Data)
- ✓ Loss of Telecommunications
- ✓ Loss of Personnel
- ✓ Denial of Physical Access
- ✓ Critical vendors' services

5.9. Banking Control Policy

Objective:

The objective of the Banking Control Policy is to prevent or reduce fraudulent banking transactions.

Requirements:

The member shall implement internal controls to minimize fraudulent banking transactions. The following are required:

- Use Multi-Factor Authentication when accessing the bank's system and making financial transactions, where available.
- Establish procedures requiring multiple approvals for request to change banking information.
- Establish procedures requiring multiple approvals and source verification for financial transaction requests over $5,000.

Technology Support Guidelines

Industry Standard Certifications	Certifications required based on support role					
	Help Desk Support	PC / Printer Repair	Server Repair & Support	System Administration	Network & Infrastructure Support	Information Security
HDI technical support professional certification	✓					
CompTIA IT Fundamentals (ITF+)	✓	✓				
CompTIA A+	✓	✓	✓	✓		
CompTIA Network +			✓	✓	✓	
CompTIA Server +			✓	✓	✓	
CompTIA Security +			●	●	✓	✓
MCSE			●	✓	●	●
CCNA					✓	✓
CISSP						✓
CEH						✓

- Certifications marked with a bullet are not required but good to have depending on customer needs.

CompTIA IT Fundamentals (ITF+)	Entry level certification focusing on essential IT skills and knowledge such as the functions and features of common operating systems, establishing network connectivity, security best practices and how to identify common software applications.
CompTIA A+	The certification focuses on validating nine major IT skills, including hardware, operating systems, software troubleshooting, networking, hardware and network troubleshooting, security, mobile devices, virtualization and cloud computing and operational procedures.
CompTIA Network +	The certification focuses on configuring, managing, and maintaining network devices, implementing, and designing functional networks, network troubleshooting and network security.
CompTIA Server +	The certification focuses on knowledge of server hardware and technology as well as troubleshooting and repairing server issues, including disaster recovery.
CompTIA Security +	The certification focuses on threats, attacks and vulnerabilities, risk management, architecture and design, technology and tools, cryptography and PKI and identity and access management.
MCSE Microsoft Certified Systems Engineer	Though Microsoft has retired the MCSE certification program as of June 30, 2020, the certification focuses on designing, managing, and supporting Windows products and architecture.
CCNA Cisco Certified Network Associate	The CCNA certification focuses network fundamentals, network access, IP connectivity, IP services, security fundamentals and automation and programmability.
CISSP Certified Information Systems Security Professional	The CISSP certification focuses on critical security issues, including risk management, cloud computing, application development security, mobile security, etc.
Certified Ethical Hacker	The CEH certification specializes in penetration testing, vulnerability testing, and cyber forensics analysis.

Cyber Incident Response Plan

Township of Mullica

Adopted: May 25, 2021

Table of Contents

1. Policy Statement

The Incident Response Plan defines our methods for identifying, tracking, and responding to technology-based security incidents.

2. Reason for the Policy

The Incident Response Plan is established to assist in protecting the integrity, availability, and confidentiality of technology and assist in complying with statutory, regulatory and contractual obligations.

Responding quickly and effectively to an Incident is critical to minimizing the spread of the Incident and/or the business, financial, legal, and/or reputational impact. Incident Response generally includes the following phases:

- Detection, Reporting, and Analysis.
- Legal.
- Forensics.
- Containment, Eradication, and Recovery.
- Other Responses (i.e. Public Relations).
- Post-Incident Review.

3. Scope

This plan governs incidents that have a significant negative impact on information technology systems and/or sensitive information (hereinafter, "Incidents"). Incidents can include denial of service, malware, ransomware, and/or phishing attacks that can significantly impact operations and/or result in the unintended disclosure of sensitive data (e.g., constituent data, Protected Health Information, Personally Identifiable Information, credit card data, and law enforcement records).

Minor events (e.g., routine detection, and remediation of a virus, a minor infraction of a security policy, or other similar issues that have little impact on day-to-day business operations) are not considered an Incident under this policy.

4. Incident Identification

For cyber insurance purposes, a security incident is an event that is a: cyber security breach, or cyber extortion threat, or data breach.

4.1 Cyber Extortion Threat

A threat against a network to:

1. Disrupt operations.
2. Alter, damage, or destroy data stored on the network.
3. Use the network to generate and transmit malware to third parties.
4. Deface the member's website.
5. Access personally identifiable information, protected health information, or confidential business information stored on the network; made by a person or group, whether acting alone,

or in collusion with others, demanding payment, or a series of payments in consideration for the elimination, mitigation, or removal of the threat.

4.2 Cyber Security Breach

Any unauthorized access to, use, or misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, viruses, worms, Trojan horses, spyware, adware, zero-day attack, hacker attack, or denial of service attack.

4.3 Data Breach

The actual or reasonably suspected theft, loss, or unauthorized acquisition of data that has or may compromise the security, confidentiality and/or integrity of personally identifiable information, protected health information, or confidential business information.

Other cyber security incidents include:

- Attempts from unauthorized sources to access systems or data.
- Unplanned disruption to a service or denial of a service.
- Unauthorized processing or storage of data.
- Unauthorized changes to system hardware, access rights, firmware, or software.
- Presence of a malicious application, such as ransomware, or a virus.
- Presence of unexpected/unusual programs.

5. Designation of an Incident Response Manager

5.1 Responsibilities

- Michael Irwin is the Incident Response Manager that is responsible for determining whether an event, or a series of security events, is declared an Incident. Dawn Stollenwerk is the back-up Incident Response Manager.
- The Incident Response Manager is responsible for ensuring that this policy is followed.
- The Incident Response Manager is responsible for establishing an Incident Response Team to support the execution of this plan.
- The Incident Response Team is tasked with executing this plan in accordance with and at the direction of the Incident Response Manager.
- Michael Irwin and Dawn Stollenwerk are responsible for ensuring that end-users have sufficient knowledge to recognize a potential security Incident and report it in accordance with this plan.
- Employees are responsible to report potential security incidents in a timely manner and provide any requires support during plan execution.

6. Incident Response Team and Notification

Establish an incident response team to be able to quickly respond to cyber security incidents, and a team broad enough to gather the needed resources and make the appropriate decisions to resolve the incident. Such team shall include the following.

Title / Position	Name	Telephone #
Chief of Police	Brian Zeck	609-561-7600 ext 131
General Counsel	James Franklin	609- 601-6600
Incident Response Manager	Michael Irwin	609-418-9939
Back-up Incident Response Manager	Dawn Stollenwerk	609-561-7070 ext 111
JIF Risk Management Consultant	Gene Siracusa	609- 646-1000 ext 714
JIF Claims Administrator	Kimberly Johnson	609-561-7070 ext 114
Technology Support Contact	Michael Irwin	609-418-9939
AXA XL Data Breach Hotline		855-566-4724

Please verify with your breach advisor/counsel that their firm will be handling the required breach notifications including, but potentially not limited to, those agencies listed below.

IC3	FBI Internet Crime Complaint Center: https://www.ic3.gov/
NJ Cybersecurity and Communications Integration Cell (NJCCIC)	Incident Reporting: https://www.cyber.nj.gov/report 609-963-6900 x7865

7. Incident Response Phases

7.1 Detection, Reporting, & Analysis

1. If a user, employee, contractor, or vendor observes a potential security event they should notify the Incident Response Manager immediately. If the Incident Response Manager is not available, the events should be immediately reported to the back-up incidence response manager or the Municipal Clerk.
2. The Incident Response Manager is responsible for communicating the Incident, its severity, and the action plan to the highest-ranking administrative official.
3. If the Incident Response Manager or the back-up incident response managerl are not available, a user should isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. If isolating the machine from the network is not possible then unplug the machine from its power source.
4. If you have determined or suspect that the Incident is a cyber security breach, cyber extortion threat, or data breach (*see Definitions Related to Cyber Liability Insurance – Section 4 of this document*) proceed to Step 5. If not, proceed to Step 6.
5. For a cyber security breach, please follow this process:

If the AXA XL Data Breach Hotline does not answer, leave a message with your contact information. Do not delay in calling the Hotline. When they respond, follow their instructions. They will refer the matter to a "breach advisor/counsel" (an attorney experienced in cybersecurity incidents) who will

coordinate the response. The Breach Counsel will gather information about the Incident and work with you to determine an action plan.

The Incident Response Manager should follow the advice from the Breach Counsel until the issue is resolved.

6. *If the Incident is determined not to be a cyber security breach, cyber extortion threat, or data breach*, the Incident Response Manager should work with the Incident Response Team to assess the Incident, develop a plan to contain the Incident, and ensure the plan is communicated to and approved by the highest-ranking administrative official.
7. The Incident Response Manager should ensure that all actions are documented as they are taken and that the highest-ranking administrative official, Incident Response Team, and outside support are regularly updated.

7.2 Containment, Eradication, & Recovery

Containment is the act of limiting the scope and magnitude of the attack as quickly as possible. Containment has two goals: preventing data of note from being exfiltrated and preventing the attacker from causing further damage.

Immediate triage:

1. Immediately contact technology expert to report the event and follow their instructions. It is now the responsibility of technology expert to notify management of the incident and to execute the security incident response plan.

2. If technology expert is not available, isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. DO NOT TURN OFF DEVICE OR REMOVE POWER SOURCE unless instructed by technology expert.

3. Incident response team assembles and assesses if the incident is a cyber security breach, cyber extortion threat, or data breach: If it is, or if there is any question the incident may or may not be one, management contacts their JIF Claims Administrator to advise them of the incident and management (or technology support) will call the Cyber Insurer Hotline. Work with the breach coach and the other partners they suggest to help resolve the incident.

4. Document all actions as they are taken.

Eradication is the removal of malicious code, accounts, or inappropriate access. Eradication also includes repairing vulnerabilities that may have been the root cause of the compromise. A complete reinstallation of the OS and applications is preferred.

Recovery allows business processes affected by the Incident to recover and resume operations. It generally includes:

- Reinstall and patch the OS and applications.
- Change all user and system credentials.
- Restore data to the system.
- Return affected systems to an operationally ready state.
- Confirm that the affected systems are functioning normally.

7.3 Forensics

Security incidents of a significant magnitude may require that a forensics investigation take place. Once that need has been established all additional investigation/containment activities need to be directed and/or performed by a forensics specialist to ensure that the evidence and chain of custody is maintained. The highest-ranking administrative official, in consultation with the Incident Response Manager and/or XL Caitlin will advise if engaging a forensics firm is required.

7.4 Post-Incident Review

To improve the Incident Response processes and identify recurring issues each Incident should be reviewed and formally reported on. The report should include:

- Information about the Incident type
- A description of how the Incident was discovered.
- Information about the systems that were affected.
- Information about who was responsible for the system and its data.
- A description of what caused the Incident.
- A description of the response to the Incident and whether it was effective.
- A timeline of events, from detection to Incident closure
- Recommendations to prevent future Incidents.
- A discussion of lessons learned that will improve future responses.

8. Periodic Review

This policy and associated subordinate procedures will be reviewed at least annually by the Incident Response Manager to adjust processes considering new risks and security best practices. Material changes in this policy should be approved by the governing body of the municipality.

9. Special Situations/Exceptions

Any personally owned devices, such as PDAs, phones, wireless devices, or other electronic devices which have been used to access organizational data and are determined to be relevant to an Incident, may be subject to retention until the Incident has been eradicated.

TOWNSHIP OF MULLICA
RESOLUTION NO. 125-2021

REFUND OF TAXES

WHEREAS, it has been brought to the attention of the Township Committee that the below amounts for 2020/2021 property taxes are to be refunded to Cape Atlantic Title.

YEAR	QTR.	BLOCK / LOT
2020	3rd & 4th	10023 / 11
2021	1st	10023 / 11

Total Amount Of Refund: $4,347.42

NOW, THEREFORE, BE IT RESOLVED, by the Township Committee of the Township of Mullica refund erroneously made taxes as noted above for the above referenced Block and Lots and refunded to Cape Atlantic Title.

Adopted: May 25, 2021

_____
KRISIT HANSELMANN
MAYOR

ATTEST:

_____
KIMBERLY JOHNSON
TOWNSHIP CLERK

P.O. Type: All
Range: First to Last
Format: Condensed

Open: N Paid: N Void: N
Rcvd: Y Held: Y Aprv: N
Bid: Y State: Y Other: Y Exempt: Y

Vendor # / PO #	Name / PO Date	Description	Status	Amount	Void Amount	Contract	PO Type
01356	APPLIED CONCEPTS, INC.						
21-00258	04/09/21	radar for new car	Open	2,292.00	0.00		
01982	ATLANTIC CITY ELECTRIC						
21-00330	04/30/21	APRIL SERVICES	Open	3,319.09	0.00		
04674	BUTTERHOF'S FARM & HOME SUPPLY						
21-00316	04/16/21	CHAIN/SUPPLIES	Open	37.22	0.00		
04677	BUSINESS CARDS TOMORROW						
21-00329	05/04/21	WHITE ENVELOPES	Open	100.00	0.00		
05271	CASA PAYROLL SERVICES, LCC						
21-00249	03/31/21	APRIL-MAY BLANKET VOUCHER	Open	173.75	0.00		B
08237	DIMEGLIO SEPTIC, INC.						
21-00358	04/30/21	APRIL SERVICEES	Open	65.00	0.00		
08242	DELL USA L.P						
21-00188	03/03/21	LAPTOP	Open	929.43	0.00		
09247	DORAN ENGINEERING						
21-00331	05/05/21	DARMSTADT #2 THRU 4/28/21	Open	3,000.00	0.00	C9000016	C
15672	G & P FLOOR MAINTENANCE						
21-00338	04/30/21	APRIL SERVICES	Open	425.00	0.00		
17284	GPANJ						
21-00359	05/17/21	2021 DUES - QPA	Open	100.00	0.00		
26498	CRYSTAL SPRINGS						
21-00355	04/01/21	APRIL SERVICES	Open	117.44	0.00		
32657	TOWNSHIP OF GALLOWAY						
21-00285	04/13/21	2ND QUARTER DISPATCH SERVICES	Open	53,726.89	0.00		
33469	THE HAMMONTON GAZETTE						
21-00346	05/01/21	MAY PUBLICATIONS	Open	413.23	0.00		
34299	VERIZON						
21-00333	04/21/21	APRIL SERVICES	Open	30.77	0.00		
21-00348	04/28/21	APRIL SERVICES	Open	30.77	0.00		
				61.54			
34302	VERIZON WIRELESS						
21-00371	05/06/21	MAY SERVICES	Open	380.28	0.00		
39876	PITNEY BOWES						
21-00349	05/15/21	POSTAGE	Open	2,000.00	0.00		

Vendor # / PO #	Name / PO Date / Description	Status	Amount	Void Amount	Contract	PO Type
48709	STAPLES CONTRACT & COMMERCIAL					
21-00332	04/20/21 OFFICE SUPPLIES - PD	Open	56.97	0.00		
21-00361	04/30/21 POLICE OFFICE SUPPLIES	Open	108.24	0.00		
21-00362	04/30/21 OFFICE SUPPLIES	Open	348.28	0.00		
			513.49			
50158	THE PRESS OF ATLANTIC CITY					
21-00354	03/31/21 MARCH-MAY PUBLICATIONS	Open	433.92	0.00		
53833	DRAGER, INC.					
21-00339	04/01/21 ALCOTEST SOLUTION	Open	180.00	0.00		
54678	VAL-U AUTO PARTS					
21-00366	03/01/21 MARCH/APRIL PURCHASES	Open	2,225.20	0.00		
55474	VITAL COMMUNICATIONS, INC.					
21-00334	04/23/21 MAY SERVICES	Open	210.00	0.00		
63968	LAWROW ELECTRIC & PLUMBING SUP					
21-00271	03/10/21 DPW SUPPLIES	Open	8.65	0.00		
64006	FLEISHMAN DANIELS LAW OFFICES					
20-00782	11/30/20 MUNICIPAL COMPLEX PROJECT	Open	2,812.60	0.00		B
64010	ACTION UNIFORM CO.					
21-00360	05/01/21 PROMOTIONAL ITEMS	Open	1,600.00	0.00		
AMAZ0005	AMAZON					
21-00367	04/01/21 POLICE OFFICE SUPPLIES	Open	387.29	0.00		
ATLAN020	ATLANTIC TACTICAL					
20-00801	12/14/20 SIG SAUERS, ETC. PD	Open	239.88	0.00		
ATLAN035	ATLANTICARE PHYSICIANS GROUP					
21-00351	04/28/21 ANNUAL HEARING TEST- DPW	Open	170.00	0.00		
BURKE005	BURKE MOTOR GROUP INC.					
21-00336	04/02/21 APRIL PURCHASES	Open	471.84	0.00		
CO002	ATLANTIC COUNTY UTILITES AUTH.					
21-00340	05/05/21 April services	Open	29,180.58	0.00	C9000015	C
21-00341	04/01/21 APRIL RECYCLING	Open	6,878.48	0.00		
			36,059.06			
COMCA005	COMCAST					
21-00365	04/28/21 APRIL SERVICES	Open	15.02	0.00		
21-00368	05/01/21 MAY SERVICES	Open	429.61	0.00		
			444.63			
COMCA010	COMCAST BUSINESS					
21-00364	05/01/21 may services	Open	396.92	0.00		

Vendor # / PO #	Name / PO Date	Description	Status	Amount	Void Amount	Contract	PO Type
GOODY005	GOODYEAR AUTO SERVICE CENTER						
21-00335	04/28/21	S22 PARTS	Open	258.02	0.00		
HYWAY005	HY-WAY MOTORS, INC.						
21-00337	04/05/21	APRIL SERVICES	Open	1,906.10	0.00	C2100001	C
MAJES005	MAJESTIC OIL COMPANY, INC.						
21-00262	04/01/21	2ND QUARTER PURCHASES	Open	793.35	0.00		B
MUNIC005	MUNICIPAL CAPITAL FINANCE						
20-00545	07/22/20	SAVIN MP3055SP COPIER LEASE	Open	88.08	0.00		B
NJ017	TREASURER, STATE OF NEW JERSEY						
21-00357	04/21/21	2021 RECYCLING COMPLIANCE FEE	Open	1,015.00	0.00		
NJ019	NJ STATE HEALTH BENEFITS FUND						
21-00342	05/01/21	MAY PREMIUM	Open	67,081.95	0.00		
NJ020	NJ DEPT OF HEALTH & SENIOR SRV						
21-00347	04/30/21	APRIL STATE FEES	Open	172.20	0.00		
SAMUE005	SAMUEL CURCIO, JR., LLC						
21-00283	04/01/21	APRIL SERVICES	Open	550.00	0.00		
SCIUL005	SCIULLO ENGINEERING SERVICES						
21-00352	03/29/21	RIVER ROAD SERVICES THRU 5/2	Open	180.00	0.00		
21-00353	05/17/21	DARMSTADT #1 THRU 5/2/21	Open	202.18	0.00	C9000003	C
				382.18			
TWP16	GREATER EGG HARBOR REGIONAL						
21-00061	01/19/21	LEVY INSTALLMENT MAY	Open	283,764.90	0.00		
TWP17	MULLICA TWP BOARD OF EDUCATION						
21-00066	01/20/21	TAX LEVY INSTALLMENT - MAY	Open	401,328.00	0.00		
YOUNG010	YOUNGBLOOD FRANKLIN SAMPOLI &						
21-00363	04/01/21	APRIL SERVICES	Open	7,495.00	0.00		

Total Purchase Orders: 49 Total P.O. Line Items: 0 Total List Amount: 878,129.13 Total Void Amount: 0.00

Totals by Year-Fund Fund Description	Fund	Budget Rcvd	Budget Held	Budget Total	Revenue Total	G/L Total	Total
Current Fund	0-01	5,432.56	0.00	5,432.56	0.00	0.00	5,432.56
Current Fund	1-01	869,322.19	0.00	869,322.19	0.00	0.00	869,322.19
Capital Fund	C-04	3,202.18	0.00	3,202.18	0.00	0.00	3,202.18
Trust Fund	T-03	172.20	0.00	172.20	0.00	0.00	172.20
Total Of All Funds:		878,129.13	0.00	878,129.13	0.00	0.00	878,129.13