South Whidbey Parks & Recreation District
Tuesday, June 18, 2024 6:00pm
Regular Board Meeting
Parks District Headquarters
5475 Maxwelton Rd., Langley WA
Online attendance is available. Visit swparks.org/about/meetingsminutes or email director@swparks.org for more information.

Regular Board Meeting

I. **Call to Order**

II. **Public Comment**

III. **Approval of Minutes (05/15/2024)**

IV. **Treasurer's Report**
- A. **Summary Treasurer's Report**
- B. **Voucher List Approval**

V. **Staff Report**

VI. **Committee and Community Meeting Reports**
Where applicable, committee reports may move to unfinished or new business.

VII. **Unfinished Business**
- A. **Comprehensive Plan Programs**
  1. **Lakes Property**
     a) **Dock at Deer Lake**
  2. **Aquatic Recreation Center**
     a) **Communication with the Community**

VIII. **New Business**
- A. **Authorization of submitting Washington State grants. Resolution 2024-03 to submit to Land and Water Conservation Fund Grant and Resolution 2024-04 to submit to Washington Wildlife and Recreation Coalition.**
- B. **Field Policy Updates for Policy Manual- Discussion and possible motion to approve**
- C. **Cyber Security Check Up with the State of Washington- Results**
- D. **Sports Complex Asphalt Bid Approval**
- E. **Resolution 2024-05 to close the Property Fund**
- F. **Resolution 2024-06 to re-open the Construction Fund**

IX. **Adjournment**

South Whidbey Parks and Recreation District
May 15, 2024 – Regular Meeting Minutes

DRAFT

Regular Meeting Minutes

I. Call to Order

Commissioners Present: Jennifer Cox, Erik Jokinen, Krista Loercher and Matt Simms.
Staff Present: Skye Dunn, Tom Fallon, Carrie Monforte and Brian Tomisser

Jennifer called the Regular Meeting to order at 6:04 p.m. The attendance sheet is attached for permanent records only.

II. Public Comment

No public comment.

III. Approval of Minutes

The minutes of the Regular Meeting on 04/17/2024, were unanimously approved in a motion made by Erik.

IV. Treasurer's Report/Voucher List Approval

A. Summary Treasurer's Report

Matt reviewed the treasurer's report with the board.

B. Voucher List Approval

In a motion made by Matt, the Board unanimously approved the Maintenance and Operations Fund Vouchers #12840 through #12909 in the amount of $99,747.91, and Capital Fund Voucher #47 in the amount of $110.00.

V. Staff Report (To be attached for permanent records)

Brian reviewed the Staff Report with the commissioners. Matt provided an update on current grant applications for LCWF and WWRP Local Parks to cover aspects of the South Whidbey Aquatic Recreation Center (SWARC).

A. Recreation Seasonal Report

Skye provided a presentation on upcoming summer recreation program offerings.

VI. Committee and Community Meeting Reports

Jennifer reported on the property at the intersection of Maxwelton & SR525 which is pending sale. Krista reported takeaways from a Sno-Isle Libraries presentation regarding disabled hikers. Krista suggested looking at District offerings and improving communication to the public about accessibility at existing parks and facilities.
Matt provided an update on the solar plus storage grant contract and propane generators.

VII. Unfinished Business

A. Comprehensive Plan Programs

1. Lakes Property

a) Dock at Deer Lake
Brian reported that the WA Department of Fish and Wildlife indicated that dock project is going through a Hydraulic Project Approval process.

2. Campground
a) Island County Permit Update
Brian provided updates from a meeting with Island County regarding the permit for the campground including a need for an updated site plan. Once the County has the updated site plan, the District would receive a detailed 'to do' list. The County indicated that permits are good for 5 years, with extensions possible. The campground committee will meet June 10th to discuss this further.

3. Aquatic Recreation Center
a) Incentive for SWPAF Pool Donors
Brian stated that he was approached regarding incentives for individuals making monthly donations to support swimming programs, including a possible tour of the facility.

B. Authorization for ARC to proceed with their work on the Aquatic Recreation Center
Brian and the board discussed the projected timeline for the receipt of bond funds and options to authorize proceeding with the SWPARC project.

Matt made a motion to authorize ARC Architects up to an additional $100,000 to complete design changes in the Design Development phase and the motion was unanimously approved.

VIII. New Business

A. Policy Manual Updates – Sections 1, 2, 3 and 4
Brian presented an update to the previous draft of sections 1, 2, 3 and 4 of the District Policy Manual and the board suggested final edits.

Krista made a motion to approve the updates of section 1,2,3,4 in the policy manual, including the addition of a minimum 30-minute lunch in section 4.40, and a correction referring to the including policy manual in section 4.58.

B. Diamond Dust Infield Mix Purchase – Discussion/Decision
Staff discussed a budgeted purchase of sole source product of Diamond Dust Infield Mix.

Matt made a motion to authorize the expenditure not to exceed $8,000 for Diamond Dust Infield Mix, and it was unanimously approved.

C. Additional Service Aquatic Recreation Center, Water Supply to Site - Possible Action
Brian displayed an add service request from ARC to bring water service to the SWARC site.

Matt made a motion to approve an add service request from ARC to bring water service to the SWARC site in an amount not to exceed $135,525, and it was unanimously approved.

IX. Adjournment

There being no further business, the meeting was adjourned at 8:30 p.m.

South Whidbey Parks & Recreation Dist

5475 Maxwelton Road
Langley, WA 98260

Purchases [Vendor Detail]

June 2024

6/12/2024
012:04:58 PM

ID#	Date	Item/Acct	Description	Amount
All Whidbey Topsoil & Construction				4000830
00012910	6/4/2024	6-2583	Lawn Mix	$54.40
			All Whidbey Topsoil & Construction Total:	$54.40
ATCO International				4001400 R1
00012911	6/4/2024	6-2585	Bee Spray	$168.00
			ATCO International Total:	$168.00
Bank Account Fees				*None
00012947	6/6/2024	6-1660	Bank Account Fees for Direct De	$100.00
			Bank Account Fees Total:	$100.00
Bank Card Fees				*None
00012946	6/6/2024	6-1660	Credit Card Transaction Fees	$1,012.68
			Bank Card Fees Total:	$1,012.68
Caldwell, Chancelor				4000384
00012935	6/6/2024	1-1120	Wages from 05/16/24 to 05/31	$1,605.06
			Caldwell, Chancelor Total:	$1,605.06
Carter, Austin L.				5007725
00012936	6/6/2024	1-1120	Wages from 05/16/24 to 05/31	$2,462.01
			Carter, Austin L. Total:	$2,462.01
Conn, Britt				9603320
00012912	6/4/2024	4-4264	Swim Lesson Refund	$117.00
			Conn, Britt Total:	$117.00
Diamond Rentals				4000539
00012913	6/4/2024	6-2690	Porta Potty Service	$81.75
			Diamond Rentals Total:	$81.75
DRS - Deferred Compensation Program				4000537 R3
00012943	6/6/2024	2-1435	DCP Employer Portion	$1,570.58
00012943	6/6/2024	2-1485	DCP Employee Portion	$1,698.85
			DRS - Deferred Compensation Program Total:	$3,269.43
Dunn, Skye P				4000982
00012939	6/6/2024	1-1120	Wages from 06/01/24 to 06/15	$1,961.47
			Dunn, Skye P Total:	$1,961.47
EFTPS				*None
00012945	6/6/2024	2-1430	FMed/FSoc Payable	$3,233.97
			EFTPS Total:	$3,233.97
Enduris				4000552
00012914	6/4/2024	6-1426	New mower addition to insuranc	$203.00
			Enduris Total:	$203.00
Fallon, Thomas R.				5001388
00012940	6/6/2024	1-1120	Wages from 06/01/24 to 06/15	$3,050.60

South Whidbey Parks & Recreation Dist

Purchases [Vendor Detail]

June 2024

ID#	Date	Item/Acct	Description	Amount
Fallon, Thomas R.				5001388
			Fallon, Thomas R. Total:	$3,050.60
Great America Financial Services				4000584
00012915	6/4/2024	6-1530	Copier lease & copies	$232.45
			Great America Financial Services Total:	$232.45
Handran, Kathleen M				*None
00012932	6/6/2024	1-1120	Wages from 05/16/24 to 05/31	$328.05
			Handran, Kathleen M Total:	$328.05
Horizon Distributors, Inc.				4000603 R3
00012916	6/4/2024	6-2582	Irregation & Plumbing Supplies	$172.40
			Horizon Distributors, Inc. Total:	$172.40
Island Disposal, Inc.				4000643
00012917	6/4/2024	6-2647	Inv # 8106312S144 Refuse remo	$181.33
00012917	6/4/2024	6-2647	Inv # 8106209S144 Refuse remo	$362.64
			Island Disposal, Inc. Total:	$543.97
Les Schwab Tire Center				4000527 R2
00012918	6/4/2024	6-2881	Vehicle/mach in-shop repair	$111.95
			Les Schwab Tire Center Total:	$111.95
Lubchuk, Shelby L				*None
00012937	6/6/2024	1-1120	Wages from 05/16/24 to 05/31	$1,817.47
			Lubchuk, Shelby L Total:	$1,817.47
Lyon, Julianne				4001499
00012919	6/4/2024	6-4296	Groove Fitness	$598.40
			Lyon, Julianne Total:	$598.40
Monforte, Carrie E.				4000837
00012941	6/6/2024	1-1120	Wages from 06/01/24 to 06/15	$2,471.67
			Monforte, Carrie E. Total:	$2,471.67
Myres, Jacob				*None
00012938	6/6/2024	1-1120	Wages from 05/16/24 to 05/31	$1,817.47
			Myres, Jacob Total:	$1,817.47
Nelson, Colette				9602664
00012920	6/4/2024	4-4282	Magic Camp Refund	$202.50
00012920	6/4/2024	4-4118	Youth Sailing Camp Refund	$202.50
			Nelson, Colette Total:	$405.00
NW Natural Water Services, LLC				4000873 R2
00012921	6/4/2024	6-2680	Water Testing	$276.29
			NW Natural Water Services, LLC Total:	$276.29
Puget Sound Energy				4000705 R1
00012922	6/4/2024	6-2649	Acct.# 300000003172 Dated 06	$303.91
00012922	6/4/2024	6-2649	Acct# 200010294276 Dated 06	$47.54
			Puget Sound Energy Total:	$351.45

South Whidbey Parks & Recreation Dist

Purchases [Vendor Detail]

June 2024

ID#	Date	Item/Acct	Description	Amount
Raymond, Marcus				5010240
00012933	6/6/2024	1-1120	Wages from 05/16/24 to 05/31	$231.74
			Raymond, Marcus Total:	$231.74
RnR Cleaning - Royce Wellman				4001171
00012923	6/4/2024	6-1535	Monthly Janitoria Service - Office	$451.19
			RnR Cleaning - Royce Wellman Total:	$451.19
Sachs, Kathleen				*None
00012934	6/6/2024	1-1120	Wages from 05/16/24 to 05/31	$573.39
			Sachs, Kathleen Total:	$573.39
Sebo's Do-It Center				4000731
00012927	6/4/2024	6-2585	Park Building Maintenance/Janit	$58.72
			Sebo's Do-It Center Total:	$58.72
Skewes, Janet				4001512
00012924	6/4/2024	6-4291	Dog Sports Class	$480.00
			Skewes, Janet Total:	$480.00
Sound Safety Products, Inc				5003242
00012925	6/4/2024	6-2436	Safety Gear	$150.49
			Sound Safety Products, Inc Total:	$150.49
South Whidbey School District #206				4000751 R1
00012926	6/4/2024	6-2434	Inv # Parks-2024-08 Fuel	$1,034.57
			South Whidbey School District #206 Total:	$1,034.57
Tomisser, Brian				4001346 R1
00012942	6/6/2024	1-1120	Wages from 06/01/24 to 06/15	$3,724.59
			Tomisser, Brian Total:	$3,724.59
VISA - Heritage Bank				4000793 R4
00012928	6/4/2024	6-1549	Amazon - moving boxes	$21.21
00012928	6/4/2024	6-1549	Amazon - moving boxes	$32.63
00012928	6/4/2024	6-4534	Amazon - signage/program equi	$180.56
00012928	6/4/2024	6-2905		$180.56
00012928	6/4/2024	6-2880	O'Reilly Auto Parts - Vehicle/Mac	$83.48
00012928	6/4/2024	6-1552	NRPA Membership - conferences	$695.00
00012928	6/4/2024	6-1530	Crystal Springs - office supplies	$211.63
00012928	6/4/2024	6-1530	Amazon - office supplies	$38.71
00012928	6/4/2024	6-4191	Amazon - Triathlon	$176.22
00012928	6/4/2024	6-2649	Pugest Sound Energy - electrical	$82.66
00012928	6/4/2024	6-1530	Amazon - Credit for Office Suppl	($38.71)
			VISA - Heritage Bank Total:	$1,663.95
WA State Dept of Retirement				4000531
00012944	6/6/2024	6-1205	PERS Employer Portion	$2,414.14
00012944	6/6/2024	2-1480	PERS Employee Portion	$1,672.60
			WA State Dept of Retirement Total:	$4,086.74
Welever, Nathan E				4001447 R1
00012929	6/4/2024	6-4296	April Island Mat Club Wrestling	$368.00
			Welever, Nathan E Total:	$368.00

South Whidbey Parks & Recreation Dist

Purchases [Vendor Detail]

June 2024

ID#	Date	Item/Acct	Description	Amount
Whidbey Telecom				4000828
00012930	6/4/2024	6-2650	Alarm Monitoring	$81.61
00012930	6/4/2024	6-1541	Telephone, Web Housing, Intern	$364.81
			Whidbey Telecom Total:	$446.42
Zep Manufacturing Company				4000833
00012931	6/4/2024	6-2585	Park Building Maintenance/Janit	$97.05
			Zep Manufacturing Company Total:	$97.05
			Grand Total:	$39,812.79

South Whidbey Parks & Recreation Dist

Profit & Loss [Budget Analysis]

January 2024-May 2024

6/13/2024
2:29:31 PM

		Selected Period	Budgeted	$ Difference
4-0000	Income			
4-1000	Misc. Revenues			
4-1002	Advertising	$50.00	$0.00	$50.00
	Total Misc. Revenues	$50.00	$0.00	$50.00
4-2000	Taxes			
4-2110	Property taxes - M & O	$907,521.10	$913,880.00	($6,358.90)
4-2200	Timber excise taxes	$401.95	$0.00	$401.95
	Total Taxes	$907,923.05	$913,880.00	($5,956.95)
4-4100	Recreation Programs			
4-4110	Adult Sports			
4-4113	Adult Basketball	$0.00	$400.00	($400.00)
4-4114	Adult Softball League	$3,500.00	$2,000.00	$1,500.00
4-4117	Adult Volleyball	$645.00	$0.00	$645.00
4-4118	Adult Sailing	$5,725.00	$4,500.00	$1,225.00
4-4119	Pickleball	$17,921.00	$11,450.00	$6,471.00
4-4120	Adult Soccer/Futsal	$0.00	$800.00	($800.00)
4-4129	Miscellaneous Adult Sports	$0.00	$435.00	($435.00)
4-4130	Youth Sports			
4-4131	Tennis Classes	$3,510.00	$4,100.00	($590.00)
4-4132	Youth Basketball	$8,243.50	$4,000.00	$4,243.50
4-4135	Falcon Programs	$1,290.00	$800.00	$490.00
4-4136	Youth Soccer/Futsal	$1,495.00	$0.00	$1,495.00
4-4190	Special Event - Sports			
4-4191	Triathlon	$11,910.00	$15,090.00	($3,180.00)
4-4192	Chum Run	$0.00	$1,500.00	($1,500.00)
4-4199	Polar Bear Dive Revenue	$1,600.00	$750.00	$850.00
4-4200	Misc. Programs			
4-4210	Adult Misc. Programs			
4-4219	Adult General Program	$0.00	$500.00	($500.00)
4-4250	Youth Misc. Programs			
4-4252	Cheer	$406.00	$0.00	$406.00
4-4260	Other Youth Programs	$6,555.00	$8,250.00	($1,695.00)
4-4263	Archery	($69.00)	$0.00	($69.00)
4-4264	Aquatics	$31,434.00	$31,525.00	($91.00)
4-4265	Skimboarding	$2,000.00	$2,300.00	($300.00)
4-4266	Youth Sailing	$12,292.50	$9,500.00	$2,792.50
4-4267	Paddle Sports	$2,402.50	$3,170.00	($767.50)
4-4282	Cultural Youth Camps	$8,790.00	$12,000.00	($3,210.00)
4-4290	Special Events			
4-4291	Dog Classes	$10,260.00	$7,500.00	$2,760.00
4-4292	Concerts and Movies	$2,250.00	$1,500.00	$750.00
4-4296	New Program Directions	$3,505.00	$1,200.00	$2,305.00
	Total Recreation Programs	$135,665.50	$123,270.00	$12,395.50
4-6000	SWARC Revenue			
4-6010	SWARC DOC Grant Funding	$352,380.74	$273,200.00	$79,180.74
	Total SWARC Revenue	$352,380.74	$273,200.00	$79,180.74
4-8000	Other Revenue			
4-8003	Park Facility Rental	$3,605.00	$2,300.00	$1,305.00
4-8005	Other Revenue	$817.46	$90.00	$727.46
4-8006	Interest from M & O	$4,082.96	$1,562.50	$2,520.46
4-8008	Interest from Reserve Fund	$4,304.51	$1,355.00	$2,949.51
4-8009	Reserve Fund - Transfers In	$151,169.00	$151,169.00	$0.00
4-8010	Transfer from Reserve to M&O	$31,623.00	$31,623.00	$0.00
4-8100	Scholarship Donations	$40.00	$30.00	$10.00
	Total Other Revenue	$195,641.93	$188,129.50	$7,512.43
	Total Income	$1,591,661.22	$1,498,479.50	$93,181.72
5-0000	Cost of Sales			
	Gross Profit	$1,591,661.22	$1,498,479.50	$93,181.72
6-0000	Expenses			
6-1000	Administration			
6-1010	Wages - Director	$50,578.80	$50,578.75	$0.05
6-1012	Wages - Administrator	$34,463.50	$34,855.00	($391.50)
6-1014	Wages - Admin Assistant 2	$8,376.40	$15,195.00	($6,818.60)

South Whidbey Parks & Recreation Dist

Profit & Loss [Budget Analysis]

January 2024-May 2024

6/13/2024
2:29:32 PM

		Selected Period	Budgeted	$ Difference
6-1201	FICA District's Share	$4,400.97	$5,840.00	($1,439.03)
6-1202	WA State Unemployment Ins	$930.70	$1,350.00	($419.30)
6-1203	Labor & Industries Ins	$6,527.24	$11,600.00	($5,072.76)
6-1204	Health Ins	$41,143.59	$51,250.00	($10,106.41)
6-1205	Retirement-PERS	$21,343.50	$22,460.00	($1,116.50)
6-1206	LTD/AD&D/Life Ins	$2,252.33	$1,895.00	$357.33
6-1207	Dental Insurance	$3,414.40	$4,165.00	($750.60)
6-1208	B&O Tax	$534.99	$800.00	($265.01)
6-1209	DCP Employer Expense	$14,055.26	$14,975.00	($919.74)
6-1210	Family & Medical Leave	$1,598.30	$2,600.00	($1,001.70)
6-1301	Accounting Service	$15,174.90	$20,358.00	($5,183.10)
6-1302	Legal Service	$0.00	$800.00	($800.00)
6-1303	Professional Service	$109.69	$0.00	$109.69
6-1427	State Audit	$15,877.45	$8,000.00	$7,877.45
6-1428	Election Costs	$9,106.35	$9,106.00	$0.35
6-1429	Building Lease	$2,198.90	$2,500.00	($301.10)
6-1530	Office Supplies	$2,170.45	$2,294.00	($123.55)
6-1531	Dues & Publications	$330.00	$400.00	($70.00)
6-1532	Print & Advertising	$50.00	$600.00	($550.00)
6-1533	Staff Clothing	$79.34	$125.00	($45.66)
6-1535	Contracted Services	$2,255.95	$2,500.00	($244.05)
6-1540	Postage	$68.00	$150.00	($82.00)
6-1541	Telephone	$3,193.14	$3,750.00	($556.86)
6-1543	Propane	$2,252.68	$2,125.00	$127.68
6-1550	Travel & Vehicle Allowance	$25.00	$250.00	($225.00)
6-1552	Conferences & Training	($159.00)	$1,250.00	($1,409.00)
6-1660	Misc Fees & Charges	$1,460.66	$3,125.00	($1,664.34)
6-1690	Computer Equip & Supplies	$2,965.73	$4,585.00	($1,619.27)
6-1691	Office Equipment	$191.42	$950.00	($758.58)
6-1692	Volunteer Recognition	$0.00	$100.00	($100.00)
	Total Administration	$246,970.64	$280,531.75	($33,561.11)
6-2000	Maintenance			
6-2001	Maintenance Wages			
6-2010	Maintenance Supervisor	$41,700.77	$42,175.00	($474.23)
6-2012	Maintenance Wages - PT	$68,460.23	$84,338.00	($15,877.77)
	Total Maintenance Wages	$110,161.00	$126,513.00	($16,352.00)
6-2200	Maintenance O & M			
6-2434	Gas & Lube Products	$2,664.73	$5,000.00	($2,335.27)
6-2436	Safety Gear	$784.51	$400.00	$384.51
6-2550	Travel & Vehicle Allowance	$111.00	$335.00	($224.00)
6-2581	Garden Maint & Hort	$1,588.50	$500.00	$1,088.50
6-2582	Irrg & Plumb Supplies	$2,881.33	$1,400.00	$1,481.33
6-2583	Sport Field Supplies	$0.00	$8,250.00	($8,250.00)
6-2584	Misc Bld Repair	$1,895.64	$2,750.00	($854.36)
6-2585	Park Bld Maint/Jan Supp	$3,588.26	$3,125.00	$463.26
6-2586	Fertilizer & Turf	$13,621.76	$7,000.00	$6,621.76
6-2610	Playground Maintenance	$357.36	$600.00	($242.64)
6-2647	Refuse Removal	$2,807.93	$2,875.00	($67.07)
6-2649	Electrical Utilities	$6,458.09	$5,000.00	$1,458.09
6-2650	Alarm System Monitoring	$244.85	$718.75	($473.90)
6-2670	Road & Trail Maintenance	$2,814.61	$3,000.00	($185.39)
6-2680	Water System Maintenance	$945.60	$1,260.00	($314.40)
6-2690	Septic	$1,979.25	$3,250.00	($1,270.75)
6-2760	Contract Services	$0.00	$150.00	($150.00)
6-2880	Veh & Mach Repair/Parts	$7,090.24	$3,250.00	$3,840.24
6-2881	Veh/Mach In-shop Repair	$1,756.95	$5,835.00	($4,078.05)
6-2901	Misc Equip Rental	$0.00	$150.00	($150.00)
6-2902	Misc. Equipment/Tools	$755.92	$500.00	$255.92
6-2905	Sign/Art Work Maintenance	$129.82	$800.00	($670.18)
6-2906	Trustland Trails	$0.00	$600.00	($600.00)
6-2907	Lakes	$509.73	$200.00	$309.73
	Total Maintenance O & M	$52,986.08	$56,948.75	($3,962.67)
	Total Maintenance	$163,147.08	$183,461.75	($20,314.67)
6-2950	Interest Expense	$0.00	$40.00	($40.00)
6-3000	Capital Equipment/Projects			
6-3001	Projects/Equipment	$0.00	$235,000.00	($235,000.00)

South Whidbey Parks & Recreation Dist

Profit & Loss [Budget Analysis]

January 2024-May 2024

6/13/2024
2:29:33 PM

		Selected Period	Budgeted	$ Difference
6-3002	Pickleball Court Expense	$2,689.00	$62,750.00	($60,061.00)
	Total Capital Equipment/Projects	$2,689.00	$297,750.00	($295,061.00)
6-4000	Programs			
6-4009	Program Wages			
6-4010	Programs Wages - FT	$29,671.88	$27,905.00	$1,766.88
6-4012	Programs Wages - PT	$7,000.51	$6,250.00	$750.51
6-4100	Recreation Programs			
6-4110	Adult Sports			
6-4114	Adult Softball League	$983.41	$200.00	$783.41
6-4119	Pickleball	$271.07	$4,600.00	($4,328.93)
6-4130	Youth Sports			
6-4131	Tennis Classes	$20.00	$0.00	$20.00
6-4132	Youth Basketball	$4,557.37	$8,100.00	($3,542.63)
6-4190	Special Event - Sports			
6-4191	Triathlon	$741.16	$900.00	($158.84)
6-4199	Polar Bear Dive Expense	$0.00	$1,200.00	($1,200.00)
6-4200	Misc. Programs			
6-4210	Adult Misc. Programs			
6-4216	Fitness	$20.00	$0.00	$20.00
6-4250	Youth Misc. Programs			
6-4252	Cheer	$2,138.40	$2,300.00	($161.60)
6-4290	Special Events			
6-4291	Dog Classes	$9,136.00	$8,000.00	$1,136.00
6-4296	New Program Directions	$1,272.57	$1,200.00	$72.57
6-4500	Misc. Program Expenses			
6-4532	Print & Advertising	$673.44	$1,050.00	($376.56)
6-4534	Program Equipment & Supplies	$0.00	$875.00	($875.00)
6-4570	Unfunded Scholarships	$50.00	$125.00	($75.00)
	Total Programs	$56,535.81	$62,705.00	($6,169.19)
6-6000	SWARC Expenses			
6-6010	SWARC Architectural Services	$234,998.90	$197,200.00	$37,798.90
6-6020	SWARC Legal Services	$1,719.50	$0.00	$1,719.50
6-8000	Miscellaneous Costs			
6-8006	Investment Fee Operations Fund	$0.00	$75.00	($75.00)
6-8008	Investment Fees Reserve Fund	$0.00	$75.00	($75.00)
6-8009	Tsf to Reserve Fund from M&O	$151,169.00	$151,169.00	$0.00
6-8010	Reserve Fund - Transfers Out	$31,623.00	$31,623.00	$0.00
	Total Miscellaneous Costs	$182,792.00	$182,942.00	($150.00)
	Total Expenses	$888,852.93	$1,204,630.50	($315,777.57)
	Net Profit / (Loss)	$702,808.29	$293,849.00	$408,959.29

Account Transactions

1/1/2024 To 5/31/2024

ID#	Src	Date	Memo/Payee	Debit	Credit	Job No.
2-2100 Mortgage Loans						
00012737	PJ	3/20/2024	Purchase; Heritage Bank - Oly	$14,779.00		
				$14,779.00	$0.00	
2-2200 Bank Loans						
00012676	PJ	2/20/2024	Purchase; Heritage Bank - Sea	$4,715.33		
00012874	PJ	5/16/2024	Purchase; Heritage Bank - Sea	$4,715.33		
				$9,430.66	$0.00	

Fund Balances

Fund Balances as of May 31, 2024

M&O	$1,267,257.25
Reserve	$505,664.61
Capital (Maxwelton Trails Bond)	$59,530.42
Property (Campground)	$189,834.64
Bond - (Park Improvement Bond)	$727,345.08
TOTAL	$ 2,749,632.00

South Whidbey
Parks & Recreation District

Memo

To: Board of Commissioners
From: Staff
Date: 06/18/2024
Re: Staff Report for June 2024

Recreation/Programs

- Chum Run looks like it is going to tentatively be at Fort Casey this fall. Date TBD
- Six softball teams signed up, down two from last summer.
- Ballroom dance classes have begun this month.
- Camps begin June 22nd. Numbers overall for summer programs look good.
- We hired Christine Silvernail as our new Recreation and Event Coordinator. This is a seasonal position.
- Disc Golf clinic happening today (June 18th) at the Sports Complex

Facilities and Grounds

- No report this month

Director's Items

- 35 residents attended the public meeting June 12 at the South Whidbey Community Center gymnasium to discuss the Outdoor Pickleball Court design. Received good feedback and architect is now incorporating the feedback into one updated design.
- The District received a AA- bond rating, which is very good and should result in a good rate for our bonds. Bond pricing is scheduled for June 26th and we anticipate receiving the $15 million in July.
- Sections 5 and 6 of the Policy Manual have been moved to the July agenda for review. The delay is due to the extensive work required to prepare for the Bond Rating.
- We were told by Island County last week that their deadline for us to receive our monthly treasure report is by the 10th business day of the month, not the 10th of the month, as we had previously understood. It will be a consideration for Board meeting dates going forward, especially in months where the deadline to receive the report is 48 hours or less before the Board meeting. There are five months this year where that occurs.

Upcoming Events

07/17/24 Regular Board Meeting 6:00 pm

Memo

South Whidbey
Parks & Recreation District

To: Board of Commissioners
From: Brian Tomisser
Date: 06/18/2024
Re: Comprehensive Plan Programs

Lakes Property

- I reached out to the Department of Fish and Wildlife early last week to see if there was an update on the SEPA work being done at Deer Lake.

Campground

- Campground committee met on June 10th. Any relevant information will be shared during the Committee and Community Meetings Reports.

Aquatic Recreation Center

- Tom and I met on site with Davido and ARC to discuss water access to the site of the Aquatic Recreation Center. One item they are looking into is whether it would be efficient and cost effective to use the previous well that is closed for the primary well for the Center.
- Now that we have re-activated ARC, I have asked Paul Curtis to start attending Board meetings quarterly to give a short update and answer any questions you may have. He will do this virtually and probably starting in August or September.
- We had a couple of community members reach out and ask about how to receive updates on the project. We have added a link to our homepage and created a spot where I will create regular updates on the project.

WASHINGTON STATE
Recreation and
Conservation Office

Applicant Resolution/Authorization

Organization Name (sponsor) South Whidbey Parks and Recreation District

Resolution No. or Document Name Resolution 2024-03

Project(s) Number(s), and Name(s) 24-2007 Dev, South Whidbey Aquatic Recreation Center LWCF

This resolution/authorization authorizes the person(s) identified below (in Section 2) to act as the authorized representative/agent on behalf of our organization and to legally bind our organization with respect to the above Project(s) for which we seek grant funding assistance managed through the Recreation and Conservation Office (Office).

WHEREAS, grant assistance is requested by our organization to aid in financing the cost of the Project(s) referenced above;

NOW, THEREFORE, BE IT RESOLVED that:

1. Our organization has applied for or intends to apply for funding assistance managed by the Office for the above "Project(s)."

2. Our organization authorizes the following persons or persons holding specified titles/positions (and subsequent holders of those titles/positions) to execute the following documents binding our organization on the above projects:

Grant Document	Name of Signatory or Title of Person Authorized to Sign
Grant application (submission thereof)	Matthew Simms, Commissioner
Project contact (day-to-day administering of the grant and communicating with the RCO)	Brian Tomisser, Executive Director Carrie Monforte, Business Manager
RCO Grant Agreement (Agreement)	Brian Tomisser, Executive Director
Agreement amendments	Brian Tomisser, Executive Director
Authorizing property and real estate documents (Notice of Grant, Deed of Right or Assignment of Rights if applicable). These are items that are typical recorded on the property with the county.	Brian Tomisser, Executive Director

The above persons are considered an "authorized representative(s)/agent(s)" for purposes of the documents indicated. Our organization shall comply with a request from the RCO to provide documentation of persons who may be authorized to execute documents related to the grant.

3. Our organization has reviewed the sample RCO Grant Agreement on the Recreation and Conservation Office's WEB SITE at: https://rco.wa.gov/wp-content/uploads/2019/06/SampleProjAgreement.pdf. We understand and acknowledge that if offered an agreement to sign in the future, it will contain an indemnification and legal venue stipulation and other terms and conditions substantially in the form contained in the sample Agreement and that such terms and conditions of any signed Agreement shall be legally binding on the sponsor if our representative/agent enters into an Agreement on our behalf. The Office reserves the right to revise the Agreement prior to execution.

4. Our organization acknowledges and warrants, after conferring with its legal counsel, that its authorized representative(s)/agent(s) have full legal authority to act and sign on behalf of the organization for their assigned role/document.

5. Grant assistance is contingent on a signed Agreement. Entering into any Agreement with the Office is purely voluntary on our part.

6. Our organization understands that grant policies and requirements vary depending on the grant program applied to, the grant program and source of funding in the Agreement, the characteristics of the project, and the characteristics of our organization.

7. Our organization further understands that prior to our authorized representative(s)/agent(s) executing any of the documents listed above, the RCO may make revisions to its sample Agreement and that such revisions could include the indemnification and the legal venue stipulation. Our organization accepts the legal obligation that we shall, prior to execution of the Agreement(s), confer with our authorized representative(s)/agent(s) as to any revisions to the project Agreement from that of the sample Agreement. We also acknowledge and accept that if our authorized representative(s)/agent(s) executes the Agreement(s) with any such revisions, all terms and conditions of the executed Agreement shall be conclusively deemed to be executed with our authorization.

8. Any grant assistance received will be used for only direct eligible and allowable costs that are reasonable and necessary to implement the project(s) referenced above.

9. [for Recreation and Conservation Funding Board Grant Programs Only] If match is required for the grant, we understand our organization must certify the availability of match at least one month before funding approval. In addition, our organization understands it is responsible for supporting all non-cash matching share commitments to this project should they not materialize.

10. Our organization acknowledges that if it receives grant funds managed by the Office, the Office will pay us on only a reimbursement basis. We understand reimbursement basis means that we will only request payment from the Office after we incur grant eligible and allowable costs and pay them. The Office may also determine an amount of retainage and hold that amount until all project deliverables, grant reports, or other responsibilities are complete.

11. **[for Acquisition Projects Only]** Our organization acknowledges that any property acquired with grant assistance must be dedicated for the purposes of the grant in perpetuity unless otherwise agreed to in writing by our organization and the Office. We agree to dedicate the property in a signed "Deed of Right" for fee acquisitions, or an "Assignment of Rights" for other than fee acquisitions (which documents will be based upon the Office's standard versions of those documents), to be recorded on the title of the property with the county auditor. Our organization acknowledges that any property

acquired in fee title must be immediately made available to the public unless otherwise provided for in policy, the Agreement, or authorized in writing by the Office Director.

12. **[for Development, Renovation, Enhancement, and Restoration Projects Only–If our organization owns the project property]** Our organization acknowledges that any property owned by our organization that is developed, renovated, enhanced, or restored with grant assistance must be dedicated for the purpose of the grant in perpetuity unless otherwise allowed by grant program policy, or Office in writing and per the Agreement or an amendment thereto.

13. **[for Development, Renovation, Enhancement, and Restoration Projects Only–If your organization DOES NOT own the property]** Our organization acknowledges that any property not owned by our organization that is developed, renovated, enhanced, or restored with grant assistance must be dedicated for the purpose of the grant as required by grant program policies unless otherwise provided for per the Agreement or an amendment thereto.

14. **[Only for Projects located in Water Resources Inventory Areas 1-19 that are applying for funds from the Critical Habitat, Natural Areas, State Lands Restoration and Enhancement, Riparian Protection, or Urban Wildlife Habitat grant categories; Aquatic Lands Enhancement Account; or the Puget Sound Acquisition and Restoration program, or a Salmon Recovery Funding Board approved grant]** Our organization certifies the following: the Project does not conflict with the Puget Sound Action Agenda developed by the Puget Sound Partnership under RCW 90.71.310.

15. This resolution/authorization is deemed to be part of the formal grant application to the Office.

16. Our organization warrants and certifies that this resolution/authorization was properly and lawfully adopted following the requirements of our organization and applicable laws and policies and that our organization has full legal authority to commit our organization to the warranties, certifications, promises and obligations set forth herein.

This resolution/authorization is signed and approved on behalf of the resolving body of our organization by the following authorized member(s):

Signed _____

Title Chair, Board of Commissioners Date June 18, 2024

On File at: South Whidbey Parks & Recreation District 5475 Maxwelton Rd., Langley, WA 98260

This Applicant Resolution/Authorization was adopted by our organization during the meeting held: (Local Governments and Nonprofit Organizations Only):

Location: 5475 Maxwelton Road, Langley, WA 98260 Date: 06/18/2024

Washington State Attorney General's Office

Approved as to form Brian Fuller 2/13/2020
Assistant Attorney General *Date*

You may reproduce the above language in your own format; however, text may not change.

WASHINGTON STATE
Recreation and
Conservation Office

Applicant Resolution/Authorization

Organization Name (sponsor) South Whidbey Parks and Recreation District

Resolution No. or Document Name Resolution 2024-04

Project(s) Number(s), and Name(s) 24-2008 Dev, South Whidbey Aquatic Rec. Center WWRP

This resolution/authorization authorizes the person(s) identified below (in Section 2) to act as the authorized representative/agent on behalf of our organization and to legally bind our organization with respect to the above Project(s) for which we seek grant funding assistance managed through the Recreation and Conservation Office (Office).

WHEREAS, grant assistance is requested by our organization to aid in financing the cost of the Project(s) referenced above;

NOW, THEREFORE, BE IT RESOLVED that:

1. Our organization has applied for or intends to apply for funding assistance managed by the Office for the above "Project(s)."

2. Our organization authorizes the following persons or persons holding specified titles/positions (and subsequent holders of those titles/positions) to execute the following documents binding our organization on the above projects:

Grant Document	Name of Signatory or Title of Person Authorized to Sign
Grant application (submission thereof)	Matthew Simms, Commissioner
Project contact (day-to-day administering of the grant and communicating with the RCO)	Brian Tomisser, Executive Director Carrie Monforte, Business Manager
RCO Grant Agreement (Agreement)	Brian Tomisser, Executive Director
Agreement amendments	Brian Tomisser, Executive Director
Authorizing property and real estate documents (Notice of Grant, Deed of Right or Assignment of Rights if applicable). These are items that are typical recorded on the property with the county.	Brian Tomisser, Executive Director

The above persons are considered an "authorized representative(s)/agent(s)" for purposes of the documents indicated. Our organization shall comply with a request from the RCO to provide documentation of persons who may be authorized to execute documents related to the grant.

3. Our organization has reviewed the sample RCO Grant Agreement on the Recreation and Conservation Office's WEB SITE at: https://rco.wa.gov/wp-content/uploads/2019/06/SampleProjAgreement.pdf. We understand and acknowledge that if offered an agreement to sign in the future, it will contain an indemnification and legal venue stipulation and other terms and conditions substantially in the form contained in the sample Agreement and that such terms and conditions of any signed Agreement shall be legally binding on the sponsor if our representative/agent enters into an Agreement on our behalf. The Office reserves the right to revise the Agreement prior to execution.

4. Our organization acknowledges and warrants, after conferring with its legal counsel, that its authorized representative(s)/agent(s) have full legal authority to act and sign on behalf of the organization for their assigned role/document.

5. Grant assistance is contingent on a signed Agreement. Entering into any Agreement with the Office is purely voluntary on our part.

6. Our organization understands that grant policies and requirements vary depending on the grant program applied to, the grant program and source of funding in the Agreement, the characteristics of the project, and the characteristics of our organization.

7. Our organization further understands that prior to our authorized representative(s)/agent(s) executing any of the documents listed above, the RCO may make revisions to its sample Agreement and that such revisions could include the indemnification and the legal venue stipulation. Our organization accepts the legal obligation that we shall, prior to execution of the Agreement(s), confer with our authorized representative(s)/agent(s) as to any revisions to the project Agreement from that of the sample Agreement. We also acknowledge and accept that if our authorized representative(s)/agent(s) executes the Agreement(s) with any such revisions, all terms and conditions of the executed Agreement shall be conclusively deemed to be executed with our authorization.

8. Any grant assistance received will be used for only direct eligible and allowable costs that are reasonable and necessary to implement the project(s) referenced above.

9. [for Recreation and Conservation Funding Board Grant Programs Only] If match is required for the grant, we understand our organization must certify the availability of match at least one month before funding approval. In addition, our organization understands it is responsible for supporting all non-cash matching share commitments to this project should they not materialize.

10. Our organization acknowledges that if it receives grant funds managed by the Office, the Office will pay us on only a reimbursement basis. We understand reimbursement basis means that we will only request payment from the Office after we incur grant eligible and allowable costs and pay them. The Office may also determine an amount of retainage and hold that amount until all project deliverables, grant reports, or other responsibilities are complete.

11. **[for Acquisition Projects Only]** Our organization acknowledges that any property acquired with grant assistance must be dedicated for the purposes of the grant in perpetuity unless otherwise agreed to in writing by our organization and the Office. We agree to dedicate the property in a signed "Deed of Right" for fee acquisitions, or an "Assignment of Rights" for other than fee acquisitions (which documents will be based upon the Office's standard versions of those documents), to be recorded on the title of the property with the county auditor. Our organization acknowledges that any property

acquired in fee title must be immediately made available to the public unless otherwise provided for in policy, the Agreement, or authorized in writing by the Office Director.

12. **[for Development, Renovation, Enhancement, and Restoration Projects Only–If our organization owns the project property]** Our organization acknowledges that any property owned by our organization that is developed, renovated, enhanced, or restored with grant assistance must be dedicated for the purpose of the grant in perpetuity unless otherwise allowed by grant program policy, or Office in writing and per the Agreement or an amendment thereto.

13. **[for Development, Renovation, Enhancement, and Restoration Projects Only–If your organization DOES NOT own the property]** Our organization acknowledges that any property not owned by our organization that is developed, renovated, enhanced, or restored with grant assistance must be dedicated for the purpose of the grant as required by grant program policies unless otherwise provided for per the Agreement or an amendment thereto.

14. **[Only for Projects located in Water Resources Inventory Areas 1-19 that are applying for funds from the Critical Habitat, Natural Areas, State Lands Restoration and Enhancement, Riparian Protection, or Urban Wildlife Habitat grant categories; Aquatic Lands Enhancement Account; or the Puget Sound Acquisition and Restoration program, or a Salmon Recovery Funding Board approved grant]** Our organization certifies the following: the Project does not conflict with the Puget Sound Action Agenda developed by the Puget Sound Partnership under RCW 90.71.310.

15. This resolution/authorization is deemed to be part of the formal grant application to the Office.

16. Our organization warrants and certifies that this resolution/authorization was properly and lawfully adopted following the requirements of our organization and applicable laws and policies and that our organization has full legal authority to commit our organization to the warranties, certifications, promises and obligations set forth herein.

This resolution/authorization is signed and approved on behalf of the resolving body of our organization by the following authorized member(s):

Signed _____

Title Chair, Board of Commissioners Date June 18, 2024

On File at: South Whidbey Parks & Recreation District 5475 Maxwelton Rd., Langley, WA 98260

This Applicant Resolution/Authorization was adopted by our organization during the meeting held: (Local Governments and Nonprofit Organizations Only):

Location: 5475 Maxwelton Road, Langley, WA 98260 Date: 06/18/2024

Washington State Attorney General's Office

Approved as to form Brian Faller 2/13/2020
Assistant Attorney General *Date*

You may reproduce the above language in your own format; however, text may not change.

South Whidbey
Parks & Recreation District

Memo

To: Board of Commissioners

From: Brian Tomisser, Director

Date: 06/18/2024

Re: New Field Policy

Early in the year staff noticed some issues with field use policies and our user groups and wanted to improve our policies to clarify our expectations and minimize frustration with park users. In your packet is the updated Field Policy draft for your review.

This was sent to Little Leage and the Youth Soccer Club on May 1st. They were given until May 24th to give us feedback. We received feedback from the Soccer Club that was incorporated into the updated draft.

It was then given to the Field Committee, Erik and Matt, for their input.

Staff recommend that you approve the new Field Policy as written and that it be added into our Policy Manual, under section 3.03.06, the 'Field Use' section.

Field Policy Draft- Addendum to Policy Manual section 3.03

Winter Policies

- Winter season defined as November 1 – March 1
- Mandatory pre-season meeting in November with coaches and Sponsor Organization representatives.
    - Coaches will be required to sign consent to policy form.
- Soccer teams training with full sized goals & all games default to the Elementary field as their primary field
- No games scheduled November 1-March 1 before 11:00am.
- The game schedule needs to be approved by Parks Department staff **prior** to distribution to parents.
- Fields will be closed for a minimum of 2 days following any snow accumulation that covers the field.

Select Teams

- All select teams require a separate application and will pay $50/month, paid in advance, for up to three field uses a week. This fee will not be prorated if fields are not available for the entire month.
- The applicant for the select team will be the point of contact (POC) for all communication. In most cases the POC should be the coach. If it is anyone other than the coach, preapproval is required.

General Policies

- Field decisions on location and availability made by SWPRD staff are final and not negotiable.
    - The SWPRD reserves the right to suspend field availability at any time during periods of inclement weather and for necessary field maintenance or improvement projects.
- All Sponsor Organizations must identify one or at most two representatives that communicate with SWPRD staff. If the representative(s) are unavailable, they need to appoint a temporary contact person.
- All concerns or questions initiated by coaches, parents or volunteers directed to SWPRD staff go through the Sponsor Organization representative(s) only or the SWPRD Director. With the exception of a select teams POC.
    - Field use may be revoked if there is persistent badgering, harassment, or negative communication from any volunteer or persons connected to the Sponsor Organization or person in charge of rental.
- Charges will be incurred for unauthorized or unscheduled use
    - In the event of a significant violation, access to SWPRD parks and facilities may be curtailed or restricted in accordance with the District Conduct Policy
    - Anyone who refuses to leave the park when instructed by staff may have their access to SWPRD parks and facilities terminated in accordance with the District Conduct Policy
- All fee based private instruction on the sports fields requires an application and payment.
    - If anyone accesses the on-site storage units for the purpose of unauthorized private instruction, the sponsoring organization will be notified and if that individual is associated with their association, they will be expected to address the issue and if needed revoke access from that individual.
- High school soccer teams will primarily use the elementary soccer field for practices. As a guiding principle, U14, U15 and U17 teams will be scheduled at the elementary field.
- All regular field user groups must turn in applications annually, which includes a Certificate of Insurance and confirmation that background checks have been completed on all volunteers.
- Groups of more than 10 people that meet regularly must apply for field use to the SWPRD.
- No more than 100 users in the park from one user group at a time. Scheduling should allow for gaps so that large groups are not scheduled back-to-back to prevent parking and septic issues.

- Parks staff will strive to give at least 48 hours' notice when a change or cancellation of a field occurs. There will be times when staff will give less notice due to weather or circumstances beyond their control. When this happens, staff will notify user representatives as soon as possible.

Updated 6/4/24

South Whidbey
Parks & Recreation District

Memo

To: Board of Commissioners

From: Brian Tomisser, Director

Date: 06/18/2024

Re: Cyber Security Check up

As part of our financial audit through the State of Washington, we were made aware of a free service provided to public agencies to do a 'Cyber Check Up' regarding how your organization is doing in terms of computer security. Skye and I had multiple meetings with their staff and as a result we received a list of recommendations of how we can improve our practice. A copy of their report is provided in your Board packet.

Staff have reviewed these and will be incorporating many changes. In addition, we will be creating a new portion of the policy manual regarding Cyber Security and will bring that to the Board later in 2024. The issue of a Cyber Security policy was also brought up during our bond rating process. So, adding this prior to our next bond rating in 2025, will show improvement and hopefully help our next rating.

Cyber Checkup

Results & Recommendations

South Whidbey Parks and Recreation Dist

May 21, 2024

sao.wa.gov/BeCyberSmart

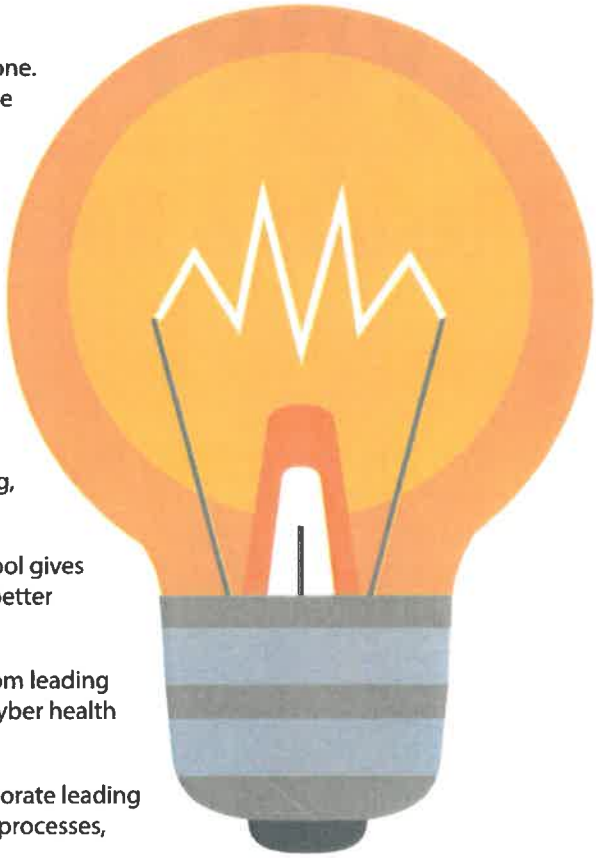
Center for Government Innovation

Introduction

About the Center for Government Innovation

The Washington State Auditor's Office created the Center for Government Innovation to help local governments solve problems and improve operations. Since its inception in 2012, the Center has provided tools, resources and training—at no cost—to thousands of government staff and elected officials across the state.

Our free tools and services include:



Lean Services – We help you improve how work gets done. Whether it's permitting, purchasing or any other area, the Center's Lean specialists can help your government optimize efficiency, quality and customer service.

Teambuilding & Leadership – We offer engaging and interactive CliftonStrengths workshops to help strengthen your team, increase trust and productivity, and promote workplace harmony and employee satisfaction.

Online Resource Library – We provide a variety of free guides, best practices and checklists to help you improve your government's internal controls, grants management, procurement practices, financial reporting, operations, cybersecurity, technology, and more.

Financial Intelligence Tool (FIT) – Our interactive FIT tool gives you the data you need to help your government make better business decisions and improve its financial health.

#BeCyberSmart – We've gathered the best practices from leading organizations to help you improve your government's cyber health with our checkups, resources and training.

Technical Advice – We offer guidance on how to incorporate leading best practices into your government's internal controls, processes, cybersecurity and more.

To learn more about how the Center can help your government, reach out to us at 564.999.0818 or email center@sao.wa.gov.

Executive Summary

Background

At South Whidbey Park District's request, SAO's Center for Government Innovation performed a high-level checkup of your organization's cyber health to identify potential gaps that could leave you vulnerable to common threats and offer recommendations for improving your defenses. Our cybersecurity specialist conducted the checkup from 5/14/24 to 5/21/24 .

Our checkups are built on the framework developed by the Center for Internet Security (CIS) in its Critical Security Controls, Version 8.0. The CIS Controls are a list of highly effective defensive actions organizations can take to improve their cybersecurity. Our checkups can complement your government's regular and ongoing cyber defenses, maintenance, and monitoring activities, but are not intended as a replacement for a detailed cybersecurity audit.

Results

During your cyber checkup, we reviewed 20 safeguards that cover seven areas of IT security.

Overall, we found that South Whidbey Parks and Recreation District has implemented a few of our recommended safeguards for a strong cybersecurity program. We encourage you to use the results of this cyber checkup to begin building a solid security foundation for your government.

The table on the following page is an overview of your checkup results. It lists each of the 20 safeguards and our assessment of whether your government has fully implemented the safeguard, has partially implemented the safeguard, or has not implemented the safeguard. In the pages following the table, we explain what each safeguard addresses, why it's important, and how it contributes to good cyber health, with resources that can help you put the safeguard into practice.

Recommendations

Based on our review, we offer recommendations to help you improve your government's cybersecurity. Each safeguard description includes our recommendations for those safeguards that need improvement or have not been implemented.

Next steps

In your final cyber checkup meeting, the Center's cybersecurity specialist will go over these results with you and answer your questions. It is up to your government to decide next steps to put any recommendations into action. If you need technical assistance in the coming months, please don't hesitate to reach out to the Center by calling 564-999-0818 or emailing center@sao.wa.gov.

South Whidbey Parks and Recreation District

Cyber Checkup Results: Overview

Area	#	Does your organization...?	Strength of your safeguard		
			Strong	Needs improvement	Not implemented
Policies & Training	1.	Establish and maintain written IT policies		✓	
	2.	Have a cybersecurity awareness program in place			✓
Incident Response	3.	Have a process for employees to report cybersecurity incidents		✓	
	4.	Designate a lead and a backup to oversee incident response and recovery		✓	
	5.	Maintain an inventory of emergency contacts and service providers			✓
Accounts & Passwords	6.	Require employees to use strong and unique passwords			✓
	7.	Encourage employees to use password managers	✓		
	8.	Restrict administrator privileges to dedicated administrator accounts			✓
	9.	Protect accounts with administrative privileges by using multifactor authentication (MFA)			✓
	10.	Require remote workers to use MFA			✓
Computers & Other Devices	11.	Install anti-virus programs on all computers	✓		
	12.	Regularly apply security patches on all computers and applications	✓		
	13.	Use only fully supported browsers and email clients			✓
	14.	Apply timed lockouts on all device screens			✓
Data Protection	15.	Encrypt data on computers or other devices containing sensitive information			✓
	16.	Back up data regularly and automatically	✓		
	17.	Block unnecessary email attachments	✓		
Network	18.	Maintain firewalls on all computers and devices		✓	
	19.	Use DNS filtering services to block access to malicious domains			✓
Credit Cards	20.	Meet PCI DSS requirements for credit cards	✓		

Policies & Training

Safeguard 1: Establish and maintain written IT policies

About this safeguard

IT policies set the rules and procedures for how your staff or contractors should use IT resources within your government. Policies should cover everything from email usage and security processes to software and hardware inventory management and data retention standards. Policies should be written down to avoid misunderstandings and provide continuity in case of staff turnover.

Why this safeguard is important

Written and approved IT policies help organizations protect their data and other valuable assets. Policies work together with technical security controls to protect confidential information from unauthorized access, corruption, and loss. Documented IT policies also set your government's expectations for how employees use the IT system and can help them avoid making a mistake that could increase your risk of a cyberattack.

What we observed during the checkup

Your organization has some written IT policies, but more are needed

Our recommendations

IT policies are the foundation of almost all controls reviewed in a cyber checkup. We recommend you strengthen your existing policies, and write new ones to close gaps. Your policies don't have to be complicated or overly technical. In fact, if you want your employees to read and apply them, you should make them easy to read and understand.

To get started:

Decide which policies apply and are appropriate for your government. At a minimum, experts recommend all organizations have policies that address the areas listed below.

- **Acceptable Use.** Covers what employees should consider appropriate use of official information resources and technology.
- **Social Media Accounts.** If your government uses social media (such as Facebook, Twitter, etc.), this policy describes acceptable use for social networking, including who can access social media and post to your agency's social media sites.
- **Incident Response.** Covers how to respond to a data breach or other cybersecurity incident, including who is in charge, who should be notified, and steps to take to minimize harm.

Safeguard 1: Establish and maintain written IT policies *(continued)*

- **Email.** Describes the appropriate use of government-issued email accounts and addresses the use of personal, third-party email, like Gmail.
- **Personal Device Use.** Discusses employees' personal devices and circumstances under which they can connect them to the network.
- **Passwords.** Describes requirements for a password, how often it must be changed, reuse of passwords, and prohibited passwords.
- **Use of Multi-Factor Authentication (MFA).** Covers the circumstances and specific types of accounts (such as IT administrators versus all employees) that must use MFA.

Once you have written your IT policies, decide how and when to share them with employees. Consider including your IT policies in your onboarding process for new employees, and requiring staff to take mandatory training or refreshers on a regular basis. In some cases, you might require employees to sign a copy of the policy as an acknowledgment they have read and agree to abide by it. We recommend you review your IT policies annually.

Resources and references you can use

- The SANS Institute offers policy guidance and sample language for a variety of different types of IT policies.
- The Center for Internet Security has a policy template guide you can download with links to dozens of IT policy templates.

This safeguard supports CIS Controls 1.2, 2.3, 9.1

WORD FORMAT
Can be edited

Policies & Training

Safeguard 2: Have a cybersecurity awareness program in place

About this safeguard

A cybersecurity awareness program trains employees to be mindful of cybersecurity risks as they perform their daily tasks. Employees should be aware of common fraud and phishing schemes, as well as basic techniques bad actors use to trick unsuspecting employees.

Why this safeguard is important

People are often an organization's weakest link. Hackers focus on taking advantage of human nature to gain access to your government's networks and sensitive information. Through social engineering techniques like phishing and smishing (using text messages instead of email), they manipulate human behaviors to gain access to login credentials and networks that, if improperly used, could reveal critical data or otherwise harm your government. While you may have put technical solutions in place to reduce the likelihood malicious activities will succeed, your overall security requires an embedded culture of cybersecurity awareness to be truly effective. With regular training, people can become your government's first line of defense.

What we observed during the checkup

Your organization does not have a cybersecurity awareness program.

Our recommendations

- Develop and implement a policy requiring employees to take regular cybersecurity awareness training. You can find links to example policies in the Resources section below.
- Create a cybersecurity awareness program that fits your government's needs. Awareness encompasses everything from a formal security awareness training program to a monthly email with cybersecurity tips, each designed to influence employees' behavior. There are many low-cost and free resources (see Resources below) to help you get started. You'll find tools for delivering training modules, assessments, and newsletters to keep employees engaged.
- Conduct training as part of onboarding for new employees and then annually for all staff.
- Review your training program and its associated policy annually to ensure your program is keeping up with evolving types of cyberattacks.

Resources and references you can use

- The National Institute of Standards and Technology (NIST) provides a sample template you can use to develop your own security awareness training policy.
- SAO's "People matter in cybersecurity" offers advice for starting an awareness program.
- Infosec Institute offers a free toolkit and training resources you can download.
- NIST provides a list of free and low-cost trainings you can use today to start your program.

This safeguard supports CIS Control 14.1

Incident Response

Safeguard 3: Have a process for employees to report cybersecurity incidents

About this safeguard

Written procedures tell staff how to report a suspected cybersecurity incident. The definition of what to consider a cybersecurity incident is wide-ranging. It encompasses an employee clicking on an untrustworthy email link and unleashing malware or losing a USB stick that contains confidential data, to someone gaining unauthorized access to your network and holding it for ransom.

Why this safeguard is important

A cybersecurity incident can put your government's critical systems or sensitive data at risk. Few IT departments or managed service providers have the resources to identify every security incident that takes place on your network. That's why it's important that employees not only have a method for reporting suspected incidents, but are encouraged to do so. Their efforts can help identify incidents early so you can take steps to reduce the harm.

Keep in mind that some security breaches must be reported to the Attorney General's Office and SAO. To learn more, visit SAO's webpage that explains when and how you are required to report a cybersecurity incident.

What we observed during the checkup

Your organization has an informal process for employees to report incidents, but this information does not appear in your written policies.

Our recommendations

- Develop a written procedure that clearly explains what types of incidents or issues to report, when and how to report incidents (by email, phone, instant message, etc.), and who to tell.
- Ensure that all employees are aware of the process and encouraged to use it. A best practice is to include it as part of your cybersecurity awareness training program.
- Review your process annually or more often if there are significant organizational changes that could affect it.

Resources and references you can use

- Here is a sample incident report form that you can modify for your government.
- The National Institute of Standards and Technology (NIST) offers a Computer Security Incident Handling Guide that walks you through all the steps of preparing for a potential incident and responding to one when it happens.

This safeguard supports CIS Control 17.3

Incident Response

Safeguard 4: Designate both a lead and a backup person to oversee incident response and recovery

About this safeguard

"Incident response and recovery" refers to the policy and plans you have in place to address and resolve a cyberattack. The plan itself must be flexible enough to cover a variety of attacks: data breaches, malware outbreaks, network intrusions, or denial of service attacks that shut down a machine or network. This safeguard is concerned with whether you have designated a lead person who is responsible for coordinating and documenting the incident response and recovery efforts when an attack occurs.

Why this safeguard is important

In today's computer-driven business world, cyber incidents are virtually unavoidable. It's important that you are set up for success when a cyberattack occurs. Knowing who will manage the incident can help limit the duration between attack and clean up.

What we observed during the checkup

Your organization has designated both a lead and a backup person to manage incident response, but this information does not appear in your written policies.

Our recommendations

Ensure that your government has identified a lead position (usually an IT manager, finance director, or similar role) and a backup to coordinate and document the incident response. You can designate positions within your organization or a third-party vendor, or use a hybrid approach. If you use a third-party vendor, be sure to designate an employee to oversee the vendor's work.

Resources and references you can use

- The National Institute of Standards and Technology (NIST) offers sample policies and more information about incident response and recovery in its Computer Security Incident Handling Guide. Page 16 provides specific information for incident response personnel.
- The Center for Internet Security (CIS) offers templates for response planning and communications. You can download a PDF document with links to policy templates.

This safeguard supports CIS Control 17.1

Incident Response

Safeguard 5: Maintain an inventory of emergency contacts and service providers

About this safeguard

"Emergency contacts" refers to those people who should be informed of a cybersecurity incident. The list typically includes internal staff, third-party vendors, law enforcement, relevant government agencies (like SAO or the Attorney General's Office), and other stakeholders.

"Service providers" refers to your government's internet provider, IT service provider(s), software vendor(s), and any other person or company that supports your IT systems.

Why this safeguard is important

When a security incident occurs, you need to be ready to launch a fast, effective response, and that includes communicating with everyone who needs to know what happened. Keep in mind that you may not have access to online channels or email after a cyberattack, so it's important to have a printed list of emergency contacts and service providers.

What we observed during the checkup

Your organization does not maintain an inventory of emergency contacts and service providers.

Our recommendations

- Make a comprehensive list of emergency contacts and service providers that includes the name of the person to contact and a phone number. For your service providers, include account information and any service agreements.
- Keep the list up to date by reviewing it annually or whenever you add IT hardware or software.
- Print several copies and give them to the incident response lead and backup, so they can reach everyone who should be informed of security incidents immediately.

Resources and references you can use

- The National Institute of Standards and Technology (NIST) provides detailed information about incident response and recovery.
- The Center for Internet Security (CIS) offers templates for response planning and communications. You can download a PDF document with links to policy templates.

This safeguard supports CIS Controls 15.1 and 17.2

Accounts & Passwords

Safeguard 6: Require employees to use strong and unique passwords

About this safeguard

A password is an employee's authentication to log into a computer system or application. A strong password is one that is long, complex, and hard to guess. A unique password means that each employee has their own login credentials to access work accounts and applications, which no one else can use.

Why this safeguard is important

The purpose of a password is to ensure that only authenticated users can access resources, so a password that is easy to guess is a cybersecurity risk. Hackers can run a program that will try thousands of commonly used passwords per second, and often manage to access a computer network or account in this manner. And if the same password is used for multiple accounts, then a hacker can gain access to a significant amount of sensitive data. Allowing employees to share work accounts and passwords can also result in major security risks. For example, it can be difficult to trace the user responsible for a security incident if it involves a shared account. Employees participating in malicious activities can deny any accusations, pointing out that they are not the only ones with access to the account in question.

What we observed during the checkup

Your organization does not require employees to use strong and unique passwords.

Our recommendations

- Establish and enforce a policy that requires each employee to have their own unique login credentials to access work accounts and applications.
- Establish and enforce a policy to address password requirements that includes length (typically at least 14 characters), complexity, attempts before locking out, password history requirements, and password change frequency. You might tailor requirements based on the level of access a given account has to a critical system. For example, administrative accounts should have stricter requirements.
- Teach employees how to create unique, unguessable passwords. Training should remind staff:
  - > Don't use personal information or words related to their job, hobbies, or interests.
  - > Do use a mix of upper and lowercase letters, numbers, and special characters.
- Keep in mind some organizations that regulate areas of your business, such as the Criminal Justice Information Services (CJIS) and Payment Card Industry Data Security Standard (PCI DSS), may impose their own password requirements.

Resources and references you can use

- The Center for Internet Security (CIS) offers an easy-to-follow password policy guide that not only provides best practices, but explains the reasoning behind the recommendations.
- Microsoft offers an evergreen summary of best practices for developing and enforcing password policies; the website also offers suggestions for setting password policies in Microsoft 365.

This safeguard supports CIS Control 5.2, CIS Password Policy Guide

Safeguard 7: Encourage employees to use password managers

About this safeguard

A password manager is a computer application that allows users to store and manage multiple account passwords in an encrypted database behind a master password. This means users only have to remember one password. Many password managers can also generate strong, random passwords so the user doesn't have to invent them on their own.

Why this safeguard is important

All too many people use very weak – and easily guessable – passwords. Worse, they then reuse them on multiple websites. Hackers appreciate the easy access: having guessed right once, they gain access to enter unrelated systems. Using a password manager allows employees to store strong passwords so they don't have to commit them all to memory or keep them in a document that, if hacked, exposes all passwords.

What we observed during the checkup

Your organization encourages employees to use password managers.

Our recommendations

- If you have IT support or use an IT service provider, ask them about obtaining a password manager for staff to use. Password managers are available as a cloud-based subscription or as an installed software program. The cost is typically between $10 and $60 a year for each user.
- If your government doesn't have IT support, you could opt for a free, cloud-based password manager. Free applications may come with some limitations, but they often provide the necessary features to store your passwords securely. If you choose to use a free password manager, make sure it meets your government's needs. For example, some will limit the number of stored passwords or restrict usage on mobile devices.
- In either case, set expectations with your staff – either as a requirement or an encouraged behavior – that they use whatever password management solution you choose.

Resources and references you can use

- CNET ranks what they consider the best password managers of 2022, and several of them are free. Password Safe is a free version you may want to explore.
- To learn more about how password managers work, Consumer Reports walks you through it in a concise article.

This safeguard supports CIS Password Policy Guide

Safeguard 8: Restrict administrator privileges to dedicated administrator accounts

About this safeguard

A user with admin privileges can change system settings, install software or system updates, create users accounts, and change passwords. Users without admin privileges cannot perform such system-level modifications.

Only certain trusted users – usually just IT staff – should be granted admin privileges; these users can perform necessary work only when logged into separate accounts dedicated to administrative tasks. Everyone else should have only a standard user account that prohibits admin access. This prevents employees from doing things like uninstalling applications that your government needs, installing applications that your government doesn't want, or changing important files.

Why this safeguard is important

Admin privileges are essential to the proper function of any IT infrastructure because they enable trusted users to install software and to change and amend accounts. However, unmanaged admin privileges also present a huge risk to the security of your data. Hackers often target accounts with administrative privileges: with the keys to your entire system, they can quickly spread malware, lock users out of the network, and more.

Restricting administrative privileges to only those who need it, like IT staff, makes it more difficult for intruders to disrupt your computer or network operations, steal information, or gain access to confidential data. Restricting admin privileges is the one of most powerful measures you can take to protect your government's computer system.

What we observed during the checkup

Your organization does not restrict admin privileges to dedicated administrator accounts.

Safeguard 8: Restrict administrator privileges to dedicated administrator accounts *(continued)*

Our recommendations

- If your government has IT support or uses a service provider, ask them what administrative privileges exist, for which systems or software, and who has access to these accounts and why.
- If you don't have IT support or your organization is quite small, you can still protect your system by requiring employees to use separate, dedicated user accounts to perform administrative tasks.
- In either situation, here are the basic steps to take to set up a formal process for issuing and managing accounts with admin privileges,
  - > Start by determining who actually needs administrative privileges based on their job function.
  - > Develop and put in place policies and procedures regarding granting, reviewing, and revoking privileges.
  - > Assign administrative accounts to those employees who need higher privileges that are separate from their standard user account. Make sure each account is linked to a specific employee, and maintain a list of names and related account information.
  - > Ensure that administrative accounts do not have internet access or access to email.
  - > Ensure that staff with administrator privileges are trained to carry out their duties. This includes understanding that they use their standard user account for day-to-day work, logging into their admin account only when they need to install software or change login information. As soon as they have completed the task, they should sign out of the admin account.
  - > Regularly review employees' requirements to have a privileged account, and update access to these accounts when staff change duties, leave the organization, or are involved in a security incident.

Resources and references you can use

- InfoSecurity Magazine explains what administrative privileges are and why you should use them.
- Microsoft also has a web page about how administrative privileges work.
- Windows 101 explains how to set up accounts for administrators and standard users.

This safeguard supports CIS Control 5.4

Accounts & Passwords

Safeguard 9: Protect accounts with administrative privileges by using multifactor authentication (MFA)

About this safeguard

This safeguard addresses a common technique for protecting accounts with administrative privileges: multifactor authentication (MFA). Multifactor means users can only access certain computer systems or applications if they possess two of three secure elements: 1) Something they know, such as a password, pin, or answer to a security question, 2) Something they have, such as a cell phone where they can retrieve a texted code, a hardware security key, or a smart card with an embedded chip, or 3) Something they are, usually a biometric like a fingerprint or voice recognition.

Why this safeguard is important

Accounts with administrative privileges should be protected with MFA because of the increased risk to the IT system if they are compromised. MFA adds an extra layer of authentication that hackers are unlikely to be able to replicate when trying to log into your government's computer systems.

For example, MFA using a smartphone will send a unique verification code to the administrator's device after the employee has entered their user name and password. The correct code must be entered into the system before the application will unlock. Even with a stolen user name and password, hackers are unlikely to have access to the smartphone connected to the user account. Without the verification code, hackers will have a more difficult time trying to access the system.

What we observed during the checkup

Your organization does not use MFA to protect accounts with administrative privileges.

Our recommendations

- Check with your IT support or service provider whether MFA is being used on accounts with administrative privileges. If not, determine what is needed to implement MFA on these accounts.
- If software your government uses came with a MFA option, make sure it is enabled for all accounts with administrative privileges. If you're unsure if MFA is available, contact your software vendor to find out the steps you need to take to activate it.
- If MFA isn't an option with your current software or service, evaluate whether you want to keep using that product or service, or find something new with better security features.
- Be sure your IT policy includes requirements for MFA on administrative accounts.
- If your government can't implement MFA right now, refer to Safeguard 8 for suggestions on improving security for administrative accounts.

Resources and references you can use

- Cybersecurity & Infrastructure Security Agency (CISA) offers a succinct summary of multifactor authentication.
- Microsoft provides an overview of the types of administrative accounts that should have MFA enabled as well as sample policy language.

This safeguard supports CIS Control 6.5

Safeguard 10: Require remote workers to use MFA

About this safeguard

"Remote workers" refers to employees who may access your government's systems or applications remotely. This includes any staff who work from home or who may log in from a different worksite than your main office. This control considers whether you have a policy – and a process – in place for employees working off-site to use multifactor authentication (MFA) whenever they log in to their computers and other government-issued devices or access your software or network. (See Safeguard 9 for a detailed explanation of how MFA works.)

Why this safeguard is important

Working off-site – whether from home, at a client's office, or a remote workplace – adds risks to your IT systems because remote computer connections are more vulnerable to cybercrime than those connected directly to in-office systems. For example, remote employees logging into your network via unsecured, free Wi-Fi in a public space expose their devices – and your network – to criminals who are "network snooping" in hopes of picking up passwords or credit card information. Aside from that, research has shown that remote employees tend to fall for phishing schemes more often than employees working in the office, and they are less likely to inform their manager or IT. MFA adds an extra layer of authentication that hackers will not be able to acquire when trying to log into your government's computer systems.

What we observed during the checkup

Your organization does not require remote users to use MFA.

Our recommendations

- Ensure your IT policies include requirements for remote users to use MFA when accessing your government's systems.
- Ask your IT support or service provider if MFA is available for your software and network systems, and what you need to do to enable it for employees who access your system or applications remotely. Make sure they complete the activation steps.
- If MFA isn't an option, evaluate the risks of continuing to use that product or service versus the costs of switching to new services with better security features for your remote users.
- If your government can't implement MFA right now, put the following safeguards in place:
  - > Monitor user logs for unexpected or suspicious activity, such as someone logging in during non-working hours or from another country. Monitor vulnerable systems like email servers, your virtual private networks (VPNs), network management systems, or other business systems that contain critical or sensitive information.
  - > Require remote employees to use a separate, dedicated user account to perform any administrative tasks. (See Safegaurds 8 and 9 for additional suggestions on improving security for administrative accounts.)

Resources and references you can use

- Cybersecurity & Infrastructure Security Agency (CISA) offers a succinct summary of Multifactor Authentication.
- Windows 101 explains how to set up accounts for admins and standard users.

This safeguard supports CIS Control 6.4

Safeguard 11: Install anti-virus programs on all computers

About this safeguard

Modern anti-virus programs help protect IT systems and individual computers from malicious software. They are designed to prevent, detect, and remove malicious software code, like viruses, worms, Trojans, adware, and more.

Why this safeguard is important

Malware (a term that encompasses computer viruses) is a favorite tool of the attacker because it's relatively easy to deploy on unsecured networks and it runs autonomously. It's critical that up-to-date anti-virus programs are installed on any computer or device capable of connecting to the internet. To forgo such protection is extremely risky.

What we observed during the checkup

Your organization has installed anti-virus programs on all computers.

Our recommendations

- If you have IT support or a service provider, ensure that they have installed anti-virus software on your government's computers and other devices, and that they regularly update it. They should also schedule regular scans to check for issues at the network level and monitor the overall health of your network. If you're using a service provider, this should be a standard part of your contract.
- If you don't have IT support, your Windows and Apple Mac computers can still be protected.
  - > **Windows:** Microsoft Defender Antivirus (formerly known as Windows Defender) installs automatically when you install the Windows operating system. This antivirus software scans, detects and removes viruses, spyware, and malware. There is no need to download it as it's included for free on Windows.
  - > **Apple:** Mac computers come with the built-in antivirus software XProtect. The MacOS also has a feature known as Gatekeeper, which blocks downloaded software that lacks a digital signature indicating the developer has been approved by Apple.

Resources and references you can use

- TechTarget explains the different types of anti-malware available and includes a video that explains why it's important to have.
- Here's video that explains why you need anti-malware protection and how Microsoft Defender works.
- You can follow these instructions to implement Microsoft Defender on individual computers.
- Apple's website provides more information about its XProtect antivirus software.

This safeguard supports CIS Control 10.1

Safeguard 12: Regularly apply security patches on all computers and applications

About this safeguard

A security patch is software that corrects errors in computer software code. Security patches are issued by software companies to address vulnerabilities in the company's product. Common areas that will need patches include operating systems, applications, and software running network equipment. This control is most effective when all patches issued by a software developer are applied promptly.

Why this safeguard is important

Security patches prevent and deter hackers and cybercriminals from exploiting known vulnerabilities in your software that could open the door to data breaches and long-term infections. Patches also are a way to fix bugs and improve the application's compatibility with the rest of the system.

What we observed during the checkup

Your organization regularly applies security patches on all computers and applications.

Our recommendations

- If you have IT support or a service provider, ensure they install patches regularly, and test them regularly. This can be done manually or automatically. For manual updates, someone must visit the software vendor's website to download and install the patch files. Automatic patching is preferable because once you authorize the vendor to push automatic patches to its software, no one will need to remember to check for updates in the future.
- If you don't have IT support, you'll need to install patches to every computer individually. While there is no cost for these patches, you'll need to stay vigilant in updating them when they are released. You'll see notices from your operating system and browsers when updates are available.

Resources and references you can use

- MakeUseOf provides a succinct overview of what patches do and their importance.
- TechWare explains how to find out what patches you need to install and offers best practices for doing so.
- UniversalClass provides a step-by-step tutorial for installing patches.

This safeguard supports CIS Controls 7.3, 7.4

Safeguard 13: Use only fully supported internet browsers and email clients

About this safeguard

Web browser applications are programs that allow users to view and interact with websites on the internet. Examples of browsers include Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari.

An email client refers to a computer program used to access and manage a user's email. Examples include Outlook, Apple's Mail app, Mozilla Thunderbird, and Gmail.

This control ensures that you're using the current, fully supported release of whichever browser or email client you've chosen to use.

Why this safeguard is important

Hackers target email and web browsers with several types of attacks. For example, they can attach a file containing ransomware to an email that pretends to be from a reputable source, or include a link that appears to be for a legitimate website, but actually points to a malicious site that enables the hacker to collect the user's account credentials.

Certain features of email clients make them particularly vulnerable, and successful attacks can enable hackers to breach your network and compromise your systems, applications, and data. To reduce the risk of security incidents, you should only use fully supported browsers and email clients.

What we observed during the checkup

Your organization installs specific internet browsers, but it is recommended you manage them with group policies.

Our recommendations

- Ensure your IT policies include your requirements for browsers and email clients to prevent employees from downloading applications from the internet or using their own personal email accounts for government business.
- If you have IT support or use a service provider, they can install and manage your browsers and email clients at the network level. Specify that only fully supported browsers and email clients are allowed, and ensure they update them promptly when new versions are released.
- If you don't have IT support or a service provider, you'll need to update your browsers manually on each computer. Updates are free. Some browsers, like Google Chrome, update automatically. For others, you'll need to monitor when updates are needed (most will alert you). Most email clients also update automatically, including Outlook and Gmail, so no action is needed.

Resources and references you can use

- MakeUseOf explains why it's important to update your browser.
- WikiHow provides step-by-step instructions to manually update each of the available browsers.

This safeguard supports CIS Control 9.1

Safeguard 14: Apply timed lockouts on all device screens

About this safeguard

A timed lockout on a computer screen refers to the amount of time until an inactive computer locks the screen, requiring the user to enter a password to resume working. Although the screen is locked, the computer continues to run in the background, so documents and applications aren't closed out.

Why this safeguard is important

Any time an employee walks away from their computer or tablet without locking the screen or logging off, it poses a security risk to your government. Someone can use the computer in an unauthorized way, such as sending an email from the employee's account, tampering with or deleting files, or accessing and downloading confidential data. This control helps you reduce the window of opportunity for such intrusions by setting the computer to automatically lock the screen after a few minutes of inactivity.

What we observed during the checkup

Your organization does not apply timed lockouts on device screens.

Our recommendations

- Make sure your IT policies include requirements for timed lockouts on all computer screens. The recommended timed lockout is 15 minutes for operating systems and two minutes for mobile devices.
- If you have IT support or a service provider, they can configure automatic session locking on every computer from the network level.
- If you don't have IT support or a service provider, you can either configure session locking individually on each computer or require employees to manually lock their computers when they are away from them. If you choose the latter path, be sure to include this requirement in your IT policies. Instructions for both options can be found below.

Resources and references you can use

- TechBar provides a good overview of why it's a good idea to lock computers.
- Cornell University provides step-by-step instructions on how to configure session locking.

This safeguard supports CIS Control 4.3

Data Protection

Safeguard 15: Encrypt data on computers or other devices containing sensitive information

About this safeguard

Encryption is the process through which data is encoded so that it is unreadable or inaccessible to unauthorized users. It helps protect private information and sensitive data by using mathematical algorithms to scramble messages, which means you need a special key or passcode to decode the message.

Any computer or other device that can store sensitive data, such as smartphones and tablets, should be encrypted.

Why this safeguard is important

Even if unauthorized people gain access to encrypted data – for example, by stealing a laptop from a parked car – they won't be able to read it. Data encryption helps protect the private information and sensitive data your government holds from exposure during a data breach.

Furthermore, if your government collects personally identifiable information (PII) used to process financial payments, you are legally required by the Payment Card Industry Data Security Standards (PCI DSS) to secure that data.

What we observed during the checkup

Your organization does not encrypt data on end-users devices.

Our recommendations

- If you have IT support or a service provider, ask them about using encryption on all hard drives. Many anti-virus programs include encryption software, so you may already have it and just need to activate it. You can also purchase stand-alone encryption tools.
- If you don't have IT support, it is straightforward to check your computers to see if encryption is enabled, and to set it up if it isn't. Most computers come with built-in encryption programs, so there's no extra cost; Windows uses BitLocker and Apple uses FileVault. When you set up full hard drive encryption, you will be directed to create a special key or passcode to unlock the files. Be sure to keep a written copy of the passcode in a safe place away from your computer or device! (See instructions in the resource section below.)

Resources and references you can use

- Business News Daily provides an overview of encryption as well as step-by-step instructions on how to access BitLocker and FileVault.

This safeguard supports CIS Control 3.6

Data Protection

Safeguard 16: Back up data regularly and automatically

About this safeguard

Data backup is the practice of copying data from a primary location to a secondary one. "Data" encompasses documents, media files, configuration files, machine images, operating systems, and registry files: it's essentially any data you want to preserve. The frequency of the backup depends on the sensitivity of the data, and the effect on your government if some were lost. Automated backups are a stronger control than relying on a person to perform the task.

Why this safeguard is important

Making backups of data is critically important. Backups protect against human errors, hardware failure, ransomware attacks, virus attacks, power failure, and natural disasters. Backups can help save time and money if these failures occur.

The backup process can be automated with backup software so that no human intervention is necessary. Automated backups gather, compress, encrypt, and transfer data automatically from a computer system to a backup location. Manual backups are generally a bit riskier, since human actions always introduce the possibility of error or simple forgetfulness.

What we observed during the checkup

Your organization backs up data regularly and automatically

Our recommendations

- Ensure your IT policies include what should be backed up and how frequently, where the backup should be located, and how it will be protected.
- If you have IT support or a service provider, make sure they comply with your IT policy on data backups.
- If you don't have IT support, you can still set up automated backups without too much trouble. Most external backup drives come with straightforward instructions and software to transfer the data you want to back up on a set schedule. You can also back up each computer manually, either to an external drive or to a cloud-based solution.

Resources and references you can use

- SAO's "Backup and Recovery Best Practices" provides tips for creating a data backup policy as well as an overview of best practices.
- The U.S. Department of Homeland Security describes the different options for storing your backup data.
- Microsoft provides step-by-step instructions on how to backup and recover your data manually.

This safeguard supports CIS Control 11.2

Data Protection

Safeguard 17: Block unnecessary email attachments

About this safeguard

"Email attachments" refer to the files that can be attached to an email and sent to a recipient. Common file types you've likely seen or used include .docx (Microsoft Word), .pptx (PowerPoint), .jpg (image file), or .mp3 (music file). These file types tell your computer which application to use when opening that file.

However, some file types are much more susceptible to hacking and can do greater harm if you download and open them from an email. This control recommends you automatically block any file type that is not essential to your business operations from being sent or received via email.

Why this safeguard is important

Email attachments are an attacker's favorite method to spread malware. The attachment carries software that is designed to damage or exploit your device or network. Opening the infected attachment launches the malware. Cybercriminals also use email attachments to carry out phishing and ransomware schemes.

Some email attachments are regarded as high risk, such as executable files (.exe), scripts, compressed files, and ISO files, and should never be opened. But all email attachments, including Word, Adobe Acrobat, and PowerPoint files, can be manipulated and contaminated, which means you should exercise caution when opening attachments you're weren't expecting.

What we observed during the checkup

Your organization blocks unnecessary email attachments.

Our recommendations

- If you have IT support or a service provider, ensure that they have set up your email accounts to block high-risk email attachments for all computers at the network level. They should also have anti-malware software configured to scan incoming emails for malicious code or executable files.
- If you don't have IT support, most email software provides at least some protection. Most email clients, like Outlook, do this by default. You can also manually set up email attachment blocking (see more in the Resource section below).
- Develop and implement a policy requiring employees take regular training on handling email attachments, and ensure it is covered in your cybersecurity awareness training.
- Consider choosing to share files via file hosting services instead of emailing attachments. OneDrive is included in Microsoft 365, while GoogleDrive and DropBox are free but have limits on data storage size (you can increase storage by paying a subscription fee).

Resources and references you can use

- TrendMicro provides a complete list of email attachment file types that should be blocked.
- Microsoft offers step-by-step instructions to set up attachment blocking.

This safeguard supports CIS Control 9.6

Safeguard 18: Maintain firewalls on all computers and devices

About this safeguard

A firewall is a security mechanism designed to prevent unauthorized access to a single computer or a network of computers. A firewall monitors incoming and outgoing network traffic, and either permits or blocks it based on security rules. It is used mostly as a first line of defense to protect your IT systems from online threats such as hackers and viruses.

A firewall can either be software or hardware. Software firewalls can be installed on each computer and monitor the network traffic. Hardware firewalls are typically installed where there is more network traffic, such as between the internet and your network (also known as the "gateway"). This safeguard doesn't specify which to choose, only to ensure your computers and all devices are protected behind a firewall.

Why this safeguard is important

Every time you are connected to the internet, you expose your computer to all sorts of dangerous programs and bad actors that want to infiltrate your computer to steal your personal information, or use your computer to launch attacks on other computers. A good firewall system can deter or prevent attackers from infiltrating your system and stealing your data.

What we observed during the checkup

Your organization maintains firewalls on some devices.

Our recommendations

- Ensure your IT support or service provider has installed firewalls between your computers or network and the internet. If you have a service provider, ensure that firewall installation is included in your contract.
- If you don't have IT support, you can still protect your computers using software/systems that are bundled with both Windows and Apple operating systems. The Resources section below has links to websites explaining how to get them up and running.

  > **Windows**: Windows Firewall is included at no cost in your Windows operating system.

  > **Apple**: The MacOS also comes with built-in firewall protection.

Resources and references you can use

- How-to Geek offers an overview of what a firewall actually does.
- ComputerHope provides step-by-step instructions to enable the Windows Firewall.
- Apple's website provides information about its firewall for Macs.

This safeguard supports CIS Control 4.5

Network

Safeguard 19: Use Domain Name Service (DNS) filtering to block access to malicious domains

About this safeguard

The Domain Name System (DNS) makes it possible for websites to have easy-to-remember domain names. For example, SAO's domain name, "sao.wa.gov", is easy for people to remember but it's of no use to a computer. Computers rely on a series of numbers called an IP address to find a webpage. The DNS converts a domain name into a corresponding IP address.

DNS web filtering takes place at the DNS lookup stage of a web request, before your computer connects to the server hosting the web content. The filter checks the requested IP address against a list of known malicious websites. If the requested website is on the list, you will be blocked from accessing the website.

DNS filters can also be used to block employees or guest Wi-Fi users from accessing specific sites. For example, your government might choose to block social media sites during work hours.

Why this safeguard is important

DNS filtering is a very important cybersecurity measure that prevents employees from accessing malicious sites that can administer phishing, ransomware, or other cyberattacks. It blocks threats based on the reputation of IP addresses, and blocks downloads of file types associated with malware.

What we observed during the checkup

Your organization does not use DNS filtering to block access to known malicious domains.

Our recommendations

- Typically, DNS filtering is a service offered by a third-party vendor; costs are based on a price-per-user, with discounts for annual or bulk subscriptions. You can get free DNS filtering by becoming a member of the Multi-State Information Sharing and Analysis Center (MS-ISAC), which provides cybersecurity resources to governments. Membership in MS-ISAC is free for local governments.
- Ensure your IT support or service provider has set up DNS filters to block malicious websites.
- If you don't have IT support and for some reason are not a member of MS-ISAC, you can still protect your IT system by purchasing DNS filtering services directly from a vendor. Well-known providers include Cisco, Webroot, and Avast.

Resources and references you can use

- TechRadar explains in more detail what DNS filtering is and how it works.
- To sign up for MS-ISAC, visit the registration page. Once you've registered, you can sign up for their DNS filtering service and enter your email address, which is all that is required.

This safeguard supports CIS Control 9.2

Credit Cards

Safeguard 20: Meet PCI DSS requirements for credit cards

About this safeguard

The Payment Card Industry Data Security Standards (PCI DSS) is a set of requirements to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. Any organization that accepts credit cards must follow the 12 PCI DSS requirements listed here:

1. Use and maintain firewalls to protect cardholder data
2. Use proper password protections
3. Protect stored cardholder data
4. Encrypt transmitted cardholder data
5. Use and maintain anti-virus protection
6. Properly update software
7. Restrict data access to only authorized personnel
8. Use unique IDs for authorized personnel to access critical data systems
9. Restrict physical access to cardholder data
10. Create and maintain access logs to cardholder data
11. Scan and test for vulnerabilities regularly
12. Support information security with organizational policies and programs

Why this safeguard is important

Being "PCI compliant" means your government has met the requirements of the Payment Card Industry Security Standards Council. If you don't meet PCI standards, you are not only more likely to experience account data breaches, you could also be subject to financial penalties from your payment processors.

What we observed during the checkup

Your organization appears to be aware of PCI DSS requirements.

Our recommendations

PCI DSS is required by contract for those handling cardholder data, including local governments. Your agency must always be compliant, and your merchant bank must validate your status annually. If you have questions about what you must do to be compliant, consult your bank.

Resources and references you can use

- The PCI Data Security Standards website offers information about implementing the standards as well as training opportunities.

South Whidbey
Parks & Recreation District

Memo

To: Board of Commissioners

From: Brian Tomisser, Director

Date: 06/18/2024

Re: Asphalting of Parking Lot Sports Complex

Staff received four bids to overlay the asphalt of the Sports Complex parking lot. As part of your packet, I've included the Bid Tabulation for the project.

The project includes overlaying the main parking lot, approximately 42,000 square feet and the entrance to the sports complex from the gate to Langley Road, approximately 1700 square feet.

Also included was an alternative bid to continue asphalting the maintenance building parking lot, approximately 7000 square feet. The 2024 budget has $130,000 allocated for this project.

The lowest bid is from Krieg Construction for a total $96,259.00. This includes the base bid and the alternative bid. Tax is not included in the bid. With sales tax it comes to a little less than $105,000. Staff recommend the Board authorize the Director to enter a contract not to exceed $105,000 with Krieg Construction for overlaying the asphalt at the Sports Complex parking lot and laying new asphalt at the Maintenance Facility.

South Whidbey Parks and Recreation District

INVITATION TO BID TABULATION

Asphalt of Sports Complex with Alternate for Maintenance Building

Department/Contact: Brian Tomisser, Executive Director
Submission Deadline: 06/12/2024

- Bids opened 02/01/2024 at 2:00 PM by Brian Tomisser.
  - Present: Danny Krieg (Krieg Construction), Tom Fallon (staff), Carrie Monforte (staff)

Estimate: **BIDS RECEIVED FROM:**

Name	**Base Bid Sports Complex 1 ½ "**	**Alternate Bid Maintenance Shop**	**Total Bid**
Lakeside Industries Inc	$82,750	$24,000	$106,750.00
Western Refinery Services, Inc	$78,780	$27,560	$106,340.00
Krieg Construction	$78,975	$17,284	$96,259.00 -Lowest Bid
Rainier Asphalt	$123,149.95	$13,782.46	$136,932.41

South Whidbey
Parks & Recreation District

Memo

To: Board of Commissioners

From: Brian Tomisser, Director

Date: 06/18/2024

Re: Fund Management

Staff have been working to analyze our funds and how they are being used. With the impending bond proceeds, we need a designated fund, however we do not feel we need to add a sixth fund with the County.

With that said, staff makes the following recommendations:

- Resolution 2024-05: This would close the Property Fund (Fund #665), which has been used for the campground project. With the campground project not currently active, we will transfer the remaining balance of available funds into the Capital Fund (#768). We will internally still track these funds the exact same way, so the transferred funds will be designated for the future campground.

- Resolution 2024-05: This would re-open the Construction Fund (Fund #741). This fund will be used for the Aquatic Recreation Center project and the bond proceeds.

We have consulted with the Island County Treasurer seeking feedback about the two possible action steps. His response included no concerns or anything that would prohibit these moves.

SOUTH WHIDBEY PARKS AND RECREATION DISTRICT
RESOLUTION 2024-05

Resolution to Close Property Fund #665

WHEREAS, South Whidbey Parks and Recreation District has Property Fund #665 ;

WHEREAS, South Whidbey Parks and Recreation District no longer has a need for Property Fund #665 ;

NOW, THEREFORE, BE IT RESOLVED, by the Board of Commissioners of the South Whidbey Parks and Recreation District, of Island County, in the State of Washington, has agreed that the District should close Property Fund #665 and transfer the balance as of May 31, 2024 in the amount $189,834.64, plus any accrued interest between this date and the date of transfer to the Capital Fund #768.

ADOPTED, at a regular meeting of the Board of Park District Commissioners of South Whidbey Parks and Recreation District, on June 18, 2024.

BY: _____

Jennifer Cox, Chair

ATTEST:

_____ _____

Jennifer Cox, Chair Matthew Simms, Treasurer

_____ _____

Erik Jokinen, Vice-Chair Krista Loercher, Secretary

_____

Jake Greve, Commissioner-at-large

SOUTH WHIDBEY PARKS AND RECREATION DISTRICT
RESOLUTION 2024-06

Resolution to Open Construction Fund #741

WHEREAS, South Whidbey Parks and Recreation District is in need of a Construction Fund #741 to manage the funds for a current Park District Bond project;

WHEREAS, South Whidbey Parks and Recreation District has had this Construction Fund #741 to manage the funds for past Park District Bond projects which was closed March 20, 2013 ;

NOW, THEREFORE, BE IT RESOLVED, by the Board of Commissioners of the South Whidbey Parks and Recreation District, of Island County, in the State of Washington, has agreed that the District should open Construction Fund #741.

ADOPTED, at a regular meeting of the Board of Park District Commissioners of South Whidbey Parks and Recreation District, on June 18, 2024.

BY: _____

Jennifer Cox, Chair

ATTEST:

_____ _____

Jennifer Cox, Chair Matthew Simms, Treasurer

_____ _____

Erik Jokinen, Vice-Chair Krista Loercher, Secretary

_____

Jake Greve, Commissioner-at-large