AGENDA

COVID-19 Meeting Notice

To address concerns relating to COVID-19 and to comply with the prohibitions on gatherings under Santa Barbara County Health Officer Order No. 2021-12.4, this meeting will be held by remote video conferencing, as authorized by Governor Newsom's Executive Order N-29-20.

Members of the public who wish to observe the meeting and/or offer public comment by video conferencing should contact the District at least 24 hours before the meeting at (805) 967-4519 or RMangus@GoletaSanitary.org to obtain the meeting ID and passcode.

Members of the public with disabilities who wish to request a reasonable modification or accommodation to observe the meeting and/or offer public comment should contact the District at least 24 hours before the meeting at the foregoing telephone number or email address for instructions on how to access the meeting.

AGENDA

REGULAR MEETING OF THE GOVERNING BOARD
OF THE GOLETA SANITARY DISTRICT
A PUBLIC AGENCY

One William Moffett Place
Goleta, California 93117

April 5, 2021

CALL TO ORDER: 6:30 p.m.

ROLL CALL OF MEMBERS

BOARD MEMBERS:
Jerry D. Smith
Steven T. Majoewsky
George W. Emerson
Sharon Rose
Edward Fuller

CONSIDERATION OF THE MINUTES OF THE BOARD MEETING

The Board will consider approval of the Minutes of the Special Meeting of March 24, 2021

PUBLIC COMMENTS - Members of the public may address the Board on items within the jurisdiction of the Board.

POSTING OF AGENDA – The agenda notice for this meeting was posted at the main gate of the Goleta Sanitary District and on the District's web site 72 hours in advance of the meeting.

BUSINESS:

1. REVIEW AND CONSIDERATION OF 2021 ACTION PLAN SUMMARY
(Board may take action on this item.)

2. CONSIDERATION OF AMENDMENT TO ORDINANCE NO. 73 TO UPDATE INDUSTRIAL WASTE CONTROL PERMIT CLASSIFICATIONS TO CORRESPOND TO SEWER USE ORDINANCE NO. 92 AND REVISED FEE SCHEDULE
(Board may take action on this item.)

3. DISCUSSION AND CONSIDERATION OF CYBER SECURITY CONTROL STANDARDS
(Board may take action on this item.)

4. GENERAL MANAGER'S REPORT

5. LEGAL COUNSEL'S REPORT

6. COMMITTEE/DIRECTOR'S REPORTS AND APPROVAL/RATIFICATION OF DIRECTOR'S ACTIVITIES

7. PRESIDENT'S REPORT

8. ITEMS FOR FUTURE MEETINGS

9. CORRESPONDENCE
(The Board will consider correspondence received by and sent by the District since the last Board Meeting.)

10. APPROVAL OF BOARD COMPENSATION AND EXPENSES AND RATIFICATION OF CLAIMS PAID BY THE DISTRICT
(The Board will be asked to ratify claims.)

ADJOURNMENT

Any public records which are distributed less than 72 hours prior to this meeting to all, or a majority of all, of the District's Board members in connection with any agenda item (other than closed sessions) will be available for public inspection at the time of such distribution at the District's office located at One William Moffett Place, Goleta, California 93117.

MINUTES

MINUTES

SPECIAL MEETING OF THE GOVERNING BOARD
GOLETA SANITARY DISTRICT
A PUBLIC AGENCY
PACIFICA SUITES HOTEL
5490 HOLLISTER AVENUE
SANTA BARBARA, CALIFORNIA 93117

March 24, 2021

CALL TO ORDER: President Smith called the meeting to order at 10:02 a.m.

BOARD MEMBERS PRESENT: Jerry D. Smith, Steven T. Majoewsky, George W. Emerson, Sharon Rose, Edward Fuller

BOARD MEMBERS ABSENT: None

STAFF MEMBERS PRESENT: Steve Wagner, General Manager/District Engineer and Rob Mangus, Finance and Human Resources Manager/Board Secretary and Laura Romano, Management Analyst (via zoom).

OTHERS PRESENT: None

APPROVAL OF MINUTES: Director Rose made a motion, seconded by Director Majoewsky, to approve the minutes of the Regular Board meeting of 03/15/21. The motion carried by the following vote:

(21/03/2183)

AYES:	5	Smith, Majoewsky, Emerson, Rose, Fuller
NOES:		None
ABSENT:		None
ABSTAIN:		None

POSTING OF AGENDA: The agenda notice for this meeting was posted at the main gate of the Goleta Sanitary District and on the District's website 24 hours in advance of the meeting.

PUBLIC COMMENTS: None

BUSINESS:

1. ANNUAL PLANNING WORKSHOP
The Governing Board, General Manager, and Finance and Human Resources Manager/Board Secretary met to discuss various issues related to District operations, including but not limited to prior year goals, financial data and performance information.

Board recessed for lunch at 12:10 p.m.

Board was called to order after lunch at 1:05 p.m.

No Board action was taken.

ADJOURNMENT

There being no further business, the meeting was adjourned at 2:25 p.m.

Jerry D. Smith
Governing Board President

Robert O. Mangus, Jr.
Governing Board Secretary

Steven T. Majoewsky

George W. Emerson

Sharon Rose

Edward Fuller

AGENDA ITEM #1

AGENDA ITEM: 1

MEETING DATE: April 5, 2020

I. NATURE OF ITEM

Review and Consideration of 2021 Action Plan Summary

II. BACKGROUND INFORMATION

The District's Governing Board held its annual planning meeting on Wednesday, March 24, 2021 at the Pacifica Suites. At this meeting, the Board reviewed the District's 2020 annual report along with the prior year and year to date financial information. A preliminary draft action plan for 2021 was developed based on this information that included 25 separate goals and 71 actions related to the District's Strategic Plan.

A copy of the 2021 Action Plan summary based on the review and comments at the annual planning meeting is attached to this report. Once approved, a detailed timeline for the implementation of all stated actions will be prepared and brought to the Board for review on a quarterly basis through the end of FY 2021-22.

III. COMMENTS AND RECOMMENDATIONS

Staff recommends the Board review and approve the attached 2021 Action Plan Summary subject to any revisions as desired.

IV. REFERENCE MATERIALS

2021 Action Plan Summary

Goleta Sanitary District 2021 Annual Plan Summary

CATEGORY #1 CAPITAL IMPROVEMENTS

* Implement Long Range Master Plan (LRMP) Projects
* Implement Phase 1 of Biosolids & Energy Strategic Plan (BESP)
* Implement Lystemize Refeed Pilot Project
* Complete Planned Office Space Improvements

Goal #1 Implement LRMP Projects

Action Items: 1 Update CS CIP based on updated CCTV inspections
2 Complete PS&E of Lift Station Rehabilitation Project
3 Board approval of CEQA and PS&E
4 Put project out to bid
5 Initiate construction of Lift Station Rehabilitation Project

Goal #2 Implement BESP Phase 1 Improvements

Action Items: 6 Complete final design and environmental review of BESP Phase 1 Improvements
7 Board approval of CEQA and PS&E
8 Determine construction timeline
9 Obtain regulatory permits
10 Put project out to bid
11 Integrate BESP improvements into LRMP

Goal #3 Implement Lystemize Refeed Pilot Project

Action Items: 12 Implement refeed test procedures and collect relevant data
13 Board consideration of proforma and potential for long term use
14 Update LRMP as needed

Goal #4 Complete Planned Office Space Improvements

Action Items: 15 Complete office space improvements in staff kitchen area

Responsibility: Board, GM, staff, contractor, consultants, legal counsel

Goleta Sanitary District 2021 Annual Plan Summary

CATEGORY #2 ENGINEERING

* Implement recommended reclamation facility filter improvements
* Initiate peer review/conceptual engineering analysis of onsite water reuse facility
* Update LRMP/CIP Storyboard and post to District Website
Analyze outfall access, structural integrity and cathodic protection alternatives
Analyze sludge dewatering alternatives

Goal #5 Investigate Reclamation Facility Filter Improvements

Action Items: 16 Implement recommended reclamation facility filter improvements

Goal #6 Initiate Review/Conceptual Engineering of onsite water reuse facility

Action Items: 17 Prepare and issue RFQ for engineering analysis
18 Select Consultant and complete study
19 Board consideration of study findings

Goal #7 Update LRMP/CIP Storyboard and post on District Website

Action Items: 20 Incorporate BESP and other new CIPs into LRMP and update CIP story map online

Goal #7 Analyze outfall access Structural integrity and cathodic protection alternatives

Action Items: 21 Incorporate BESP and other new CIPs into LRMP and update CIP story map online

Responsibility: Board, GM, staff, consultants, legal counsel

Goleta Sanitary District 2021 Annual Plan Summary

CATEGORY #3 FINANCE

- Adopt & Implement Capacity Exceedance Policy
- Conduct Rate Study based on results of CASA F&L Study
- Consider alternative project delivery and finance options for future capital projects

Goal #8 Adopt and Implement Capacity Exceedance Policy

Action Items: **22** Complete outreach to affected users and schedule public hearing on proposed
23 Board consideration of Capacity Exceedance Policy
24 Implement policy as directed by Board

Goal #9 Conduct rate study based on results from CASA's Flow & Loadings Study

Action Items: **25** Continue participation in CASA F&L study
26 Prepare RFQ/P for selection of rate study consultant
27 Board consideration of rate study consultant
28 Conduct rate study based on results of CASA F&L study
29 Board consideration of rate study
30 Board adoption new rate structure

Goal #10 Consider alternative project delivery and finance options for future capital projects

Action Items: **31** Research alternative project delivery and finance options for future capital projects
32 Board consideration of alternative project delivery and finance options

Responsibility: Board, GM, staff, consultants, legal counsel

Goleta Sanitary District 2021 Annual Plan Summary

Category #4 BOARD GOVERNANCE AND ORGANIZATIONAL MANAGEMENT

* Retain Platinum Level District of Distinction Recognition from CSDA
* Improve collaboration with partner agencies
* Implement District Based Elections Pursuant to CVRA
* Implement Effective Utility Management Practices
* Conduct triennial Board self-assessment

Goal #11 Retain Platinum Level District of Distinction Recognition from CSDA

Action Items: 33 Complete DOD training and tasks as required

34 Complete and submit DOD application to CSDA prior to deadline for consideration

Goal #12 Improve collaboration with partner agencies

Action Items: 1 Schedule meetings with UCSB on existing and future energy sustainability efforts

36 Schedule meetings with GWD and COG on expanded rec water/reuse

37 Schedule meetings with SBMA on pretreatment proposal

38 Meet with contract entities to consider approval of Multi-Jurisdictional Agreements

Goal #13 Implement District Based Elections Pursuant to the CVRA

Action Items: 39 Obtain 2020 Census demographic data

40 Conduct public hearings to gather public input on voting district areas

41 Prepare draft voting district maps

42 Conduct public hearings on proposed voting district areas

43 Adopt voting district areas and send information to County in time for 2022 election

Goal #13 Implement Effective Utility Management Practices

Action Items: 44 Prioritize and initiate implementation of identified EUM BMPs

Goal #14 Conduct triennial Board self-assessment

Action Items: 45 Conduct Board self-assessment

46 Board consideration of self-assessment recommendations

Responsibility: Board, GM, staff, legal counsel, consultants

Goleta Sanitary District 2021 Annual Plan Summary

CATEGORY #5 ENVIRONMENTAL STEWARDSHIP AND RESILIENCY PLANNING

* Maintain certification as Santa Barbara County Green Business
* Develop Outline for District Wide Resiliency Plan
* Develop Climate Adaptation and Business Continuity Plan

Goal #15 Maintain certification as Santa Barbara County Green Business

Action Items: **47** Review green business certification criteria to ensure compliance
48 Submit application if required to renew/maintain certification
49 Continue to support and participate in SBC Green Business program

Goal #17 Initiate Development of District Wide Resiliency Plan

Action Items: **50** Prepare draft RP
51 Board consideration of draft RP
52 Post approved RP on District website

Goal #18 Develop Climate Adaptation and Business Continuity Plans

Action Items: **53** Select consultant to assist with preparation of Climate Adaptation Plan
54 Prepare Draft Climate Adaptation Plan
55 Prepare Draft Business Continuity Plan
56 Board Consideration of Draft Climate Adaptation and Business Continuity Plans

Responsibility: Board, GM, staff, consultants, legal counsel

CATEGORY #6 OUTREACH PROGRAM

* Implement approved outreach program activities
* Develop outreach plan for election by Districts (CRVA) (Citizen academy)

Goal #19 Implement annual outreach program activities

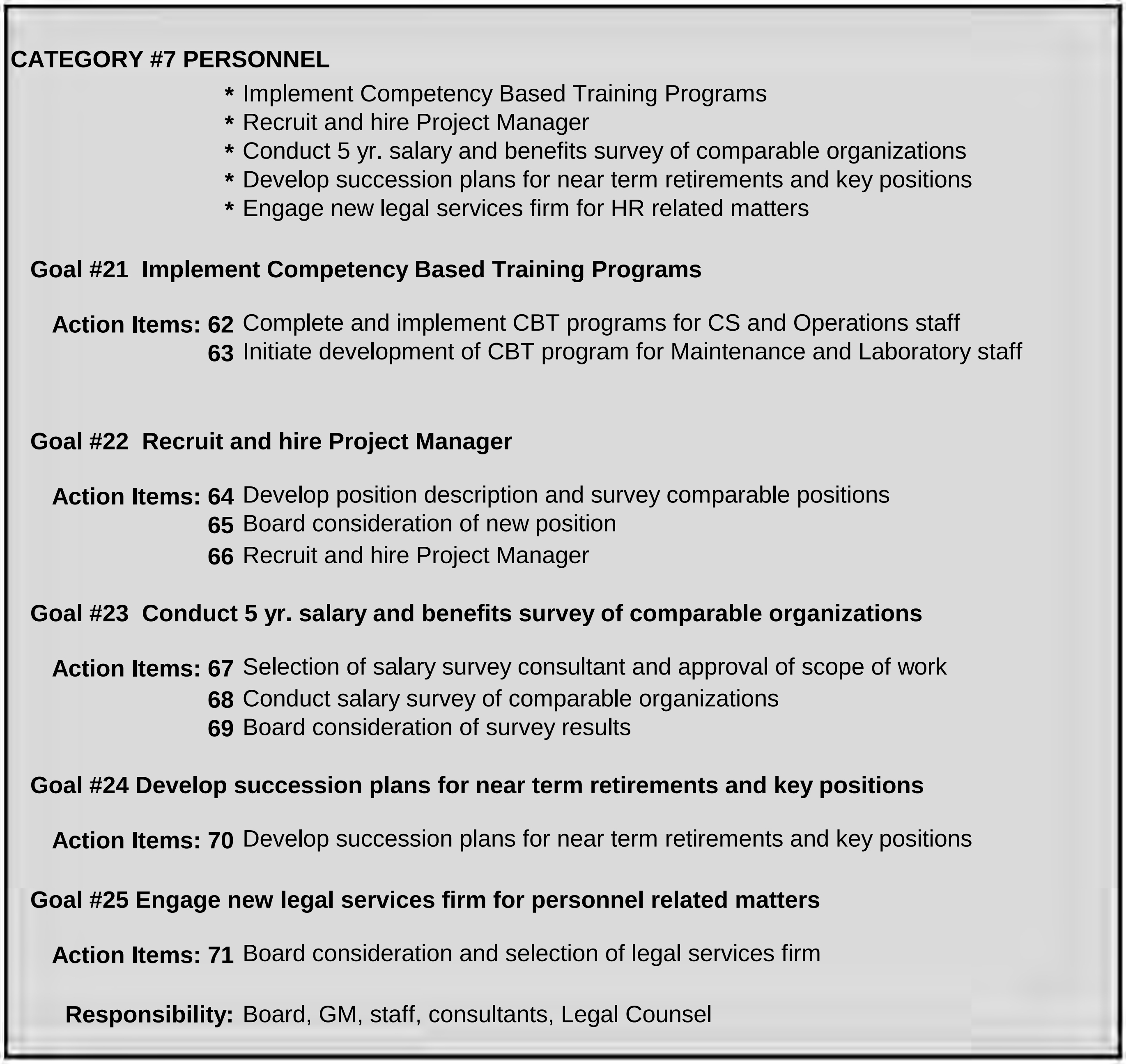
Action Items: **57** Review annual outreach program with Board Outreach Committee
58 Board consideration of annual outreach program

Goal #20 Develop Outreach Program for Transition to District Elections

Action Items: **59** Review election outreach program with Board Outreach Committee
60 Board consideration of election outreach program
61 Board consideration of establishment of Citizen Advisory Board or Academy

Responsibility: Board, GM, staff, consultants

Goleta Sanitary District 2021 Annual Plan Summary



CATEGORY #7 PERSONNEL

- Implement Competency Based Training Programs
- Recruit and hire Project Manager
- Conduct 5 yr. salary and benefits survey of comparable organizations
- Develop succession plans for near term retirements and key positions
- Engage new legal services firm for HR related matters

Goal #21 Implement Competency Based Training Programs

Action Items: **62** Complete and implement CBT programs for CS and Operations staff
63 Initiate development of CBT program for Maintenance and Laboratory staff

Goal #22 Recruit and hire Project Manager

Action Items: **64** Develop position description and survey comparable positions
65 Board consideration of new position
66 Recruit and hire Project Manager

Goal #23 Conduct 5 yr. salary and benefits survey of comparable organizations

Action Items: **67** Selection of salary survey consultant and approval of scope of work
68 Conduct salary survey of comparable organizations
69 Board consideration of survey results

Goal #24 Develop succession plans for near term retirements and key positions

Action Items: **70** Develop succession plans for near term retirements and key positions

Goal #25 Engage new legal services firm for personnel related matters

Action Items: **71** Board consideration and selection of legal services firm

Responsibility: Board, GM, staff, consultants, Legal Counsel

AGENDA ITEM #2

AGENDA ITEM: 2

MEETING DATE: April 5, 2021

I. NATURE OF ITEM

Consideration of Amendment to Ordinance No. 73 to Update Industrial Waste Control Permit Classifications to Correspond to Sewer Use Ordinance No. 92 and Revised Fee Schedule

II. BACKGROUND INFORMATION

During 2018-2020, a technical re-evaluation of the District's local limits and a review of the pretreatment program was conducted by outside contractors to ensure continued protection of the District's collection system and water resource recovery plant. In response to changing influent characteristics due to drought conditions and increased water conservation efforts, a decision was made to revise the industrial wastewater discharge permit classifications to add flexibility in controlling wastewater discharge from *all* types of non-residential users. The existing Industrial Waste Control (IWC) permit categories I–IV were regrouped into categories A, B, and C. These and other minor modifications were incorporated into the revised Sewer Use Ordinance (SUO) and adopted by the Board as Ordinance No. 92 on December 7, 2020. As is standard procedure, any changes made to the District's SUO, once adopted, must be incorporated into other relevant governing documents.

District Ordinance No. 73, adopted December 7, 2009, is the general regulation establishing the District's fees for plan checks, reviews, permits, inspections and deposits, including IWC permits. The fees under Ordinance No. 73 are subject to adjustment annually (on July 1st) to reflect any increases in the cost of living since the date of the last adjustment.

Modifications to Ordinance No. 73 are required to reflect the recent changes to the IWC permit categories included in Ordinance No. 92. No changes are currently proposed for the Collection System schedule of fees. The proposed fees for the new IWC permit categories are consistent with the fees for current permit classifications so that no existing users would be charged additional IWC permit fees due to the change in permit categories.

The attached memo prepared by District legal counsel sets forth a proposed timeline and a summary of the actions that need to be taken by the District to approve a revised schedule of fees for IWC permits.

II. COMMENTS AND RECOMMENDATIONS

It is recommended that the Board authorize the publication of a notice of a public hearing to be held on April 19, 2021 for the Board to (i) consider the adoption of an ordinance to update the IWC permit classifications to correspond to the current Ordinance No. 92 Section 6.8 IWC permit classifications, and (ii) approve a revised schedule of IWC permit fees.

IV. REFERENCE MATERIAL

Ordinance No. 73

Ordinance No. 92 Section 6.8 – Industrial Wastewater Discharge Permit Classification

Proposed “Schedule of Fees”, originally “Exhibit A” in Ordinance No. 73

Memo setting forth timeline and summary of required actions

Notice of Public Hearing

ORDINANCE NO. 73

ORDER OF THE GOVERNING BOARD OF THE GOLETA SANITARY DISTRICT ADOPTING AN ORDINANCE AND GENERAL REGULATION ESTABLISHING REVISED FEES FOR PLAN CHECKS, REVIEWS, PERMITS, INSPECTIONS AND DEPOSITS

WHEREAS, the Goleta Sanitary District (the "District") has completed an evaluation of the fees it charges for plan checks, reviews, permits, inspections and deposits (collectively, the "Fees"); and

WHEREAS, based on said evaluation, the Governing Board of the District has determined that adjustments to the Fees are necessary in order to cover the District's costs of providing service; and

WHEREAS, the District desires to adopt a revised schedule of Fees as set forth herein.

NOW, THEREFORE, BE IT ORDAINED by the Governing Board of the Goleta Sanitary District, as follows:

1. Repeal of Prior Enactments

All District ordinances, regulations, resolutions, policies, procedures and administrative provisions that are inconsistent with the provisions of this Ordinance, including but not limited to Ordinance No. 60 adopted on February 18, 2003, are hereby repealed.

2. Revised Fees

The schedule of Fees attached hereto as Exhibit "A" is hereby adopted.

3. Cost of Living Adjustments

The Fees shall be adjusted on July 1 of each year to reflect any increases in the cost of living since the date of the last adjustment, as determined pursuant to the Consumer Price Index published by the United States Department of Labor, Bureau of Labor Statistics, for the Los Angeles-Riverside-Orange County area (All Urban Consumers, All Items, 1982-1984 = 100). When calculating such increases, the Fees shall be rounded to the nearest whole dollar amount.

4. Use of Fees

Revenues derived from the collection of the Fees shall be placed in the District's Running Expense Fund pursuant to District Resolution No. 99-360. Said revenues shall be for the purpose of covering the District's administrative and labor costs associated with the services provided by the District.

5. General Findings

The Governing Board hereby finds that (a) the Fees adopted pursuant to this Ordinance are in an amount necessary to cover the District's administrative and labor costs, (b) in compliance with Article XIIIA Section 4 of the California Constitution and Sections 50076 of the Government Code, the Fees do not constitute a special tax requiring voter approval, and (c) the revenues forecast to be generated by the Fees do not exceed the estimated reasonable cost of providing the services for which the Fees are imposed.

6. CEQA Findings

The Governing Board hereby further finds that (a) under Section 21080(b)(8) of the Public Resources Code, this Ordinance only increases fees to meet operating expenses, including employee wage rates and fringe benefits, and to fund services associated with the operation of the District's sewer system, (b) there is no substantial evidence in the record before the District that this Ordinance or the adoption of the Fees will have a significant effect on the environment, and (c) no environmental review is required. In accordance with Section 21152(b) and (c) of the Public Resources Code, the Governing Board hereby directs the Secretary of the District to file a Notice of Exemption with the Santa Barbara County Clerk.

7. Partial Invalidity

If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be unconstitutional, ineffective, or in any manner in conflict with the laws of the United States, or the State of California, such decision shall not affect the validity of the remaining portions of this Ordinance. The Governing Board of the District hereby declares that it would have passed this Ordinance and each section, subsection, sentence, clause, and phrase, hereof, irrespective of the fact that any one or more section, subsection, sentence, clause, or phrase be declared unconstitutional, ineffective, or in any manner in conflict with the laws of the United States or the State of California.

8. Publication

The Secretary of the District is hereby directed to cause this Ordinance to be published once in a newspaper published in the District.

9. Effective Date

This Ordinance shall have an effective date of January 1, 2010.

ADOPTED, SIGNED, AND APPROVED this 7th day of December, 2009, by the following vote of the Governing Board of the Goleta Sanitary District:

AYES: Fox, Carter, Majoewsky, Emerson, Smith

NOES: None

ABSENT: None

ABSTAIN: None

COPY

John R. Fox, President
of the Governing Board

COUNTERSIGNED:

COPY

Kamil S. Azoury, Secretary
of the Governing Board

EXHIBIT "A"

FEES EFFECTIVE JANUARY 1, 2010

COLLECTION SYSTEM

PERMIT TYPE	FEES
Plan check and review fees (commercial/industrial and large development projects only)	Minimum fee: $100.00 (Per hour rate: $100.00)
Permit fees	$150.00
Inspection fees	$150.00
Inspection fees for industrial establishments	$200.00
Mainline inspections	$400/100 ft
Cleanouts/inspection only - no permit fees	N/A
Deposit	$500.00 (Maximum)

INDUSTRIAL WASTE CONTROL

PERMIT TYPE	FEES	
	Initial Fee*	Renewal Fee*
Class I, 0	$200.00	$100.00
Class II, 12	$400.00	$200.00
Class III, 24	$800.00	$400.00
Class IV, SIU, 1	$1,200.00	$600.00
Class IV CIU, 11	$1,600.00	$800.00
Restaurants	$300.00	$150.00
"Zero-discharge"	$100.00	$50.00

* The District reserves the right to charge industrial users the initial fee instead of the renewal fee if the District determines that the renewed permit contains significant changes.

The fees set forth in this Exhibit "A" are subject to adjustment on July 1 of each year to reflect any increases in the cost of living since the date of the last adjustment.

Notice of Exemption

TO: □ Office of Planning and Research
P.O. Box 3044
1400 Tenth Street, Room 222
Sacramento, CA 95812-3044

or

☒ County Clerk
County of Santa Barbara
105 E. Anapamu Street
Santa Barbara, CA, 93101

FROM: Goleta Sanitary District
One William Moffett Place
Goleta, CA 93117

Project Title: Adoption of Ordinance No. 73 revising fees for conducting plan checks, reviews and inspections and issuing permits

Project Location – Specific: Throughout Goleta Sanitary District

Project Location – City: City of Goleta, City of Santa Barbara and unincorporated areas

Project Location – County: Santa Barbara

Description of Project: Ordinance adopting revised fees for conducting plan checks, reviews and inspections and issuing permits

Name of Public Agency approving project: Goleta Sanitary District

Name of Person or Agency carrying out project: Goleta Sanitary District

Exempt status: (check one)

□ Ministerial project.

□ Not a project.

□ Emergency Project.

□ Categorical Exemption.
State type and class number:

□ Declared Emergency.

☒ Statutory Exemption.
State Code section number: Section 21080(b)(8) of Public Resources Code

□ Other. Explanation:

Reason why project is exempt:

Rate increase for services of the kind described in Section 21080(b)(8) of the Public Resources Code to fund operating expenses, including employee wage rates and fringe benefits, and to fund services associated with the operation of the District's sewer system within the existing service area of the District. There is no substantial evidence that this ordinance or the change in fees will have a significant effect on the environment.

Lead Agency
Contact Person: Kamil S. Azoury

Telephone: (805) 967-4519

Signature of Lead Agency Representative:

COPY

Kamil S. Azoury, General Manager

Dated: December 7, 2009

Date Received for Filing: ______________________

ORDINANCE NO. 92

ORDER OF THE GOVERNING BOARD OF THE GOLETA SANITARY DISTRICT ADOPTING AN ORDINANCE AND GENERAL REGULATION REGULATING THE USE OF THE GOLETA SANITARY DISTRICT SEWERAGE SYSTEM AND REPEALING ORDINANCE NO. 77

BE IT ORDAINED by the Governing Board of the Goleta Sanitary District of the County of Santa Barbara, State of California, that the following ordinance and general regulation be adopted:

TABLE OF CONTENTS

Section 6 – INDIVIDUAL WASTEWATER DISCHARGE PERMITS

6.8 Industrial Wastewater Discharge Permit Classification

Industrial Wastewater Discharge Permits shall be classified as follows:

Class A: This classification is for Significant Industrial Users, SIUs, defined in Section 1.4 of this ordinance, and are industrial users regulated under National Categorical Pretreatment Standards, and/or have a reasonable potential for adversely affecting the POTW’s operation or for violating any Pretreatment Standard or Requirement.

Class B: This classification is for Industrial Users that are not classified as an SIU, but may require a permit to communicate and formalize industrial wastewater discharge rules and obligations i.e. implementation of Best Management Practice(s), District inspection/compliance monitoring, equipment installation, self-monitoring/reporting, etc. and will involve verification of ongoing compliance with this ordinance and pretreatment standards or requirements.

Class C: This classification is for:

(1) non-residential users that handle and store toxic or hazardous wastes on site but can demonstrate and certify that they do not directly or indirectly discharge these wastes to the sewer.

(2) Users who require discharge approval for a temporary and/or short-term duration.

(3) Users that have the same or substantially similar types of operations, discharge same types of waste, require similar compliance monitoring and/or best management practices, require the same standard treatment equipment and are more appropriately controlled under this type of document.

These non-residential users may be required to submit (a) an application for a Class C permit setting forth requirements for self-monitoring, reporting, and/or equipment installation, or (b) a certified zero industrial wastewater discharge statement setting forth such survey or other information as the District may require to establish that such user will not directly or indirectly discharge toxic or hazardous wastes to the sewer.

PROPOSED AMENDED EXHIBIT "A"

FEES

COLLECTION SYSTEM Effective January 1, 2010	
PERMIT TYPE	**FEES**
Plan check and review fees (commercial/industrial and large development projects only)	Minimum fee: $100.00 (Per hour rate: $100.00)
Permit fees	$150.00
Inspection fees	$150.00
Inspection fees for industrial establishments	$200.00
Mainline inspections	$400/100 ft
Cleanouts/inspection only - no permit fees	N/A
Deposit	$500.00 (Maximum)

INDUSTRIAL WASTE CONTROL PERMITS Effective May 1, 2021		
PERMIT TYPE	**FEES**	
	Initial Fee*	**Renewal Fee***
Class A	$2000	$1000
Class B	$500	$248
Class C	$126	$63

* The District reserves the right to charge users the initial fee instead of the renewal fee if the District determines that the renewed permit contains significant changes.

The fees set forth in this Amended Exhibit "A" are subject to adjustment on July 1 of each year to reflect any increases in the cost of living since the that date the fees or were established or the date of the last adjustment, whichever is more recent.

HM
&G

HOWELL MOORE & GOUGH
ATTORNEYS AT LAW • LLP

MEMO

To: Steve D. Wagner

From: Richard G. Battles

Subject: Procedures for Approving Revised Fees for Industrial Waste Control Permits

Date: March 29, 2021

Set forth below is a proposed timeline and a summary of the actions that need to be taken by the Goleta Sanitary District to approve a revised schedule of fees for industrial waste control permits.

DATE	LAW	ACTION
April 5, 2021		• The District's Governing Board authorizes the scheduling and noticing of a public hearing to consider the revised fee schedule.
By April 8, 2021	Gov. Code §§6062a and 66018.	• The District publishes a notice of the time and place of the hearing to consider the revised fee schedule. • Publication shall be for 10 days in a newspaper regularly published once a week or oftener. Two publications, with at least five days intervening between the dates of first and last publication not counting such publication dates, are sufficient. The period of notice commences upon the first day of publication and terminates at the end of the tenth day, including the first day.
April 19, 2021	Gov. Code §66018; H&S Code §§5471 and 6520.5.	• Following the expiration of the 10-day publication period set forth above, the District conducts a public hearing to consider oral or written presentations regarding the proposed fee revisions. • The District adopts a resolution by a

		majority vote setting forth CEQA findings, approving a Preliminary Environmental Review form and authorizing the filing of a Notice of Exemption. • The Governing Board adopts an ordinance by a 2/3 vote approving the revised fee schedule and setting forth findings.
By April 23, 2021	H&S Code §§6490 and 6491.3; Pub. Resources Code §21152(b); 14 Cal. Code Reg. §15062.	• The ordinance is entered in the District's minutes. • The ordinance is published once in a newspaper published in the District. • A notice of exemption under CEQA is filed with the County Clerk.[1]
May 1, 2021	H&S Code §6490	• The ordinance takes effect upon the expiration of the week of publication, unless a later date is specified in the ordinance. May 1 is the proposed date for the Ordinance to become effective.

[1] The filing of a notice of exemption and the posting of the notice starts a 35-day statute of limitations period on legal challenges to the District's decision that the project is exempt from CEQA. 14 Cal. Code Reg. §15062(d).

GOLETA SANITARY DISTRICT

NOTICE OF HEARING ON PROPOSED ORDINANCE
AND GENERAL REGULATION ESTABLISHING REVISED
FEES FOR INDUSTRIAL WASTE CONTROL PERMITS

NOTICE IS HEREBY GIVEN that the Goleta Sanitary District will hold a public hearing to consider the adoption of an ordinance establishing revised fees for industrial waste control permits. The time and place for the hearing on said ordinance has been set for Monday April 19, 2021, at 6:30 p.m. at the Board Room of the Goleta Sanitary District, One William Moffett Place, Goleta, California.

Members of the public who wish to observe the hearing and/or offer comments by video conferencing should contact the District at least four (4) hours before the hearing at (805) 967-4519 or RMangus@GoletaSanitary.org to obtain the meeting ID and passcode.

Dated: April 5, 2021

AGENDA ITEM #3

AGENDA ITEM: 3

MEETING DATE: April 5, 2021

I. NATURE OF ITEM

Discussion and Consideration of Cyber Security Control Standards

II. BACKGROUND INFORMATION

The District relies on a wide range of computer technologies and systems to provide wastewater collection, treatment and disposal services to the Goleta Valley. As the prevalence of cyber-attacks continues to increase across all business sectors, the risk of cyber related attacks on the District’s computer systems also continues to increase. Cyber security and risk mitigation have been common topics at recent wastewater seminars and conferences.

In response to this growing concern, the District adopted the Center for Internet Security’s (CIS’s) control standards in 2019 to improve its cyber security posture.

The CIS publishes the *CIS Critical Security Controls* (CSC) to help organizations better defend against known attacks by distilling key security concepts into actionable controls to achieve greater overall cyber security defense. The California Sanitation Risk Management Agency (CRSMA) has recommended that agencies implement the CIS controls to reduce cyber security risk.

A principal benefit of the CIS Controls (Controls) is the priority and focus on a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. The list of controls was created by a group of cyber security experts from the National Security Agency (NSA), the US Department of Energy nuclear energy labs, law enforcement organizations and some of the nation's top forensics and incident response organizations. The Controls are updated based on new attacks that are identified and analyzed by groups from Verizon and Symantec so the Controls can stop or mitigate those attacks.

There are currently 20 Controls that are organized into 3 categories: Basic, Foundational and Organizational. Each control has a list of recommended actions (sub-controls) to ensure effective implementation. There are a total of 172 recommended sub-controls. 142 of these are being considered for implementation at the District. A copy of the *CIS Controls Version 7 Summary* and list of all the controls along with a status report of the controls being considered for implementation is attached to this report.

As of the end of 2020, 79 of the recommended control standards have been implemented or are in progress, 59 are pending and 4 have been reviewed and dropped as they are not applicable to our systems. A majority of the remaining controls (to be implemented) deal with the ongoing training of staff on how to identify potential cyber threats and reduce exposure and risk.

Implementation of the remaining control standards will continue through the end of FY 2021-22.

III. COMMENTS AND RECOMMENDATIONS

Effective cyber security is not a single effort, product or even a secure system but rather an operational mindset to be incorporated at all levels of the organization. The adoption and implementation of the CIS control standards is a key step in this process. Staff will continue to work toward full implementation of the CIS control standards and any future updates in order to improve the District's cyber security and minimize the risk of cyber-attacks.

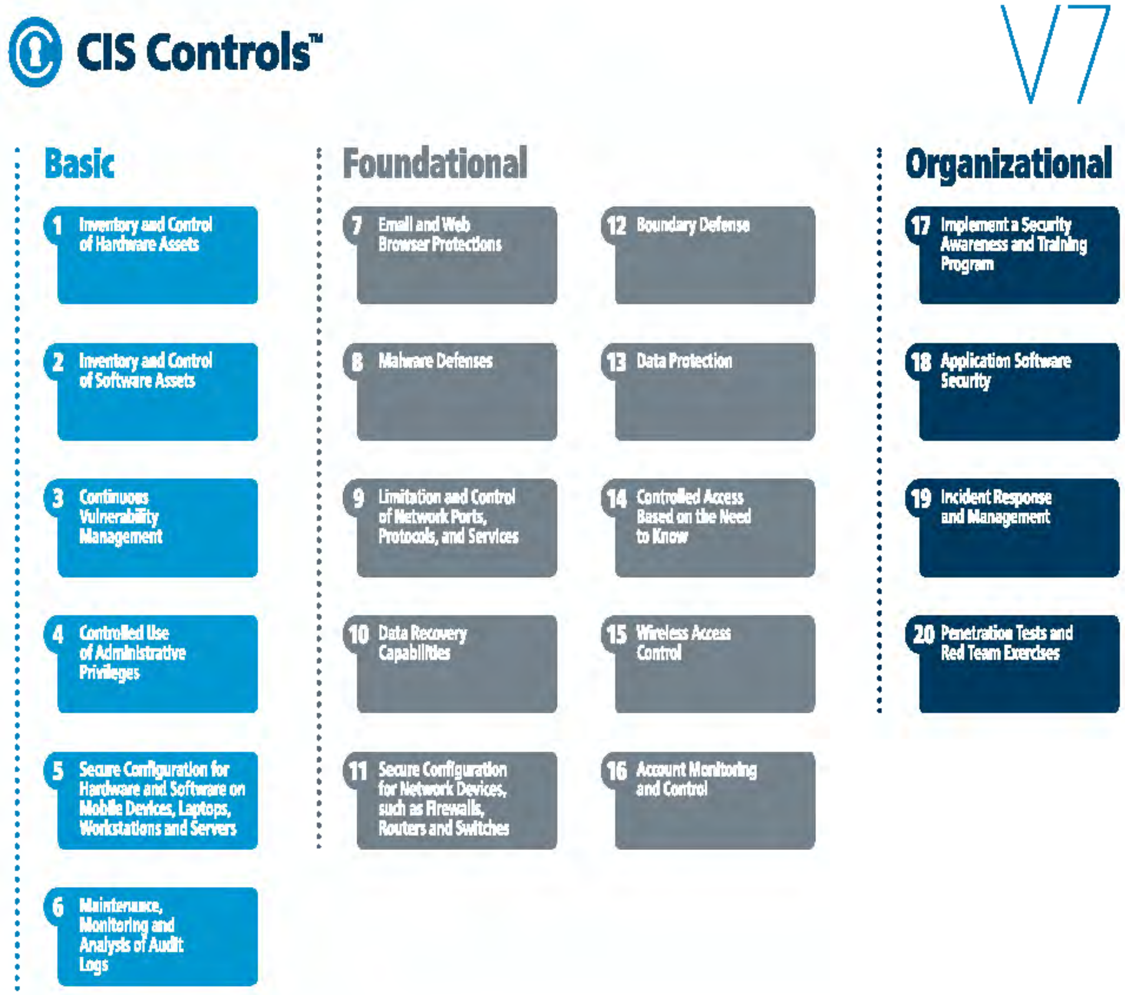
This report is for informational purposes only. As such, no Board action is required at this time.

IV. REFERENCE MATERIAL

CISC Version 7 Summary and List

CIS Controls Implementation Status Report

CIS. Center for Internet Security®



CIS Controls™ V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

CIS Controls Version 7

March 2018 marks the release of CIS Controls Version 7, the newest iteration of these 20 important cybersecurity recommendations. The CIS Controls are a prioritized set of actions any organization can follow to improve their cybersecurity posture.

Cybersecurity + Community

Version 7 of the CIS Controls was developed over the last year to align with the latest cyber threat data and reflect today's current threat environment. We recognize that the cybersecurity world is constantly shifting and reacting to new threats and vulnerabilities, that often results in chaos and confusion about which steps to take in order to harden systems and data.

In order to cut through the confusion, we collaborated on CIS Controls V7 with a global community of cybersecurity experts – leaders in academia, industry, and government – to secure input from volunteers at every level. Our public call for comment on Version 7 from January 24 – February 7, 2018 included feedback from a community of over 300 individuals dedicated to improving cybersecurity for all. The CIS Controls best practices are developed using a consensus approach involving discussion groups, forums, and community feedback.

Key Principles

The development of CIS Controls V7 was guided by 7 key principles which helped ensure a more robust end result.

1. **Address current attacks, emerging technology, and changing mission/business requirements for IT:** As part of our fundamental promise, the CIS Controls have been updated and re-ordered to reflect both the availability of new cybersecurity tools and changes in the current threat landscape that all organizations are facing**.**

2. **Bring more focus to key topics like authentication, encryptions, and application whitelisting:** Guidance for each of these major security topics is covered in detail by CIS Controls V7 in a clearer, stronger, and more consistent fashion across the entire CIS Controls.

3. **Better align with other frameworks:** With mapping to NIST Cybersecurity Framework, it's never been easier to function in a multi-framework world.

4. **Improve the consistency and simplify the wording of each sub-control – one "ask" per sub-control:** The community worked tirelessly to clarify and simplify each CIS Control, making it easier for users to follow along. By eliminating multiple tasks within a single sub-control, the CIS Controls are easier to measure, monitor, and implement.

5. **Set the foundation for a rapidly growing "ecosystem" of related products ad services from both CIS and the marketplace:** We have much more documented experience with adopters and vendors since Version 6; for V7 we make it easier for everyone to understand, track, import, integrate the CIS Controls into products, services, and corporate decision-making**.**

6. **Make some structural changes in layout and format:** To help keep the Controls relevant and adaptive to various different organizations, we've restructured our content to be more flexible than before.

7. **Reflect the feedback of a world-side community of volunteers, adopters, and supporters:** We are only as strong as the amazing volunteers that support us and we hope to continue to provide a means of gathering and harnessing the global cybersecurity community for the benefit of everyone.

By following these 7 key principles, the CIS Controls have become a more flexible, measurable, and helpful resource for any business or organization looking to secure its systems and data.

Version 7 – What's Old, What's New

CIS Controls V7 keeps the same 20 controls that businesses and organizations around the world already depend upon to stay secure; however, the ordering has been updated to reflect the current threat landscape. We've also updated the sub-controls to be more clear and precise, implementing a single "ask" per sub-control.

CIS Controls V7 separates the controls into three distinct categories: basic, foundational, and organizational.

- **Basic (CIS Controls 1-6):** Key controls which should be implemented in every organization for essential cyber defense readiness.

- **Foundational (CIS Controls 7-16):** The next step up from basic – these technical best practices provide clear security benefits and are a smart move for any organization to implement.

- **Organizational (CIS Controls 17-20):** These controls are different in character from 1-16; while they have many technical elements, CIS Controls 17-20 are more focused on people and processes involved in cybersecurity.

At CIS, we listen carefully to all of your feedback and ideas for the CIS Controls. In particular, many of you have asked for more help with prioritizing and phasing in the CIS Controls for your cybersecurity program. This topic deserves more thought than we had time for in this Version 7 update, so we've decided to address it separately in the near future. We'll soon be surveying CIS Controls adopters to better understand your needs in this area. You can also help out by sending us your feedback and ideas on prioritization now (controlsinfo@cisecurity.org), or by joining the CIS WorkBench Community (https://workbench.cisecurity.org/communities/71).

The CIS Controls Version 7 in PDF format contains additional narratives around each CIS Control.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description
1				**Inventory and Control of Hardware Assets**	
1	1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
1	1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.
1	1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.
1	1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.
1	1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.
1	1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.
1	1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.
1	1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.
2				**Inventory and Control of Software Assets**	
2	2.1	Applications	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.
2	2.2	Applications	Identify	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
2	2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
2	2.4	Applications	Identify	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.
2	2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

2	2.6	Applications	Respond	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner
2	2.7	Applications	Protect	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
2	2.8	Applications	Protect	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.
2	2.9	Applications	Protect	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.
2	2.10	Applications	Protect	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.
3				**Continuous Vulnerability Management**	
3	3.1	Applications	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
3	3.2	Applications	Detect	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.
3	3.3	Users	Protect	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
3	3.4	Applications	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
3	3.5	Applications	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
3	3.6	Applications	Respond	Compare Back-to-back Vulnerability Scans	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
3	3.7	Applications	Respond	Utilize a Risk-rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.
4				**Controlled Use of Administrative Privileges**	
4	4.1	Users	Detect	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
4	4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

4	4.3	Users	Protect	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
4	4.4	Users	Protect	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
4	4.5	Users	Protect	Use Multifactor Authentication For All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.
4	4.6	Users	Protect	Use of Dedicated Machines For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
4	4.7	Users	Protect	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.
4	4.8	Users	Detect	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.
4	4.9	Users	Detect	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.
5				**Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**	
5	5.1	Applications	Protect	Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized operating systems and software.
5	5.2	Applications	Protect	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
5	5.3	Applications	Protect	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
5	5.4	Applications	Protect	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
5	5.5	Applications	Detect	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.
6				**Maintenance, Monitoring and Analysis of Audit Logs**	
6	6.1	Network	Detect	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
6	6.2	Network	Detect	Activate audit logging	Ensure that local logging has been enabled on all systems and networking devices.

6	6.3	Network	Detect	Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
6	6.4	Network	Detect	Ensure adequate storage for logs	Ensure that all systems that store logs have adequate storage space for the logs generated.
6	6.5	Network	Detect	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
6	6.6	Network	Detect	Deploy SIEM or Log Analytic tool	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.
6	6.7	Network	Detect	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.
6	6.8	Network	Detect	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.
7				**Email and Web Browser Protections**	
7	7.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.
7	7.2	Applications	Protect	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.
7	7.3	Applications	Protect	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.
7	7.4	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
7	7.5	Network	Protect	Subscribe to URL-Categorization service	Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.
7	7.6	Network	Detect	Log all URL requests	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.
7	7.7	Network	Protect	Use of DNS Filtering Services	Use DNS filtering services to help block access to known malicious domains.
7	7.8	Network	Protect	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.
7	7.9	Network	Protect	Block Unnecessary File Types	Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.

7	7.10	Network	Protect	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.
8				**Malware Defenses**	
8	8.1	Devices	Protect	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.
8	8.2	Devices	Protect	Ensure Anti-Malware Software and Signatures are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
8	8.3	Devices	Protect	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.
8	8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
8	8.5	Devices	Protect	Configure Devices Not To Auto-run Content	Configure devices to not auto-run content from removable media.
8	8.6	Devices	Detect	Centralize Anti-malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.
8	8.7	Network	Detect	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.
8	8.8	Devices	Detect	Enable Command-line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.
9				**Limitation and Control of Network Ports, Protocols, and Services**	
9	9.1	Devices	Identify	Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.
9	9.2	Devices	Protect	Ensure Only Approved Ports, Protocols and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.
9	9.3	Devices	Detect	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.
9	9.4	Devices	Protect	Apply Host-based Firewalls or Port Filtering	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
9	9.5	Devices	Protect	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

10				**Data Recovery Capabilities**	
10	10.1	Data	Protect	Ensure Regular Automated Back Ups	Ensure that all system data is automatically backed up on regular basis.
10	10.2	Data	Protect	Perform Complete System Backups	Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
10	10.3	Data	Protect	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
10	10.4	Data	Protect	Ensure Protection of Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
10	10.5	Data	Protect	Ensure Backups Have At least One Non-Continuously Addressable Destination	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.
11				**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches**	
11	11.1	Network	Identify	Maintain Standard Security Configurations for Network Devices	Maintain standard, documented security configuration standards for all authorized network devices.
11	11.2	Network	Identify	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.
11	11.3	Network	Detect	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.
11	11.4	Network	Protect	Install the Latest Stable Version of Any Security-related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.
11	11.5	Network	Protect	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.
11	11.6	Network	Protect	Use Dedicated Machines For All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.
11	11.7	Network	Protect	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.
12				**Boundary Defense**	
12	12.1	Network	Identify	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.

12	12.2	Network	Detect	Scan for Unauthorized Connections across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.
12	12.3	Network	Protect	Deny Communications with Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.
12	12.4	Network	Protect	Deny Communication over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.
12	12.5	Network	Detect	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.
12	12.6	Network	Detect	Deploy Network-based IDS Sensor	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.
12	12.7	Network	Protect	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.
12	12.8	Network	Detect	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.
12	12.9	Network	Detect	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.
12	12.10	Network	Detect	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
12	12.11	Users	Protect	Require All Remote Login to Use Multi-factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.
12	12.12	Devices	Protect	Manage All Devices Remotely Logging into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.
13				**Data Protection**	
13	13.1	Data	Identify	Maintain an Inventory Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.
13	13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.
13	13.3	Data	Detect	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.
13	13.4	Data	Protect	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.

13	13.5	Data	Detect	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.
13	13.6	Data	Protect	Encrypt the Hard Drive of All Mobile Devices.	Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.
13	13.7	Data	Protect	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.
13	13.8	Data	Protect	Manage System's External Removable Media's Read/write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.
13	13.9	Data	Protect	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.
14				**Controlled Access Based on the Need to Know**	
14	14.1	Network	Protect	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).
14	14.2	Network	Protect	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.
14	14.3	Network	Protect	Disable Workstation to Workstation Communication	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.
14	14.4	Data	Protect	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.
14	14.5	Data	Detect	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.
14	14.6	Data	Protect	Protect Information through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.
14	14.7	Data	Protect	Enforce Access Control to Data through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.
14	14.8	Data	Protect	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.
14	14.9	Data	Detect	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).
15				**Wireless Access Control**	

15	15.1	Network	Identify	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.
15	15.2	Network	Detect	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.
15	15.3	Network	Detect	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.
15	15.4	Devices	Protect	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.
15	15.5	Devices	Protect	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.
15	15.6	Devices	Protect	Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.
15	15.7	Network	Protect	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.
15	15.8	Network	Protect	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.
15	15.9	Devices	Protect	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.
15	15.10	Network	Protect	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.
16				**Account Monitoring and Control**	
16	16.1	Users	Identify	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.
16	16.2	Users	Protect	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.
16	16.3	Users	Protect	Require Multi-factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.
16	16.4	Users	Protect	Encrypt or Hash all Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.
16	16.5	Users	Protect	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

16	16.6	Users	Identify	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.
16	16.7	Users	Protect	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.
16	16.8	Users	Respond	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.
16	16.9	Users	Respond	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.
16	16.10	Users	Protect	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.
16	16.11	Users	Protect	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.
16	16.12	Users	Detect	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.
16	16.13	Users	Detect	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.
17				**Implement a Security Awareness and Training Program**	
17	17.1	N/A	N/A	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.
17	17.2	N/A	N/A	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.
17	17.3	N/A	N/A	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.
17	17.4	N/A	N/A	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.
17	17.5	N/A	N/A	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.
17	17.6	N/A	N/A	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.
17	17.7	N/A	N/A	Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.

17	17.8	N/A	N/A	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
17	17.9	N/A	N/A	Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.
18				**Application Software Security**	
18	18.1	N/A	N/A	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.
18	18.2	N/A	N/A	Ensure Explicit Error Checking is Performed for All In-house Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.
18	18.3	N/A	N/A	Verify That Acquired Software is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.
18	18.4	N/A	N/A	Only Use Up-to-date And Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.
18	18.5	N/A	N/A	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized and extensively reviewed encryption algorithms.
18	18.6	N/A	N/A	Ensure Software Development Personnel are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.
18	18.7	N/A	N/A	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.
18	18.8	N/A	N/A	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.
18	18.9	N/A	N/A	Separate Production and Non-Production Systems	Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.
18	18.10	N/A	N/A	Deploy Web Application Firewalls (WAFs)	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.
18	18.11	N/A	N/A	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.
19				**Incident Response and Management**	
19	19.1	N/A	N/A	Document Incident Response Procedures	Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.

19	19.2	N/A	N/A	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.
19	19.3	N/A	N/A	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.
19	19.4	N/A	N/A	Devise Organization-wide Standards for Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.
19	19.5	N/A	N/A	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.
19	19.6	N/A	N/A	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.
19	19.7	N/A	N/A	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.
19	19.8	N/A	N/A	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.
20				**Penetration Tests and Red Team Exercises**	
20	20.1	N/A	N/A	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.
20	20.2	N/A	N/A	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.
20	20.3	N/A	N/A	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.
20	20.4	N/A	N/A	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.
20	20.5	N/A	N/A	Create Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.
20	20.6	N/A	N/A	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.
20	20.7	N/A	N/A	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.
20	20.8	N/A	N/A	Control and Monitor Accounts Associated with Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.

CIS Status as of December, 2020

control	sub-control	description	status	note
1	1.1	Utilize an Active Discovery Tool	Live	
1	1.3	Use DHCP Logging to Update Asset Inventory	Live	
1	1.4	Maintain Detailed Asset Inventory	Live	
1	1.5	Maintain Asset Inventory Information	Live	
1	1.6	Address Unauthorized Assets	Live	
1	1.7	Deploy Port Level Access Control	Pending	
2	2.1	Maintain Inventory of Authorized Software	Live	
2	2.2	Ensure Software is Supported by Vendor	In Progress	
2	2.3	Utilize Software Inventory Tools	Live	
2	2.4	Track Software Inventory Information	In Progress	
2	2.6	Address unapproved software	In Progress	
3	3.1	Run Automated Vulnerability Scanning Tools	Live	
3	3.2	Perform Authenticated Vulnerability Scanning	Live	
3	3.3	Protect Dedicated Assessment Accounts	Live	
3	3.4	Deploy Automated Operating System Patch Management Tools	In Progress	
3	3.5	Deploy Automated Software Patch Management Tools	In Progress	
3	3.6	Compare Back-to-Back Vulnerability Scans	Live	
3	3.7	Utilize a Risk-Rating Process	Live	
4	4.1	Maintain Inventory of Administrative Accounts	Live	
4	4.2	Change Default Passwords	Live	
4	4.3	Ensure the Use of Dedicated Administrative Accounts	Live	
4	4.4	Use Unique Passwords	Live	
4	4.5	Use Multi-Factor Authentication for All Administrative Access	Live	
4	4.6	Use Dedicated Workstations For All Administrative Tasks	Pending	
4	4.7	Limit Access to Script Tools	Live	
4	4.8	Log and Alert on Changes to Administrative Group Membership	Pending	
4	4.9	Log and Alert on Unsuccessful Administrative Account Login	Live	
5	5.1	Establish Secure Configurations	Live	
5	5.2	Maintain Secure Images	Pending	
5	5.3	Securely Store Master Images	Pending	
5	5.4	Deploy System Configuration Management Tools	Pending	
5	5.5	Implement Automated Configuration Monitoring Systems	Pending	

6	6.1	Utilize Three Synchronized Time Sources	Pending
6	6.2	Activate Audit Logging	Live
6	6.3	Enable Detailed Logging	Live
6	6.4	Ensure Adequate Storage for Logs	Live
6	6.5	Central Log Management	In Progress
6	6.6	Deploy SIEM or Log Analytic Tools	Live
6	6.7	Regularly Review Logs	Live
7	7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	In Progress
7	7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Pending
7	7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients	Pending
7	7.4	Maintain and Enforce Network-Based URL Filters	Live
7	7.5	Subscribe to URL-Categorization Service	Live
7	7.6	Log All URL requester	Pending
7	7.7	Use of DNS Filtering Services	Live
7	7.8	Implement DMARC and Enable Receiver-Side Verification	In Progress
7	7.9	Block Unnecessary File Types	Live
8	8.1	Utilize Centrally Managed Anti-malware Software	Live
8	8.2	Ensure Anti-Malware Software and Signatures Are Updated	Live
8	8.3	Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies	Live
8	8.4	Configure Anti-Malware Scanning of Removable Devices	Live
8	8.5	Configure Devices to Not Auto-Run Content	Pending
8	8.6	Centralize Anti-Malware Logging	Pending
8	8.7	Enable DNS Query Logging	Live
8	8.8	Enable Command-Line Audit Logging	Live
9	9.1	Associate Active Ports, Services, and Protocols to Asset Inventory	Pending
9	9.2	Ensure Only Approved Ports, Protocols, and Services Are Running	Pending
9	9.3	Perform Regular Automated Port Scans	Live
9	9.4	Apply Host-Based Firewalls or Port-Filtering	Live
10	10.1	Ensure Regular Automated BackUps	Live
10	10.2	Perform Complete System Backups	Live
10	10.3	Test Data on Backup Media	Live
10	10.4	Protect Backups	Live
10	10.5	Ensure All Backups Have at Least One Offline Backup Destination	Live
11	11.1	Maintain Standard Security Configurations for Network Devices	Pending

11	11.2	Document Traffic Configuration Rules	Pending
11	11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Pending
11	11.4	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Live
11	11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Live
11	11.6	Use Dedicated Machines For All Network Administrative Tasks	Pending
11	11.7	Manage Network Infrastructure Through a Dedicated Network	Pending
12	12.1	Maintain an Inventory of Network Boundaries	Live
12	12.2	Scan for Unauthorized Connections Across Trusted Network Boundaries	In Progress
12	12.3	Deny Communications With Known Malicious IP Addresses	Live
12	12.4	Deny Communication Over Unauthorized Ports	In Progress
12	12.5	Configure Monitoring Systems to Record Network Packets	Pending
12	12.6	Deploy Network-Based IDS Sensors	Live
12	12.8	Deploy NetFlow Collection on Networking Boundary Devices	Pending
12	12.11	Require All Remote Login to Use Multi-Factor Authentication	Live
13	13.1	Maintain an Inventory of Sensitive Information	Pending
13	13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Pending
13	13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	Pending
13	13.6	Encrypt Mobile Device Data	In Progress
13	13.7	Manage USB Devices	Pending
14	14.1	Segment the Network Based on Sensitivity	Pending
14	14.2	Enable Firewall Filtering Between VLANs	Pending
14	14.3	Disable Workstation to Workstation Communication	In Progress
14	14.4	Encrypt All Sensitive Information in Transit	Pending
14	14.6	Protect Information Through Access Control Lists	Live
15	15.1	Maintain an Inventory of Authorized Wireless Access Points	Live
15	15.2	Detect Wireless Access Points Connected to the Wired Network	Pending
15	15.3	Use a Wireless Intrusion Detection System	Pending
15	15.6	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Pending
15	15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	In Progress
15	15.9	Disable Wireless Peripheral Access of Devices	Pending
15	15.1	Create Separate Wireless Network for Personal and Untrusted Devices	Live
16	16.1	Maintain an Inventory of Authentication Systems	Live
16	16.2	Configure Centralized Point of Authentication	Live
16	16.3	Require Multi-Factor Authentication	Pending

16	16.4	Encrypt or Hash all Authentication Credentials	In Progress	
16	16.5	Encrypt Transmittal of Username and Authentication Credentials	live	
16	16.6	Maintain an Inventory of Accounts	In Progress	
16	16.7	Establish Process for Revoking Access	Live	
16	16.8	Disable Any Unassociated Accounts	Live	
16	16.9	Disable Dormant Accounts	In Progress	
16	16.1	Ensure All Accounts Have An Expiration Date	In Progress	
16	16.11	Lock Workstation Sessions After Inactivity	Live	
16	16.12	Monitor Attempts to Access Deactivated Accounts	Live	
17	17.1	Perform a Skills Gap Analysis	Pending	
17	17.2	Deliver Training to Fill the Skills Gap	Pending	
17	17.3	Implement a Security Awareness Program	Pending	
17	17.4	Update Awareness Content Frequently	Pending	
17	17.5	Train Workforce on Secure Authentication	Pending	
17	17.6	Train Workforce on Identifying Social Engineering Attacks	Pending	
17	17.7	Train Workforce on Sensitive Data Handling	Pending	
17	17.8	Train Workforce on Causes of Unintentional Data Exposure	Pending	
17	17.9	Train Workforce Members on Identifying and Reporting Incidents	Pending	
18	18.1	Establish Secure Coding Practices	Pending	
18	18.2	Ensure That Explicit Error Checking is Performed for All In-House Developed Software	n/a	*
18	18.3	Verify That Acquired Software is Still Supported	In Progress	
18	18.4	Only Use Up-to-Date and Trusted Third-Party Components	In Progress	
18	18.5	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Live	
18	18.6	Ensure Software Development Personnel are Trained in Secure Coding	n/a	*
18	18.7	Apply Static and Dynamic Code Analysis Tools	n/a	*
18	18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Pending	
18	18.9	Separate Production and Non-Production Systems	n/a	*
18	18.1	Deploy Web Application Firewalls	Pending	
18	18.11	Use Standard Hardening Configuration Templates for Databases	Pending	
19	19.1	Document Incident Response Procedures	Pending	
19	19.2	Assign Job Titles and Duties for Incident Response	Pending	
19	19.3	Designate Management Personnel to Support Incident Handling	Pending	
19	19.4	Devise Organization-wide Standards for Reporting Incidents	Pending	
19	19.5	Maintain Contact Information For Reporting Security Incidents	Pending	

19	19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents	Pending
19	19.7	Conduct Periodic Incident Scenario Sessions for Personnel	Pending
20	20.1	Establish a Penetration Testing Program	In Progress
20	20.2	Conduct Regular External and Internal Penetration tests	Pending
20	20.4	Include Tests for Presence of Unprotected System Information and Artifacts	Pending
20	20.5	Create Test Bed for Elements Not Typically Tested in Production	Pending
20	20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Pending
20	20.8	Control and Monitor Accounts Associated with Penetration Testing	Pending

Legend * control has been determined to be not applicable to the organization

Status	Count	Term	Definition
Live	60	"Live"	Control is satisfied by existing process. Includes possible recurring items.
In Progress	22	"In Progress"	Control is being researched or under active development but not yet graduated to "Live" status.
Pending	56	"Pending"	Control is under review, being researched or awaiting "Live" status due to other pending systems/processes.
N/A	4	"N/A"	Control does not apply or causes undue burdeon on organization.
total items	**142**		

GENERAL MANAGER’S REPORT

GOLETA SANITARY DISTRICT
GENERAL MANAGER'S REPORT

The following summary report describes the District's activities from March 16, 2021 through April 5, 2021. It provides updated information on significant activities under three major categories: Collection System, Treatment/Reclamation and Disposal Facilities, and General and Administration Items.

1. COLLECTION SYSTEM REPORT

LINES CLEANING

Staff is conducting routine lines cleaning in the area of N. Patterson and N. Kellogg Avenues.

CCTV INSPECTION

Staff continues routine Closed-Circuit Television (CCTV) inspections in the area of Foothill and La Cumbre Roads.

2020 CCTVI PROJECT

The project cleaning and CCTV inspection work is complete. The final progress payment is being processed and National Plant Services (NPS) has submitted their recommendations for sewer pipe repairs and replacement based on their portion of the work. Staff will review and incorporate appropriate NPS recommendations with the recommendations to be made by Hazen and Sawyer for the Asset Management Program update.

2020 AERIAL IMAGERY UPDATE

The District's Geographic Information System (GIS) consultant continues with the update of the District's GIS maps.

GREASE AND OIL INSPECTIONS

Staff continues with the annual Grease and Oil inspections.

COMPETENCY-BASED TRAINING (CBT)

Staff continues to work with DKF Solutions in preparation for the upcoming Confined Space Entry training in April, 2021.

2. TREATMENT, RECLAMATION AND DISPOSAL FACILITIES REPORT

Plant flows have maintained an average of 4.1 million gallons per day (MGD). Reclamation demand has increased to 1.0 MGD. The new coagulant has been tested and is working well. This will allow for longer filter run time and fewer backwashes reducing energy consumption. Operations staff is trying new testing methods to verify effectiveness of disinfectant residuals at the facility; this will help determine proper dosage and mixing.

Centrifuge operations are continuing as planned. Dredging operations have been completed across approximately 80% of the lagoon. We plan to extend the dredging operations through the end of FY 2020-21 to maximize operational benefit, given the reduction in overall solids coming into the plant.

The Lystek refeed project has resumed. The refeed process is now feeding continuously at a lower rate, but at the same volume per week as before the shutdown. Operations staff will continue to monitor digester foaming, to date foaming has not increased significantly with the new digester feeding routine.

INDUSTRIAL WASTE SOURCE CONTROL PROGRAM

As required by the District's approved Pretreatment Program, staff has completed all first quarter Class A industrial user inspections and sampling.

3. GENERAL AND ADMINISTRATIVE ITEMS

Financial Report

The District account balances as of April 5, 2021 shown below are approximations to the nearest dollar and indicate the overall funds available to the District at this time.

Operating Checking Accounts:	$	124,454
Investment Accounts:	$	29,012,799
Total District Funds:	$	29,137,253

The following transactions are reported herein for the period 03/16/21 – 04/05/21.

Regular, Overtime, Cash-outs and Net Payroll:	$	122,079
Claims:	$	720,277
Total Expenditures:	$	842,355
Total Deposits:	$	416,283

Transfers of funds:

LAIF to Community West Bank Operational (CWB):	$	- 0 -
CWB Operational to CWB Money Market:	$	- 0 -
CWB Money Market to CWB Operational:	$	- 0 –

The District's investments comply with the District's Investment Policy adopted per Resolution No. 16-606. The District has adequate funds to meet the next six months of normal operating expenses.

Local Agency Investment Fund (LAIF)

LAIF Monthly Statement – March, 2021.
LAIF Quarterly Report – Previously submitted.
PMIA/LAIF Performance – Previously submitted.
PMIA Effective Yield – Previously submitted.

Community West Bank (CWB)

CWB Money Market Account – March, 2021.

Deferred Compensation Accounts

CalPERS 457 Deferred Compensation Plan – February, 2021.
Lincoln 457 Deferred Compensation Plan – March, 2021.

COVID-19 Response Plan Update

A verbal update will be provided at the meeting.

California State Treasurer
Fiona Ma, CPA

Local Agency Investment Fund
P.O. Box 942809
Sacramento, CA 94209-0001
(916) 653-3001

April 01, 2021

LAIF Home
PMIA Average Monthly Yields

GOLETA SANITARY DISTRICT

GENERAL MANAGER
ONE WILLIAM MOFFETT PLACE
GOLETA, CA 93117

Tran Type Definitions

Account Number: 70-42-002

March 2021 Statement

Account Summary

Total Deposit:	0.00	Beginning Balance:	2,020,014.55
Total Withdrawal:	0.00	Ending Balance:	2,020,014.55

Community West Bank

445 Pine Avenue
Goleta, CA 93117

Statement Ending 03/31/2021

GOLETA SANITARY DISTRICT **Page 1**

Customer Number: XXXXXXXX5554

RETURN SERVICE REQUESTED

GOLETA SANITARY DISTRICT
MONEY MARKET
1 WILLIAM MOFFETT PL
GOLETA CA 93117-3901

All Community West Bank branch offices are open to serve you Monday through Friday, 9:00 am to 5:00 pm.

Business Financing

When your business needs new funding or commercial real estate financing, please contact your Community West Banker. We offer flexible financing at competitive rates.

Loan Payment Mailing Address Change

The mailing address for loan payments has changed. If you are not mailing a payment with a coupon, make sure you write the loan number on the check. Please mail loan payments to:
CWB Loan Servicing, P.O. Box 80233, City of Industry, CA 91716-8233

Summary of Accounts

Account Type	Account Number	Ending Balance
PUBLIC AGENCY-MMDA	XXXXXXXX5554	$26,992,783.95

PUBLIC AGENCY-MMDA - XXXXXXXX5554

Account Summary

Date	Description	Amount		
02/27/2021	**Beginning Balance**	**$27,551,639.56**	Average Ledger Balance	$27,063,760.77
	1 Credit(s) This Period	$16,144.39		
	1 Debit(s) This Period	$575,000.00		
03/31/2021	**Ending Balance**	**$26,992,783.95**		

Account Activity

Post Date	Description	Debits	Credits	Balance
02/27/2021	**Beginning Balance**			**$27,551,639.56**
03/04/2021	XFER DEBIT 3/04/21 10:09 110093320 CHECKING 6505538	$575,000.00		$26,976,639.56
03/31/2021	INTEREST AT .6598 %		$16,144.39	$26,992,783.95
03/31/2021	**Ending Balance**			**$26,992,783.95**

CalPERS 457 Plan

February 28, 2021

This document includes important information to help you compare the investment options under your retirement plan. If you want additional information about your investment options, you can go to **https://calpers.voya.com**.

A free paper copy of the information available on the website can be obtained by contacting:

Voya Financial
Attn: CalPERS 457 Plan
P.O. Box 55772
Boston, MA 02205-5772
(800) 260-0659

Document Summary

This document has two parts. Part I consists of performance information for the plan investment options. This part shows you how well the investments have performed in the past. Part I also shows the total annual operating expenses of each investment option. Part II provides additional information concerning Plan administrative fees that may be charged to your individual account.

CalPERS 457 PLAN

Part I. Performance Information For Periods Ended February 28, 2021

https://calpers.voya.com

Table 1 focuses on the performance of investment options that do not have a fixed or stated rate of return. Table 1 shows how these options have performed over time and allows you to compare them with an appropriate benchmark for the same time periods[1]. Past performance does not guarantee how the investment option will perform in the future. Your investment in these options could lose money. Information about an investment option's principal risks is available on the website listed above.

Table 1 also shows the Total Annual Operating Expenses of each investment option. Total Annual Operating Expenses are expenses that reduce the rate of return of the investment option[2]. The cumulative effect of fees and expenses can substantially reduce the growth of your retirement savings. Visit the U.S. Department of Labor's website for an example showing the long-term fees and expenses at http://www.dol.gov/ebsa. Fees and expenses are only one of many factors to consider when you decide to invest in an option. You may also want to think about whether an investment in a particular option, along with your other investments, will help you achieve your financial goals.

Table 1 - Variable Net Return Investments

	Performance		Annualized Performance				Total Annual	
Name of Fund /	**3**	**1**	**5**	**10**	**Since**	**Inception**	**Operating Expenses[3]**	
Name of Benchmark	**Month**	**Year**	**Years**	**Years**	**Inception**	**Date**	**As a %**	**Per $1000**
Equity Funds								
State Street Russell All Cap Index Fund - Class I	7.18	34.82	16.95	-	13.41	10/07/13	0.31%	$3.10
Russell 3000 Index	7.29	35.33	17.41	-	13.81			
State Street Global All Cap Equity ex-US Index Fund - Class I	8.01	26.43	11.12	-	5.47	10/07/13	0.32%	$3.20
MSCI ACWI ex-USA IMI Index (net)	8.12	27.24	11.29	-	5.70			
Fixed Income								
State Street US ShortTerm Gov't/Credit Bond Index Fund - Class I	0.00	1.55	1.62	-	1.22	10/07/13	0.32%	$3.20
Bloomberg Barclays US 1-3 yr Gov't/Credit Bond Index	0.09	1.94	2.09	-	1.71			
State Street US Bond Fund Index - Class I	-2.13	1.17	3.21	-	3.24	10/07/13	0.31%	$3.10
Bloomberg Barclays US Aggregate Bond Index	-2.02	1.38	3.55	-	3.55			
Real Assets								
State Street Real Asset Fund - Class A	9.06	17.82	6.93	-	2.26	10/08/13	0.44%	$4.40
State Street Custom Benchmark[4]	9.20	17.76	7.30	-	2.62			
Cash (Cash Equivalents)								
State Street STIF	-0.04	0.04	1.00	-	0.72	09/02/14	0.33%	$3.30
BofA ML 3-month US T-Bill	0.03	0.40	1.20	-	0.93			
Target Retirement Date Funds[5]								
CalPERS Target Income Fund	1.48	11.77	5.90	4.55	5.82	12/01/08	0.32%	$3.20
SIP Income Policy Benchmark[6]	1.59	11.71	6.15	4.89	6.35			
CalPERS Target Retirement 2015	1.68	12.67	5.93	4.79	6.92	12/01/08	0.32%	$3.20
SIP 2015 Policy Benchmark[6]	1.79	12.61	6.17	5.24	7.47			
CalPERS Target Retirement 2020	2.82	16.54	6.86	5.29	7.62	12/01/08	0.32%	$3.20
SIP 2020 Policy Benchmark[6]	2.93	16.43	7.10	5.73	8.14			
CalPERS Target Retirement 2025	3.95	20.14	8.40	5.99	8.49	12/01/08	0.32%	$3.20
SIP 2025 Policy Benchmark[6]	4.06	20.04	8.64	6.47	8.99			
CalPERS Target Retirement 2030	5.08	23.29	9.48	6.60	9.32	12/01/08	0.32%	$3.20
SIP 2030 Policy Benchmark[6]	5.19	23.62	9.80	7.11	9.83			
CalPERS Target Retirement 2035	6.18	26.84	10.72	7.18	10.03	12/01/08	0.32%	$3.20
SIP 2035 Policy Benchmark[6]	6.29	27.17	11.03	7.73	10.60			
CalPERS Target Retirement 2040	7.11	29.37	11.95	7.72	10.55	12/01/08	0.32%	$3.20
SIP 2040 Policy Benchmark[6]	7.23	29.82	12.28	8.28	11.09			
CalPERS Target Retirement 2045	7.11	29.37	12.69	8.01	10.74	12/01/08	0.32%	$3.20
SIP 2045 Policy Benchmark[6]	7.23	29.82	13.01	8.57	11.33			
CalPERS Target Retirement 2050	7.11	29.37	12.69	8.01	10.83	12/01/08	0.32%	$3.20
SIP 2050 Policy Benchmark[6]	7.23	29.82	13.01	8.57	11.33			
CalPERS Target Retirement 2055	7.11	29.37	12.68	-	8.24	10/07/13	0.32%	$3.20
SIP 2055 Policy Benchmark[6]	7.23	29.82	13.01	-	8.61			
CalPERS Target Retirement 2060	7.11	29.35	-	-	15.47	11/01/18	0.32%	$3.20
SIP 2060 Policy Benchmark[6]	7.23	29.82	-	-	15.80			
Broad-Based Benchmarks[7]								
Russell 3000 Index	7.29	35.33	17.41	13.44	-	-	-	-
MSCI ACWI ex-USA IMI Index (net)	8.12	27.24	11.29	4.96	-	-	-	-
Bloomberg Barclays US Aggregate Bond Index	-2.02	1.38	3.55	3.58	-	-	-	-

Part II. Explanation of CalPERS 457 Plan Expenses
February 28, 2021

https://calpers.voya.com

Table 2 provides information concerning Plan administrative fees and expenses that may be charged to your individual account if you take advantage of certain features of the Plan. In addition to the fees and expenses described in Table 2 below, some of the Plan's administrative expenses are paid from the Total Annual Operating Expenses of the Plan's investment options.

Table 2 - Fees and Expenses

Individual Expenses[8]

Service	Fee Amount	Frequency	Who do you pay this fee to?	Description
Loan Origination Fee	$50	Per loan application	Voya	The charge covers the processing of your loan and applies each time you request a loan from your retirement account. This fee is deducted from your Plan account.
Maintenance Fee (For loans taken on or after April 1, 2020)	$35 ($8.75 assessed quarterly)	Annual	Voya	The charge covers the maintenance costs of your loan and applies on a quarterly basis. This fee is deducted from your Plan account.
Self-Managed Account (SMA) Maintenance Fee	$50	Annual fee deducted monthly on a pro-rata basis	Voya	Schwab Personal Choice Retirement Account is available to you if your Employer has elected it as an option. This fee is deducted pro rata on a monthly basis from your core fund investments[9] in your CalPERS 457 account. For more information about SMAs, including a complete list of fees charged by Schwab for different types of investment transactions, please contact Schwab at (888) 393-PCRA (7272). Fees may also be incurred as a result of actual brokerage account trades. Before purchasing or selling any investment through the SMA, you should contact Schwab at (888) 393-PCRA (7272) to inquire about any fees, including any undisclosed fees, associated with the purchase or sale of such investment.
Self-Managed Account (SMA) Plan Administrative Fee	0.29% ($2.90 per $1,000)	Annual fee deducted monthly on a pro-rata basis	Voya	The SMA Plan Administrative fee pays for recordkeeping costs for assets in your SMA account. This fee is deducted pro rata on a monthly basis from your core fund investments in your CalPERS 457 account. The SMA Plan Administrative Fee is subject to change based on total Plan assets.

Footnotes for Table 1 and Table 2:

[1] Fund returns shown are net of investment management and administrative expenses and fees unless otherwise noted. Benchmark performance returns do not reflect any management fees, transaction costs or expenses. Benchmarks are unmanaged. You cannot invest directly in a benchmark.

[2] Historical annual operating expenses are not available. Reported annual operating expenses are estimated based on SSGA investment management, Voya recordkeeping, and SSGA capped operating expenses.

[3] Total annual operating expenses are comprised of investment management and administrative expenses and fees incurred by the funds.

[4] State Street Real Asset Fund has a custom benchmark comprised of 25% Bloomberg Roll Select Commodity Index, 25% S&P® Global LargeMidCap Commodity and Resources Index, 15% Dow Jones U.S. Select REIT Index, 25% Bloomberg Barclays U.S. TIPS Index, and 10% S&P Global Infrastructure Index.

[5] If the ending market value (EMV) falls to zero in any one month, the inception date resets to the next month with an EMV. Performance is then calculated from the new inception date.

[6] The benchmark for each Target Retirement Date Fund is a composite of asset class benchmarks that are weighted according to each Fund's policy target weights. The asset class benchmarks are Russell 3000 Index, MSCI ACWI ex-USA IMI Index (net), Bloomberg Barclays US Aggregate Bond Index, the SSGA customized benchmark for Real Assets (see footnote 4), and BofA ML 3-month US T-Bill.

[7] Broad-based benchmarks grouped here provide comparative performance standards for domestic equity, international equity and fixed income.

[8] The CalPERS Board of Administration periodically reviews the plan administrative fees and adjusts fees to reflect expenses incurred by the Plan. Participant fees are charged to reimburse CalPERS for actual administrative fees of the Plan.

[9] Core fund investments are listed in Table 1 above the Target Retirement Date funds. Core funds include: State Street Russell All Cap Index Fund (Class I), State Street Global All Cap Equity ex-US Index Fund (Class I), State Street US Short Term Government/Credit Bond Index Fund (Class I), State Street US Bond Fund Index (Class I), State Street Real Asset Fund (Class A), and State Street Short Term Investment Fund ("STIF").

Lincoln Financial Group℠

Multi-Fund®

Performance Update

Quoted performance data represents past performance. Past performance does not guarantee nor predict future performance. Current performance may be lower or higher than the performance data quoted. Please keep in mind that double-digit returns are highly unusual and cannot be sustained.

Variable products are sold by prospectus. Consider the investment objectives, risks, charges, and expenses of the variable product and its underlying investment options carefully before investing. The prospectus contains this and other information about the variable product and its underlying investment options. Please review the prospectus available online for additional information. Read it carefully before investing.

Investment return and principal value of an investment will fluctuate so that an investor's unit values, when redeemed, may be worth more or less than their original cost.

Monthly hypothetical performance adjusted for contract fees *

						Average Annual Total Return (%) as of 3/31/2021						
Investment Options		Inception Date	Change from Previous Day	YTD as of 03/31/2021	YTD as of 03/31/2021	1 Mo	3 Mo	1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
Risk Managed												
Fidelity® VIP Freedom 2055 Portfolio℠ - Service Class[7, 9]	RM	04/11/2019	0.07	4.59	4.59	2.31	4.59	52.51	N/A	N/A	N/A	17.24
Fidelity® VIP Freedom 2060 Portfolio℠ - Service Class[7, 9]	RM	04/11/2019	0.07	4.56	4.56	2.30	4.56	52.51	N/A	N/A	N/A	17.30
Maximum Capital Appreciation												
AB VPS Global Thematic Growth Portfolio - Class B[1, 2]	MCA	01/11/1996	0.99	2.80	2.80	1.05	2.80	69.13	17.63	17.15	8.58	6.10
Delaware VIP® Smid Cap Core Series - Standard Class[5, 8]	MCA	07/12/1991	0.32	11.73	11.73	1.90	11.73	76.23	11.20	11.36	10.49	9.46
DWS Alternative Asset Allocation VIP Portfolio - Class A[1, 2, 3, 9, 10]	MCA	02/02/2009	0.42	2.59	2.59	0.41	2.59	25.39	4.91	3.60	1.69	4.38
LVIP Baron Growth Opportunities Fund - Service Class[8]	MCA	10/01/1998	1.06	1.32	1.32	-1.62	1.32	76.00	19.35	17.86	12.98	11.64
LVIP SSGA Emerging Markets 100 Fund - Standard Class[1, 19]	MCA	06/18/2008	-0.51	8.09	8.09	4.02	8.09	54.65	0.01	5.91	-0.32	2.76
LVIP SSGA Small-Cap Index Fund - Standard Class[8, 18]	MCA	04/18/1986	1.11	12.37	12.37	0.95	12.37	92.16	13.10	14.69	10.10	7.47
LVIP T. Rowe Price Structured Mid-Cap Growth Fund - Standard Class[8]	MCA	02/03/1994	1.93	-0.44	-0.44	-2.55	-0.44	66.07	18.30	17.50	12.95	7.43
Long Term Growth												
American Funds Global Growth Fund - Class 2[1]	LTG	04/30/1997	0.69	3.33	3.33	0.60	3.33	59.77	16.23	16.98	11.61	9.67
American Funds Growth Fund - Class 2	LTG	02/08/1984	1.20	3.24	3.24	1.44	3.24	79.05	24.69	22.96	15.33	12.41

Performance Update

MultiFund

Monthly hypothetical performance adjusted for contract fees *

						Average Annual Total Return (%) as of 3/31/2021						
Investment Options		Inception Date	Change from Previous Day	YTD as of 03/31/2021	YTD as of 03/31/2021	1 Mo	3 Mo	1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
American Funds International Fund - Class 2[1]	LTG	05/01/1990	-0.05	-1.52	-1.52	-1.82	-1.52	47.73	5.03	9.70	5.18	6.93
Delaware VIP Small Cap Value[5, 8]	LTG	12/27/1993	-0.22	19.69	19.69	5.61	19.69	84.75	7.59	10.84	8.50	9.41
Fidelity® VIP Contrafund® Portfolio - Service Class	LTG	01/03/1995	0.99	1.94	1.94	1.94	1.94	51.37	16.58	15.72	11.84	10.66
Fidelity® VIP Growth Portfolio - Service Class	LTG	10/09/1986	1.18	2.75	2.75	0.44	2.75	69.17	22.94	21.77	15.39	10.21
LVIP BlackRock Global Real Estate Fund - Standard Class[1, 2, 7]	LTG	04/30/2007	-0.68	6.70	6.70	3.02	6.70	37.48	6.78	4.12	4.63	1.20
LVIP Delaware Mid Cap Value Fund - Standard Class[5, 8]	LTG	12/28/1981	-0.30	14.52	14.52	6.00	14.52	76.37	8.41	11.22	9.11	10.44
LVIP Delaware Social Awareness Fund - Standard Class[5]	LTG	05/02/1988	0.33	6.74	6.74	3.76	6.74	61.07	16.25	14.78	12.18	10.12
LVIP Dimensional U.S. Core Equity 1 Fund - Standard Class	LTG	12/28/1981	0.20	9.32	9.32	4.50	9.32	66.27	14.52	14.79	12.10	9.92
LVIP Mondrian International Value Fund - Standard Class[1]	LTG	05/01/1991	-1.30	6.28	6.28	3.80	6.28	37.49	1.39	4.78	3.37	5.32
LVIP SSGA International Index Fund - Standard Class[1, 18, 20]	LTG	04/30/2008	-0.54	2.95	2.95	2.39	2.95	43.59	4.55	7.53	4.13	1.68
LVIP SSGA S&P 500 Index Fund - Standard Class[18, 21]	LTG	05/01/2000	0.37	5.87	5.87	4.27	5.87	54.50	15.32	14.86	12.50	5.64
LVIP Vanguard Domestic Equity ETF Fund - Service Class[9, 22]	LTG	04/29/2011	0.48	5.98	5.98	3.90	5.98	57.74	15.32	14.53	N/A	11.36
LVIP Vanguard International Equity ETF Fund - Service Class[1, 9, 22]	LTG	04/29/2011	-0.12	3.86	3.86	1.72	3.86	49.62	5.06	8.67	N/A	3.70
MFS® VIT Utilities Series - Initial Class[2]	LTG	01/03/1995	0.76	1.08	1.08	8.55	1.08	29.15	10.38	8.88	7.52	10.09
Growth and Income												
American Funds Growth-Income Fund - Class 2	GI	02/08/1984	0.15	6.03	6.03	4.25	6.03	48.94	12.59	14.15	11.84	10.21
BlackRock Global Allocation V.I. Fund - Class I[1, 3]	GI	02/28/1992	0.15	1.44	1.44	0.72	1.44	39.15	9.44	8.79	5.61	6.54
Delaware VIP REIT[2, 5, 7]	GI	05/04/1998	-0.91	7.84	7.84	4.38	7.84	29.59	6.38	2.18	6.32	7.30
Delaware VIP Value[5]	GI	07/28/1988	-0.82	8.73	8.73	7.00	8.73	47.18	7.84	9.35	10.33	7.95
Fidelity® VIP Freedom 2020 Portfolio℠ - Service Class[9, 11]	GI	04/26/2005	0.07	1.37	1.37	0.74	1.37	29.48	8.94	9.04	6.75	6.07

Performance Update

MultiFund

Monthly hypothetical performance adjusted for contract fees *

						Average Annual Total Return (%) as of 3/31/2021						
Investment Options		Inception Date	Change from Previous Day	YTD as of 03/31/2021	YTD as of 03/31/2021	1 Mo	3 Mo	1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
Fidelity® VIP Freedom 2025 Portfolio℠ - Service Class[9, 11]	GI	04/26/2005	0.06	1.83	1.83	0.99	1.83	33.31	9.68	9.80	7.48	6.62
Fidelity® VIP Freedom 2030 Portfolio℠ - Service Class[9, 11]	GI	04/26/2005	0.06	2.40	2.40	1.30	2.40	38.36	10.49	11.05	8.14	6.90
Fidelity® VIP Freedom 2035 Portfolio℠ - Service Class[9, 11]	GI	04/08/2009	0.11	3.71	3.71	1.90	3.71	47.10	11.69	12.33	8.92	12.13
Fidelity® VIP Freedom 2040 Portfolio℠ - Service Class[9, 11]	GI	04/08/2009	0.11	4.62	4.62	2.31	4.62	52.54	12.43	12.80	9.18	12.44
Fidelity® VIP Freedom 2045 Portfolio℠ - Service Class[9, 11]	GI	04/08/2009	0.11	4.63	4.63	2.33	4.63	52.49	12.41	12.79	9.23	12.53
Fidelity® VIP Freedom 2050 Portfolio℠ - Service Class[9, 11]	GI	04/08/2009	0.12	4.63	4.63	2.30	4.63	52.52	12.41	12.79	9.22	12.64
LVIP BlackRock Advantage Allocation Fund - Standard Class[3, 5, 12]	GI	07/28/1988	-0.07	0.48	0.48	0.55	0.48	25.80	7.13	7.38	5.62	5.82
LVIP Delaware Wealth Builder Fund - Standard Class[3, 5, 12]	GI	08/03/1987	-0.20	2.62	2.62	2.81	2.62	24.19	5.83	6.22	5.31	6.02
LVIP JPMorgan Retirement Income Fund - Standard Class[3, 5, 12]	GI	04/27/1983	0.03	0.09	0.09	0.21	0.09	20.38	5.44	5.51	4.57	6.60
Income												
Delaware VIP Diversified Income[4, 5]	I	05/16/2003	0.00	-3.18	-3.18	-1.41	-3.18	7.70	4.53	3.32	2.90	4.36
Delaware VIP High Yield[4, 5, 6]	I	07/28/1988	0.39	0.54	0.54	0.30	0.54	21.61	5.88	6.30	4.54	5.68
LVIP BlackRock Inflation Protected Bond Fund - Standard Class[4]	I	04/30/2010	0.04	-0.05	-0.05	0.45	-0.05	5.75	2.81	2.04	1.45	1.64
LVIP Delaware Bond Fund - Standard Class[4, 5]	I	12/28/1981	0.01	-3.25	-3.25	-1.33	-3.25	4.44	4.23	2.82	2.84	6.59
LVIP Delaware Diversified Floating Rate Fund[5, 15]	I	04/30/2010	0.02	-0.17	-0.17	-0.33	-0.17	4.39	0.79	0.96	0.19	0.31
LVIP Global Income Fund - Standard Class[1, 4, 12, 14]	I	05/04/2009	0.02	-3.75	-3.75	-1.22	-3.75	1.36	2.35	1.90	1.08	2.52
LVIP SSGA Bond Index Fund - Standard Class[4, 18]	I	04/30/2008	-0.02	-3.68	-3.68	-1.39	-3.68	-0.73	3.34	1.77	2.08	2.46
PIMCO VIT Total Return Portfolio - Administrative Class[4]	I	12/31/1997	0.00	-3.37	-3.37	-1.36	-3.37	2.33	3.68	2.66	2.48	4.22
Risk Managed - Asset Allocation												

Performance Update

Monthly hypothetical performance adjusted for contract fees *

						Average Annual Total Return (%) as of 3/31/2021						
Investment Options		Inception Date	Change from Previous Day	YTD as of 03/31/2021	YTD as of 03/31/2021	1 Mo	3 Mo	1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
LVIP Global Conservative Allocation Managed Risk Fund - Standard Class[1, 3, 9, 12, 16]	RMAA	05/03/2005	0.06	0.91	0.91	0.59	0.91	17.38	5.21	5.44	4.60	4.89
LVIP Global Growth Allocation Managed Risk Fund - Standard Class[1, 3, 9, 12, 16]	RMAA	05/03/2005	0.03	3.21	3.21	1.58	3.21	22.72	5.14	6.41	4.44	4.59
LVIP Global Moderate Allocation Managed Risk Fund - Standard Class[1, 3, 9, 12, 16]	RMAA	05/03/2005	0.04	2.20	2.20	1.06	2.20	19.84	4.92	6.01	4.37	4.77
LVIP SSGA Global Tactical Allocation Managed Volatility Fund - Standard Class[1, 3, 9, 12, 13, 14]	RMAA	05/03/2005	-0.13	4.64	4.64	1.80	4.64	29.68	5.34	6.31	4.15	3.87
Preservation of Capital												
LVIP Government Money Market Fund - Standard Class[12, 17]	PC	01/07/1982	0.00	-0.24	-0.24	-0.09	-0.24	-0.97	0.07	-0.23	-0.60	2.74
Risk Managed - US Large Cap												
LVIP BlackRock Dividend Value Managed Volatility Fund - Standard Class[12, 13]	RMUSL	02/03/1994	-0.47	12.88	12.88	7.01	12.88	37.68	7.93	8.98	6.20	6.73
LVIP Blended Large Cap Growth Managed Volatility Fund - Standard Class[12, 13, 14]	RMUSL	02/03/1994	0.61	3.36	3.36	2.39	3.36	38.58	12.75	12.78	8.99	7.02
Asset Allocation												
LVIP T. Rowe Price 2010 Fund (Standard Class)[9, 11, 12]	AsA	05/01/2007	0.07	1.44	1.44	0.80	1.44	25.89	7.37	6.43	4.58	4.10
LVIP T. Rowe Price 2020 Fund (Standard Class)[9, 11, 12]	AsA	05/01/2007	0.09	2.16	2.16	1.11	2.16	32.36	8.41	7.61	5.06	4.19
LVIP T. Rowe Price 2030 Fund (Standard Class)[9, 11, 12]	AsA	05/01/2007	0.11	3.49	3.49	1.69	3.49	42.14	9.91	8.57	5.50	4.41
LVIP T. Rowe Price 2040 Fund (Standard Class)[9, 11, 12]	AsA	05/01/2007	0.14	4.95	4.95	2.31	4.95	50.29	11.15	9.56	5.85	4.32
LVIP T. Rowe Price 2050 Fund (Standard Class)[9, 11, 12]	AsA	04/29/2011	0.14	5.41	5.41	2.50	5.41	53.14	11.50	10.42	N/A	5.82
LVIP T. Rowe Price 2060 Fund - Standard Class[9, 11, 12]	AsA	04/30/2020	0.16	5.87	5.87	2.65	5.87	N/A	N/A	N/A	N/A	40.99
Risk Managed - US Mid Cap												
LVIP Blended Mid Cap Managed Volatility Fund - Standard Class[8, 12, 13, 14]	RMUSM	05/01/2001	1.67	-2.03	-2.03	-2.16	-2.03	36.76	14.09	14.35	6.14	4.77

Printed On 04/01/2021 at 02:22 EST

Lincoln Financial Group is the marketing name for Lincoln National Corporation and its affiliates.

Performance Update

MultiFund

Monthly hypothetical performance adjusted for contract fees *

						Average Annual Total Return (%) as of 3/31/2021						
Investment Options		Inception Date	Change from Previous Day	YTD as of 03/31/2021	YTD as of 03/31/2021	1 Mo	3 Mo	1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
LVIP JPMorgan Select Mid Cap Value Managed Volatility Fund - Standard Class[8, 12, 13, 14]	RMUSM	05/01/2001	-0.31	13.86	13.86	6.46	13.86	44.06	5.67	6.88	5.56	6.13
Risk Managed - Global/International												
LVIP Franklin Templeton Global Equity Managed Volatility Fund - Standard Class[1, 12, 13]	RMGI	08/01/1985	-0.13	5.02	5.02	3.23	5.02	35.06	6.14	8.18	5.07	7.10
LVIP SSGA International Managed Volatility Fund - Standard Class[1, 9, 12, 13]	RMGI	12/31/2013	-0.54	2.96	2.96	2.34	2.96	33.13	1.45	4.63	N/A	0.95

* These returns are measured from the inception date of the fund and predate its availability as an investment option in the variable annuity (separate account). This hypothetical representation depicts how the investment option would have performed had the fund been available in the variable annuity during the time period. It includes deductions for the M&E charge and the contract administrative fee. If selected above, the cost for the i4LIFE® Advantage feature or a death benefit will be reflected. The cost for other riders with quarterly charges is not reflected. No surrender charge and no annual contract charge is reflected.

Performance Update

[1] **International**
Investing internationally involves risks not associated with investing solely in the United States, such as currency fluctuation, political or regulatory risk, currency exchange rate changes, differences in accounting and the limited availability of information.

[2] **Sector Funds**
Funds that target exposure to one region or industry may carry greater risk and higher volatility than more broadly diversified funds.

[3] **Asset Allocation Portfolios**
Asset allocation does not ensure a profit, nor protect against loss in a declining market.

[4] **Bonds**
The return of principal in bond funds is not guaranteed. Bond funds have the same interest rate, inflation, credit, duration, prepayment and market risks that are associated with the underlying bonds owned by the fund or account.

[5] **Macquarie Investment Management**
Investments in Delaware VIP Series, Delaware Funds, LVIP Delaware Funds or Lincoln Life accounts managed by Macquarie Investment Management Advisers, a series of Macquarie Investments Management Business Trust, are not and will not be deposits with or liabilities of Macquarie Bank Limited ABN 46 008 583 542 and its holding companies, including their subsidiaries or related companies, and are subject to investment risk, including possible delays in repayment and loss of income and capital invested. No Macquarie Group company guarantees or will guarantee the performance of the fund, the repayment of capital from the fund, or any particular rate of return.

[6] **High-yield or mortgage-backed funds**
High-yield funds may invest in high-yield or lower rated fixed income securities (junk bonds) or mortgage-backed securities with exposure to subprime mortgages, which may experience higher volatility and increased risk of nonpayment or default.

[7] **REIT**
A real estate investment trust (REIT) involves risks such as refinancing, economic conditions in the real estate industry, declines in property values, dependency on real estate management, changes in property taxes, changes in interest rates and other risks associated with a portfolio that concentrates its investments in one sector or geographic region.

[8] **Small & Mid Cap**
Funds that invest in small and/or midsize company stocks may be more volatile and involve greater risk, particularly in the short term, than those investing in larger, more established companies.

[9] **Fund of funds**
Each fund is operated as a fund of funds that invests primarily in one or more other funds, rather than in individual securities. A fund of this nature may be more expensive than other investment options because it has additional levels of expenses. From time to time, the Fund's advisor may modify the asset allocation to the underlying funds and may add new funds. A Fund's actual allocation may vary from the target strategic allocation at any point in time. Additionally, the Fund's advisor may directly manage assets of the underlying funds for a variety of purposes.

[10] **Alternative Funds**
Certain funds (sometimes called "alternative funds") expect to invest in (or may invest in some) positions that emphasize alternative investment strategies and/or nontraditional asset classes and, as a result, are subject to the risk factors of those asset classes and/or investment strategies. Some of those risks may include general economic risk, geopolitical risk, commodity-price volatility, counterparty and settlement risk, currency risk, derivatives risk, emerging markets risk, foreign securities risk, high-yield bond exposure, index investing risk, exchange-traded notes risk, industry concentration risk, leveraging risk, real estate investment risk, master limited partnership risk, master limited partnership tax risk, energy infrastructure companies risk, sector risk, short sale risk, direct investment risk, hard assets sector risk, active trading and "overlay" risks, event-driven investing risk, global macro strategies risk, temporary defensive positions and large cash positions. If you are considering investing in alternative investment funds, you should ensure that you understand the complex investment strategies sometimes employed and be prepared to tolerate the risks of such asset classes. For a complete list of risks, as well as a discussion of risk and investment strategies, please refer to the fund's prospectus. The fund may invest in derivatives, including futures, options, forwards and swaps. Investments in derivatives may cause the fund's losses to be greater than if it invested only in conventional securities and can cause the fund to be more volatile. Derivatives involve risks different from, or possibly greater than, the risks associated with other investments. The fund's use of derivatives may cause the fund's investment returns to be impacted by the performance of securities the fund does not own and may result in the fund's total investment exposure exceeding the value of its portfolio.

[11] **Target-date funds**
The target date is the approximate date when investors plan to retire or start withdrawing their money. Some target-date funds make no changes in asset allocation after the target date is reached; other target-date funds continue to make asset allocation changes following the target date. (See the prospectus for the funds allocation strategy.) The principal value is not guaranteed at any time, including at the target date. An asset allocation strategy does not guarantee performance or protect against investment losses. A "fund of funds" may be more expensive than other types of investment options because it has additional levels of expenses.

[12] **Manager of managers funds**
Subject to approval of the fund's board, Lincoln Investment Advisors Corporation (LIAC) has the right to engage or terminate a subadvisor at any time, without a shareholder vote, based on an exemptive order from the Securities and Exchange Commission. LIAC is responsible for overseeing all subadvisors for funds relying on this exemptive order.

[13] **Managed Volatility Strategy**
The fund's managed volatility strategy is not a guarantee, and the fund's shareholders may experience losses. The fund employs hedging strategies designed to reduce overall portfolio volatility. The use of these hedging strategies may limit the upside participation of the fund in rising equity markets relative to unhedged funds, and the effectiveness of such strategies may be impacted during periods of rapid or extreme market events.

[14] **Multimanager**
For those funds that employ a multimanager structure, the fund's advisor is responsible for overseeing the subadvisors. While the investment styles employed by the fund's subadvisors are intended to be complementary, they may not, in fact, be complementary. A multimanager approach may result in more exposure to certain types of securities risks and in higher portfolio turnover.

[15] **Floating rate funds**
Floating rate funds should not be considered alternatives to CDs or money market funds and should not be considered as cash alternatives.

[16] **Risk Management Strategy**
The fund's risk management strategy is not a guarantee, and the funds shareholders may experience losses. The fund employs hedging strategies designed to provide downside protection during sharp downward movements in equity markets. The use of these hedging strategies may limit the upside participation of the fund in rising equity markets relative to other unhedged funds, and the effectiveness of such strategies may be impacted during periods of rapid or extreme market events.

[17] **Money Market Funds**
You can lose money by investing in the fund. Although the fund seeks to preserve the value of your investment at $1.00 per share (or, for the LVIP Government Money Market Fund, at $10.00 per share), it cannot guarantee it will do so. An investment in the fund is not insured or guaranteed by the Federal Deposit Insurance Corporation or any other government agency. The fund's sponsor has no legal obligation to provide financial support to the fund, and you should not expect that the sponsor will provide financial support to the fund at any time.

[18] **Index**
An index is unmanaged, and one cannot invest directly in an index. Indices do not reflect the deduction of any fees.

[19] **Emerging Markets**
Investing in emerging markets can be riskier than investing in well-established foreign markets. International investing involves special risks not found in domestic investing, including increased political, social and economic instability, all of which are magnified in emerging markets.

[20] **MSCI**
The fund described herein is indexed to an MSCI® index. It is not sponsored, endorsed, or promoted by MSCI®, and MSCI®; bears no liability with respect to any such fund or to an index on which a fund is based. The prospectus and statement of additional information contain a more detailed description of the limited relationship MSCI®; has with Lincoln Investment Advisors Corporation and any related funds.

[21] **S&P**
The Index to which this fund is managed is a product of S&P Dow Jones Indices LLC (SPDJI) and has been licensed for use by one or more of the portfolio's service providers (licensee). Standard & Poor's®; and S&P® are registered trademarks of Standard & Poor's Financial Services LLC (S&P); Dow Jones® is a registered trademark of Dow Jones Trademark Holdings LLC (Dow Jones); and these trademarks have been licensed for use by SPDJI and sublicensed for certain purposes by the licensee. S&P®, S&P GSCI® and the Index are trademarks of S&P and have been licensed for use by SPDJI and its affiliates and sublicensed for certain purposes by the licensee. The Index is not owned, endorsed, or approved by or associated with any additional third party. The licensee's products are not sponsored, endorsed, sold or promoted by SPDJI, Dow Jones, S&P, their respective affiliates, or their third party licensors, and none of these parties or their respective affiliates or third party licensors make any representation regarding the advisability of investing in such products, nor do they have liability for any errors, omissions, or interruptions of the Index®.

[22] **Exchange-traded funds**
Exchange-traded funds (ETFs) in this lineup are available through collective trusts or mutual funds. Investors cannot invest directly in an ETF.

Important Disclosures

Variable products are issued by The Lincoln National Life Insurance Company, Fort Wayne, IN, distributed by Lincoln Financial Distributors, Inc., and offered by broker/dealers with an effective selling agreement. The Lincoln National Life Insurance Company is not authorized nor does it solicit business in the state of New York. **Contractual obligations are backed by the claims-paying ability of The Lincoln National Life Insurance Company.**

Limitations and exclusions may apply.

Lincoln Financial Group is the marketing name for Lincoln National Corporation and its affiliates. Affiliates are separately responsible for their own financial and contractual obligations.

Asset Categories

RM	=Risk Managed
MCA	=Maximum Capital Appreciation
LTG	=Long Term Growth
GI	=Growth and Income
I	=Income
RMAA	=Risk Managed - Asset Allocation
PC	=Preservation of Capital
RMUSL	=Risk Managed - US Large Cap
AsA	=Asset Allocation
RMUSM	=Risk Managed - US Mid Cap
RMGI	=Risk Managed - Global/International

DISTRICT CORRESPONDENCE

Board Meeting of April 5, 2021

Date: **Correspondence Sent To:**

1. 03/05/2021 Justin Reese
Subject: Sewer Service Availability
Proposed Sewer Service Connection for One Single Family Residence and One ADU
A.P.N. 061-291-027 at 691 Via Trepadora, Santa Barbara CA

2. 03/24/2021 Hunter Showalter
Microdyn-Nadir US, Inc.
Subject: Notice of Violation, Industrial Wastewater Discharge Permit A-437

3. 03/30/2021 Robert Gauna
Innovative Micro Technologies, Inc.
Subject: Notice of Violation, Industrial Wastewater Discharge Permit # A-429

4. 04/01/2021 William S. Wolf
Pacific Architects, Inc.
Subject: SSA Proposed Sewer Service Connection for One Proposed Single-Family Residence
A.P.N. 067-270-016 at 978 Via Los Padres, Santa Barbara CA

Date: **Correspondence Received From:**

1. 03/26/2021 Koff & Associates
Subject: Proposal for Compensation and Benefits Survey
Sample, Letters also received from:
   - CPS HR Consulting
   - Bryce Consulting
   - HR Know Consulting
   - Reward Strategy Group
   - Boucher Law

2. 03/26/2021 Moffatt & Nichol
Subject: RFQ for Preparation of a Climate Adaptation Plan
Sample, Letters also received from:
   - AARC Consultants, LLC
   - Rincon Consultants, Inc.
   - DUDEK
   - Integral Consulting Inc.
   - Ascent Environmental
   - Keramida Global EHS & Sustainability Services
   - Environmental Science Associates

Hard Copies of the Correspondence are available at the District's Office for review