Administrative Policy Manual

Nevada Public Employees'
Deferred Compensation Program

Updated February 2024

Table of Contents

Definitions **4**

Article I: Mission and Goals **4**

1.1 – Full Time Plans Mission 4

1.2 – Primary Goals 4

1.3 – FICA-Alternative/3121 Plan Mission 5

1.4 – Goals of FICA-Alternative Plan 5

1.5 – Program Rules and Regulations 5

Article II: Legal and Procedural **5**

2.1 – Federal Law 5

2.2 – State Law 5

2.3 – Committee Documents 5

2.4 – Committee Election Procedure 6

2.5 – National Association of Government Defined Contribution Administrators (NAGDCA) 6

Article III: Coordination of Audits **6**

3.1 – Audit Objectives – Audits are performed for different purposes. Common audit objectives are: 6

3.2 – Audit Process – The audit process normally consists of the following elements: ... 7

Article IV: Records Retention **7**

Article V: Committee Operation **7**

5.1 – Meeting Schedule 7

5.2 – Meeting Agenda 8

5.3 – Committee Action 8

5.4 – Meeting Record 8

5.5 – Budget Review and Approval 8

Article VI: Plan Administration **8**

6.1 – Activity reports 8

6.2 – Analysis of Investment Performance 9

6.3 – Quarterly Newsletter 9

6.4 – Fund Settlement Policy 9
6.5 – Administrative Account Management and Distribution of Unused Plan Revenue; if any 9
6.6 – Review of Claims and Appeals; Process and Policy 9
Article VII: Roles, Responsibilities and Duties 10
7.1 – Committee 10
7.2 – NDC Administrative Staff 10
7.3 – Executive Officer's Review Process 11
7.4 – Legal Counsel 11
7.5 – Political Sub-Divisions 11
7.6 – Professional Advisors 12
7.7 – Recordkeeper(s) 13
Article VIII: Code of Ethics 13
Article IX: Educational Travel and Conferences 15
Article X: Travel Policy 15
Addendum A: Fiduciary Compliance Checklist 19
Addendum B: Fee Policy Statement 23
Addendum C: Cybersecurity Policy Statement 26

Definitions

The same definitions apply in this Administrative Manual as are designated in the Plan Document for the State of Nevada Public Employees Deferred Compensation Program and in Nevada Revised Statutes (NRS) 287.250 et seq.

Article I: Mission and Goals

1.1 – Full Time Plans Mission

The Nevada Public Employees Deferred Compensation Program (NDC or Program) consists of a voluntary tax-deferred supplemental savings plan created pursuant to section 457(b) of the Internal Revenue Code, that provides participants and their beneficiaries with a supplement to their retirement savings. In 2023, the Program was expanded to include a 401(a) Defined Contribution Plan for eligible full-time employees. Collectively, the Program covers these two-full-time Plans as well as a FICA Alternative/3121 Plan made available exclusively to part-time employees and also noted in this manual.

NDC operates solely in the interest of plan participants and beneficiaries. The Committee, appointed by the Governor pursuant to NRS 287.325, oversees the Program investment management and Plan design governance and strives to provide quality investment options at minimal costs while maintaining high standards of customer service. The Committee and State Department of Administration appointed Executive Officer, Administrative Staff, or designee monitor the NDC contracted Recordkeeper, communicate the importance of supplemental savings through seminars, group meetings, workshops, newsletters, maintaining the Division and other informational efforts, and administer the Program in accordance with state and federal guidelines. All Program expenses are paid by the Plan participants by revenue generated from the Plans adopted cost structure.

1.2 – Primary Goals

a) Exercise functions solely in the interest of the participants and beneficiaries, and be responsive and flexible to strive meet participants' needs, within the overall best interest of the participant base as a whole;
b) Promote the collective best interests of the participants in the Program (Section 1(b) of NRS 287.330);
c) Provide a selection of core investment options in accordance with the Program's Statement of Investment Policy and ensure that the options represent a reasonable choice as to investment risk, return, style, cost and asset class; and
d) Ensure that the NDC Program Administrative staff and contracted Recordkeeper provides quality service and education to the participants and those approved participating entities supported.

1.3 – FICA-Alternative/3121 Plan Mission

Part-time, seasonal, and temporary employees of the State of Nevada or the Nevada System of Higher Education that do not qualify to participate in the State of Nevada Public Employees' Retirement System Pension Plan are required to participate in the Nevada FICA Alternative Deferred Compensation Plan, if hired on or after January 1, 2004 (State Government) or July 1, 2005 (Higher Education).

FICA is the Federal Insurance Contributions Act, and Section 3121 refers to the section under Title 26, Chapter 21 of the Internal Revenue Code. This is an alternative to Social Security coverage as permitted by the federal Omnibus Budget Reconciliation Act of 1990 (OBRA). By participating in the Plan, Participants are not subject to tax on compensation under the Old Age, Survivors and Disability Income portion of FICA. Participants are subject to the Medicare portion of FICA.

1.4 – Goals of FICA-Alternative Plan

The goal of this plan is to assist participants with maintaining an account for the purpose of capital preservation during their employment with the State of Nevada, the Nevada System of Higher Education and/or approved participating political subdivision.

1.5 – Program Rules and Regulations

The Program's Rules and Regulations are adopted by the State of Nevada Deferred Compensation Committee, and are designated in the Program's Plan Documents, the FICA Alternative Plan Document, and in the Nevada Revised Statutes (NRS) 287.250 et seq.

Article II: Legal and Procedural

2.1 – Federal Law

Nevada's Deferred Compensation Program plans are established under and intended to operate as a Section 457(b) plan, Section 401(a) plan, and 3121 FICA Alternative Plan under the Internal Revenue Code and related regulations and any amendments.

2.2 – State Law

The enabling statutes for the Plans are found in NRS 287.250 through 287.370.

2.3 – Committee Documents

The Committee shall maintain and periodically review all plan documents in accordance with Section 457(b), 401(a), and 3121 of the Internal Revenue Code to establish and operate the Plans. The NDC Executive Officer, Administrative Staff, or designee shall have the authority to implement any Committee approved changes to the adopted plan documents.

The Committee shall maintain and periodically review a Statement of Investment Policy to identify guidelines and procedures used by the Committee to review and evaluate the various investment options offered in the Program. The NDC Executive Officer,

Administrative Staff, or designee shall have the authority to implement any Committee approved changes to the adopted Investment Policy Statement.

This Administrative Manual is intended to outline other established policies and procedures of the Committee and Administrative Staff for Program administration.

2.4 – Committee Election Procedure
In accordance with NRS 287.330, the Committee at its first regularly scheduled quarterly meeting each year shall designate one of its members to serve as Chair and may also select one to serve as Vice-Chair of the Committee for a term of one year or until a successor has been designated.

2.5 – National Association of Government Defined Contribution Administrators (NAGDCA)
The Program will maintain membership and participation in the National Association of Government Defined Contribution Administrators (NAGDCA), including attendance at designated meetings, conferences, and training opportunities as appropriate and as funds are available.

Article III: Coordination of Audits

The Program will routinely have audits conducted. Audits will include an annual financial audit conducted by an independent third party and a Program compliance audit performed typically every three to five years but may be performed as often the Committee deems necessary for proper Plan governance. The Compliance Audit may be provided as a requirement of the Investment Consultant contract.

3.1 – Audit Objectives – Audits are performed for different purposes. Common audit objectives are:

a) To ensure compliance with federal and state laws, standards, rules and regulations.
b) To evaluate Program efficiency and effectiveness, including investment providers, fund managers, and payroll centers processes and procedures.
c) To attest to the validity of financial information, recordkeeping, and accounting.
d) To ensure appropriate management and internal control systems are in place.
    i. On January 2017 The NDC Administration developed and executed the following internal control per the Counsel provided by the State of Nevada's Internal Audits Division:
        a. Monthly, Staff receives a report that illustrates contributions submitted by each participating pay center in each Plan.
        b. Staff verifies a random sampling of confirmations directly with the pay center to ensure balancing for the month and document confirmations monthly.
        c. Should a discrepancy arise, the Executive Officer will address the discrepancy as soon as admiratively possible with all parties and document the resolution. Discrepancies will be managed in accordance

with the existing service guarantees within the contract and reflected in the contractor regular evaluation and/or reviewed with the Pay Center amending their processes to meet compliance.

3.2 – Audit Process – The audit process normally consists of the following elements:

a) Audit Assignment – The point at which it has been determined that an audit will be undertaken.
b) Initial Meeting – Staff meets with auditors and selected entities payroll and Human Resources administrative personnel to discuss audit process, scope of work, audit timeline, expected participation requirements, and audit objectives.
c) Field Work – The auditors' procedures for obtaining audit evidence and developing findings and recommendations. The type and extent of field work will vary according to the objectives of the audit. For example, field work may entail detailed Recordkeeper transaction-by-transaction review, payroll center(s) contribution review or may only consist of a review of the processes and procedures.
d) Closing – Auditors formally present findings to the NDC Executive Officer, Administrative Staff or designee.
e) Response – The opportunity for the NDC contracted Recordkeeper and payroll centers to respond to the auditor's findings and recommendations.
f) Follow-Up – Staff and auditors follow the progress toward resolution of any audit exceptions, significant deficiencies, or material weaknesses.

Staff and/or auditors will present a final report, including action steps for appropriate solutions or need to develop and maintain internal controls to resolve any noted significant deficiencies or material weaknesses, to the Committee.

Article IV: Records Retention

The NDC Administrative Staff will meet the requirements on the General Records Retention and Disposition Schedules (NRS 239.080). The most current version is available through the Records Management Program and at:
http://nsla.nevadaculture.org/dmdocuments/generalschedules.pdf

Article V: Committee Operation

5.1 – Meeting Schedule

The Committee will endeavor to meet at least quarterly, to review the status of investment offerings and conduct other business of the Program. The Committee may elect to engage, at their discretion, in an annual strategic planning meeting outside of the four regular quarterly meetings to discuss future governance changes, administration changes, and/or other communication/marketing administration for the upcoming year. Special meetings may be called by the Committee Chair or NDC Executive Officer, Administrative Staff, or designee as deemed necessary and reasonable, and should be budgeted accordingly. All

Program governance decisions are to be made in a open public meeting as established in and in accordance with NRS 241.

5.2 – Meeting Agenda

The meeting agenda will be drafted by the NDC Administrative Staff and circulated to the designated Committee Chair and to Committee members for input. The final agenda will be approved by the Committee Chair and posted by the NDC Administrative Staff in accordance with Nevada's Open Meeting Law (NRS 241.020(3)(a)), which requires that notice of a meeting be posted no later than 9:00 am on the third working day prior to the meeting.

5.3 – Committee Action

If a quorum (at least 3 members) is present at meetings, action can be taken by the Committee. Motions will be passed or voted down by a simple majority vote. The Committee Chair is eligible to vote on all motions. Committee members may participate at meetings via telephone, videoconference, or other appropriate electronic media approved by the Committee and shall be treated as present for the purpose of determining a quorum, voting on motions, and other lawful actions of the Committee. Meetings will be conducted in accordance with standard rules of order that the Committee may adopt from time to time.

5.4 – Meeting Record

Minutes shall be prepared by NDC Administrative Staff, formally approved by the NDC Committee, and maintained by NDC Administrative Staff pursuant to statutory guidelines (see NRS 241.035). Members of the public may request from the NDC Administrative Staff that their names be placed on the mailing or e-mail list for distribution of agendas. Documents provided to the Committee during meetings will be provided to members of the public upon request, as appropriate, or posted to the Program's website.

The Committee welcomes the participation of Plan participants and the public. There will be two comment periods allowing for three minutes of public comment with the first comment period allowing for public comment relative to items on the agenda for the meeting, and the second allowing for public comment on any item under the jurisdiction of the Committee.

5.5 – Budget Review and Approval

NDC Administrative Staff will meet with appropriate State of Nevada Department of Administration staff to develop a budget for submission to the Governor upon approval of the Department of Administration Director or designee, and the NDC Administrative Executive Officer will provide the Committee status updates of the Program budget during the quarterly meetings.

Article VI: Plan Administration

6.1 – Activity reports

The NDC Administrative Staff will provide quarterly activity reports to the Committee, including, but not limited to reports on the overall Plan activities and evaluations of the NDC

contracted Recordkeeper, making comparisons when appropriate concerning plan assets, enrollment analysis, program participation analysis, etc. NDC Administrative Staff will focus primarily on the administrative activities of the Program.

6.2 – Analysis of Investment Performance

An analysis of investment performance will be reviewed by the Committee at its quarterly meetings. The report prepared by the NDC contracted investment consultant (see definition in Article VII, Section 7.7) shall include investment option performance, in-depth economic market data, asset allocation, updates on the fund watch list, any recommendations from the NDC contracted investment consultant, and other information requested by the Committee or Executive Officer as necessary for proper monitoring.

6.3 – Quarterly Newsletter

The NDC Administrative Staff shall publish a quarterly newsletter for Participants. Newsletters shall be published as soon as administratively possible after the end of each quarter of the Calendar year.

6.4 – Fund Settlement Policy

If directed by the Committee, all fund settlement amounts will be calculated based on the effected fund(s), shareholders and timeframe of the settlement. Identified shareholders will receive settlement monies in accordance with their proportionate share based on their account balances at the time of the settlement. Shareholders due less than $10 will not receive payment, rather this amount will be returned back to the other eligible shareholders. If settlement amounts and calculations determine all shareholders are ineligible due to the $10 de minimis then the amounts will be used for Plan expenses.

6.5 – Administrative Account Management and Distribution of Unused Plan Revenue; if any

The Committee has the authority to create and maintain an administrative account in which the Plan's generated revenue used to administer the Program will be managed within. NDC Administrative Staff will continually monitor and manage the Administrative Account along with managing all accounts payable and accounts receivable activities as it pertains to agency budget and revenue management. At regular intervals throughout each calendar year, NDC Administrative Staff will reconcile and manage the amount of revenue generated by fees collected through the Program. In the event that excess revenue is generated by the Plan, the Committee may direct NDC Administrative Staff to credit the unused portion of Program revenue back to eligible participant accounts, or execute a "Fee Holiday" if deemed appropriate and directed by the Committee

6.6 – Review of Claims and Appeals; Process and Policy

Any claim or appeal to a decision or action of the Committee, Administrative Staff, or contractor of the State under the Plan, including Investment changes, Plan design changes, actions made or asserted by Administration Staff or any of the NDC contractor(s) must be filed in writing with the NDC Executive Officer or designee and shall include specific details, facts, reasons for dispute, and written proof of wrongdoing or damages (if applicable). The

NDC Executive Officer or designee is responsible for the initial review of any such claim or appeal and will attempt to determine or institute a suitable solution. The Executive Officer or designee may consult and/or involve the State Attorney General, the Department of Administration Director, and the appointed NDC Committee Chairperson for a solution of resolution or denial of a claim or appeal which may result in the claim and/or appeal being reviewed and discussed in an open meeting in accordance with the Nevada Open Meeting Law. The NDC Executive Officer or designee shall notify the claimant, and as applicable, the Participant of any action or decision that was determined within 90 days of the written claim or appeal being submitted to the NDC Executive Officer or designee in good order.

Article VII: Roles, Responsibilities and Duties

7.1 – Committee

The Committee is responsible to meet on a quarterly basis and conduct its business in accordance with the mission and primary goals as outlined in Article I of this document or established annually, along with the applicable state laws and federal requirements for the Plan. In order to discharge their fiduciary duties, members of the Committee are responsible for preparing for and participating in meetings of the Committee.

A fiduciary compliance checklist of duties and responsibilities that the Committee has governance over and responsibility for, or that they may delegate to the Executive Officer is established and provided in the Addendum Section of this Administrative Manual. The Committee shall self-evaluate the following categories of duties and responsibilities regularly:

I. General Fiduciary Responsibilities
II. Committee Structure
III. Plan & Committee Procedures
IV. Investment Management
V. Plan Administration and Compliance
VI. Plan Safeguards
VII. Communications

7.2 – NDC Administrative Staff

NDC Administrative Staff is responsible for the day-to-day administration of the Program under the direction of the State of Nevada Department of Administration Director. The Executive Officer or designee is responsible for the following:

a) Operations management, including but not limited to the day-to-day oversight; employer relations; budget oversight; employee management and oversight; and the oversight and management of participant customer service.
b) Administrative Staff management to include the following:
    i. Employee recruiting, hiring, evaluations, and termination per the established State of Nevada Department of Administration Human Resource Management guidelines and standards.

ii. Providing proper training opportunities to all employees when initially hired and refresher training as needed or mandated, either internally or externally.

c) Committee business management, including but not limited to preparation and organization of agendas and meeting materials.
d) Contractual management, including but not limited to Recordkeeping, Program Administration, investment management oversight, program compliance, and legislative management.
e) Handling all participant complaints or concerns at the Plan level to ensure resolution if possible. The Executive Officer will determine whether a participant Complaint should be brought in front of the Committee for review, discussion, and/or further and final action at one of their scheduled Committee meetings. The Executive Officer is charged with the responsibility to gather all data and facts pertinent to a participant complaint and work with the Program contractor(s) to achieve a suitable resolution that is in-line with the Program's adopted Plan Document, Administrative Manual, and State/Federal regulations and/or Codes.

The Executive Officer, under the direction and discretion of the State of Nevada Department of Administration, may employ administrative State of Nevada employees and/or contract with an independent employment company to employ a part-time or temporary administrative personnel to assist with meeting preparation, transcription of minutes, processing participant change forms, and other duties as assigned by the Executive Officer or requested by the Committee on an as needed basis.

7.3 – Executive Officer's Review Process

The State of Nevada Department of Administration Director will be responsible for conducting regular performance reviews of the Executive Officer. The Department of Administration Director may consult Committee members as to the performance of the Executive Officer and will also review and approve any potential compensation changes based on current level as well as legislative action as it relates to all State employees.

7.4 – Legal Counsel

The Attorney General's Office provides legal counsel to the Committee and NDC Administrative Staff. The Deputy Attorney General assigned to the Program is responsible for reviewing all contracts and other legal documents and to provide legal advice and assistance relating to the work of the Committee and Staff.

7.5 – Political Sub-Divisions

The Committee at its discretion may allow local government entities or qualifying political sub-divisions to join the Program. NDC Administrative Staff will work with legal counsel and the entity's designated representative to ensure the proper documentation is obtained to join the Program. NDC Administrative Staff will periodically meet with political sub-division representatives to ensure compliance with current federal and state rules and regulations, and the participating political subdivision is subject to and must conform with all financial

and compliance audit testing or sampling when selected by the Executive Officer or designee.

Eligible political sub-division representatives will submit a Program Certification which will include acknowledgement of the receipt of the following items:

a) Interlocal Agreement
b) Plan Document, including any amendments
c) Plan Summary
d) Investment Policy Statement
e) Administrative Manual
f) Remittance of contributions electronically
g) Remittance of employee termination data within (30) thirty days of an employee termination

The designated representative(s) (appointed approved representatives) will complete the necessary certification. NDC Administrative Staff will work with each of the political sub-division's designated representative(s) to ensure each entity has an understanding of the Program requirements and provide training as applicable.

NDC Administrative Staff will work with eligible governmental entities to ensure the following are being administered in accordance to Plan rules and regulations:

a) Per IRC Section 414(h), pick-up contributions for participants who contribute to Nevada PERS "employee paid" system are being excluded from participant contributions based on percentage of pay;
b) Data and money remittances must be sent electronically; and
c) Working with the NDC contracted Recordkeeper to ensure participants are not exceeding the Internal Revenue Code annual contribution limits.
d) Treas. Reg. Section 1.457-4(b)(1) **Annual Deferrals, Deferral Limitations, and Deferral agreements Under Eligible Plans** – adherence and compliance to the maximum deferral limitations, and 50+ Catch-Up and Special 457(b) Catch-Up Provision rules and guidelines.
e) Ensuring that all employees enrolling or being enrolled in the NDC Program(s) declare at least a single primary beneficiary associated with their account. Should the participant not make a beneficiary designation, the payment of the account shall be distributed according to provisions established and adopted within the Plan's current Plan Document specifically Article IX, Section 9.2(a)(b).

7.6 – Professional Advisors

The Committee shall contract with qualified advisors to discharge its fiduciary duty. Investment consultant(s) shall be contracted under the direction and management of the NDC Executive Officer and retained to ensure the Plan funds are invested effectively with proper risk controls. Committee members are not liable for investment decisions made by Plan members provided advisors are qualified and proper investment policies are in place, adhered to, and monitored.

7.7 – Recordkeeper(s)

The NDC Administrative Staff and the Plan's contracted Recordkeeper will work together, under the direction and oversight of the NDC Executive Officer, to ensure all contract parameters are being met, and the following are being administered in accordance with Plan rules and regulations:

f) To ensure compliance with IRC Section 457(b) and 414(v), excess deferrals must be distributed to the participant, with allocable net income, as soon as administratively practicable after the Plan, Recordkeeper, or designated payroll center determine that the amount is an excess deferral. The excess deferral amount is always taxed in the year it was contributed to the plan, and the earnings are taxed in the year distributed. Governmental plans report excess deferrals on Form 1099-R. Please note amounts of less than $1 will not be refunded or corrected.
g) Contribution Data and money remittances must be sent electronically.
h) Work with the eligible governmental entities to ensure participants are not exceeding the IRC annual contribution limits.

Article VIII: Code of Ethics

As Committee members appointed by the Governor of the State of Nevada and Program Administrative Staff appointed by and under the authority of the State of Nevada Department of Administration, as well as public employees of the State in most cases, members of the Committee and NDC Administrative Staff are subject to the provisions of the Nevada Ethics in Government Law in NRS 281A.010-281A.500, inclusive. Committee members and NDC Administrative Staff are encouraged to review the entire chapter and be especially familiar with the general requirements of the Code of Ethical Standards in NRS 281A.400, as well as Executive Order 2011-02 Establishing Ethics Requirements for Certain Public Officers and Employees, signed by the Governor January 3, 2011.

The keys to interpretation of the ethics statutes are reasonableness, objectivity, and disclosure. If any Committee members or NDC Administrative Staff members have questions concerning specific situations, they should feel free to consult with the Deputy Attorney General representing the Deferred Compensation Program. The following are excerpts from the Code of Ethical Standards which are most relevant to the business of the Deferred Compensation Committee.

NRS 281A.400 Subsection 1 provides that a public officer or employee shall not seek or accept any gift, service, favor, employment, engagement, emolument or economic opportunity which would tend improperly to influence a reasonable person in the public officer's or employee's position to depart from the faithful and impartial discharge of the public officer's or employee's public duties.

NRS 281A.400 Subsection 2 provides that a public officer or employee shall not use the public officer's or employee's position in government to secure or grant unwarranted

privileges, preferences, exemptions or advantages for the public officer or employee, any business entity in which the public officer or employee has a significant pecuniary interest, or any person to whom the public officer or employee has a commitment in a private capacity to the interests of that person.

NRS 281A.400 Subsection 5 provides that if a public officer or employee acquires, through the public officer's or employee's public duties or relationships, any information which by law or practice is not at the time available to people generally, the public officer or employee shall not use the information to further the pecuniary interests of the public officer or employee or any other person or business entity.

NRS 281A.400 Subsection 10 provides that a public officer or employee shall not seek other employment or contracts through the use of his official position.

Additional standards pertinent to the Committee are set forth in NRS 281A.420 Subsection 1. This subsection provides that a public officer or employee shall not approve, disapprove, vote, and abstain from voting or otherwise act upon a matter:

a) Regarding which the public officer or employee has accepted a gift or loan;
b) In which the public officer or employee has a pecuniary interest; or
c) Which would reasonably be affected by the public officer's or employee's commitment in a private capacity to the interest of others, without disclosing sufficient information concerning the gift, loan, interest or commitment to inform the public of the potential effect of the action or abstention upon the person who provided the gift or loan, upon the public officer's or employee's pecuniary interest, or upon the persons to whom the public officer or employee has a commitment in a private capacity. Such a disclosure must be made at the time the matter is considered. If the public officer or employee is a member of a body which makes decisions, the public officer or employee shall make the disclosure in public to the chair and other members of the body.

NRS 281A.420 Subsection 3 states: Except as otherwise provided in this section, in addition to the requirements of subsection 1, a public officer shall not vote upon or advocate the passage or failure of, but may otherwise participate in the consideration of, a matter with respect to which the independence of judgment of a reasonable person in the public officer's situation would be materially affected by:

a) The public officer's acceptance of a gift or loan;
b) The public officer's pecuniary interest; or
c) The public officer's commitment in a private capacity to the interests of others.

In interpreting and applying the provisions of subsection 3:

a) It must be presumed that the independence of judgment of a reasonable person in the public officer's situation would not be materially affected by the public officer's pecuniary interest or the public officer's commitment in a private capacity to the interests of others where the resulting benefit or detriment accruing to the public officer, or if the public officer has a commitment in a private capacity to the interests

of others, accruing to the other persons, is not greater than that accruing to any other member of the general business, profession, occupation or group that is affected by the matter. The presumption set forth in this paragraph does not affect the applicability of the requirements set forth in subsection 1 relating to the disclosure of the pecuniary interest or commitment in a private capacity to the interests of others.

b) The Commission must give appropriate weight and proper deference to the public policy of this State which favors the right of a public officer to perform the duties for which the public officer was elected or appointed and to vote or otherwise act upon a matter, provided the public officer has properly disclosed the public officer's acceptance of a gift or loan, the public officer's pecuniary interest or the public officer's commitment in a private capacity to the interests of others in the manner required by subsection 1. Because abstention by a public officer disrupts the normal course of representative government and deprives the public and the public officer's constituents of a voice in governmental affairs, the provisions of this section are intended to require abstention only in clear cases where the independence of judgment of a reasonable person in the public officer's situation would be materially affected by the public officer's acceptance of a gift or loan, the public officer's pecuniary interest or the public officer's commitment in a private capacity to the interests of others.

Article IX: Educational Travel and Conferences

The Committee and Executive Officer are charged with exercising fiduciary responsibility for the Program solely in the interest of the participants and their beneficiaries. As fiduciaries, they are expected to be capable of carrying out their duties and responsibilities. To accomplish this, subject to Committee and budgetary approval, Committee members and NDC Administrative Staff shall avail themselves of educational opportunities to secure adequate training to fulfill those responsibilities, including attendance at appropriate off-site meetings, events, or conferences.

Subject to budgetary limitations and authority, each Committee member and NDC Administrative Staff members shall have the opportunity to attend the NAGDCA Annual Conference, with all conference fees, airfare, lodging and any other reasonable expenses paid by the program. Committee members and NDC Administrative Staff members may attend other educational conferences to meet training needs subject to the availability of budgetary funds and subject to the NDC Program's established Travel Policy in Article X.

Article X: Travel Policy

All Committee members and NDC Administrative Staff travel will be in accordance with State Administrative Manual (SAM) 0200 and NRS 281.160. The following internal controls have been established by the Agency:

It is the responsibility of all NDC Committee members and Administrative Staff to know and adhere to State Administrative Manual (SAM) Chapter 0200. All Travel Related Claims and Expenditures must be in accordance with applicable laws, the State Administrative Manual (SAM), and policies and procedures of the NDC Administrative Manual. Travel expenditures are administered in compliance with (SAM 202.0 -0256.0). All NDC Committee members and Administrative Staff must obtain prior authorization to travel from the State of Nevada Department of Administration through the NDC Administrative Staff who will verify adequate budgetary authority. Prior authorization is accomplished by completing a Travel Request and Authorization form provided by NDC Administrative Staff no later than four (4) weeks prior to the first date of travel unless otherwise authorized by the Department of Administration Director or his designee. . The accompanying Travel Request and Authorization form must also clearly identify and separate out all business and personal travel times and costs under the parameters outlined in the travel policy adopted by the State of Nevada Department of Administration. The Travel Expense Reimbursement Claim form must clearly demonstrate that the costs borne by the State are not increased due to personal travel. The employee MUST bear any costs related to combining the State travel with personal travel. Per SAM 0210, all travel expenses of State of Nevada employees will be charged to the budget account specifically appropriated or authorized to provide for the employees' salary (if applicable) and /or Travel expenses.

The rate of reimbursement for lodging, meals, and incidentals must be compliant with the Federal government's GSA rate based on travel destination and SAM Section 200. The GSA rates can be found via the following link: http://www.gsa.gov/portal/category/104877

1. If the GSA website does not recognize the county/city that you will be traveling to, the rate defaults to the standard CONUS rates for lodging, meals, incidentals (M&IE).
2. The GSA hotel rates are maximum allowable rate in most circumstances. SAM 200 allows for adjustments when the conference rate exceeds the GSA rate. The State Department of Administration Budget Division must approve all exceptions to this rule or any projected expense over the established reimbursement rate in advance of the travel on an Out-Of-Budget Travel Request.
3. (Also refer to table below)

<u>Hours and Conditions for Claiming Meals are as follows:</u>

1. Per Diem for meals may be claimed when employees are required to be at least 50 miles (one way) from their duty station. Meal per diem timeframes are stipulated below:
    a. **Breakfast**: Employee or Committee member departs before 7:00am and/or returns after 9:00AM
    b. **Lunch**: Employee or Committee member departs before 11:30am and/or returns after 1:00PM
    c. **Dinner**: Employee or Committee member departs before 6:00PM and/or returns after 7:00PM

2. Per Diem reimbursements for meals are not allowed when meals are included in conference or registration fees.
3. Employees or Committee members may voluntarily claim amounts less than the established rates. When attending conferences or seminars, a copy of the agenda must be submitted with the Travel Expense Reimbursement Claim form in order for meals to be reimbursed.
4. Any special dietary needs that affect the application of these meal reimbursements policies for conference/seminars must be declared on the Travel Request Form prior to traveling.

Incidental Reimbursement is as follows:
Reimbursement for incidentals will occur only when travel consists of an overnight stay.

Mileage Reimbursement requests can be requested and paid as follows:
When an employee or Committee member uses his/her personal vehicle for the State's convenience, he/she can be reimbursed at the current standard mileage reimbursements rate declared by the State of Nevada. In the event that an employee or Committee member does not report to their duty station before going directly to a scheduled meeting, workshop, presentation, etc., the amount of mileage that is reimbursable is only the mileage over and above the employee or Committee member's normal commute total from their principal residence to their duty station.

Description	Receipts Required	Rates
Breakfast	No	Refer to GSA rate table & Hours and Conditions below
Lunch	No	Refer to GSA rate table & Hours and Conditions below
Dinner	No	Refer to GSA rate table & Hours and Conditions below
Lodging	Yes	Refer to GSA rate table
Incidentals - (Overnight Travel Only)	No	Refer to GSA rate table
Transportation (parking, taxi, subway/bus, etc.)	Yes	Reasonable cost with original receipt
Mileage (State's Convenience)- Based on Federal Income Tax Rate. (See Department of Administration's Policy Directive webpage for current mileage information)	No	Refer to the Policy Directives section of the Dept. of Admin., Budget Division website
Mileage (Employee's Convenience)- Based on Federal Income Tax Rate. (See Department of Administration's Policy Directive webpage for current mileage information)	No	Refer to the Policy Directives section of the Dept. of Admin., Budget Division website

All Travel Claims will be submitted to NDC Staff for processing, approval, and reimbursement. Efforts should be made to submit Travel Expense Reimbursement Claim ("Travel Claims") within 15 business days of travel, but no later than 30 days of travel unless prohibited by exceptional circumstance per SAM 0220.

Addendum A: Fiduciary Compliance Checklist

Fiduciary Compliance Checklist

I. General Fiduciary Responsibilities – Does the Committee:

- Act solely in the interest of plan participants and beneficiaries and with the exclusive purpose of providing a benefit to them
- Defray the reasonable costs of administration
- Act with the skill and diligence of a prudent person knowledgeable in the action being taken and in the best interest of the Program as a whole.
- Diversify plan investments
- Act in accordance with the established plan documents and look towards ERISA established standards as widely used practices within the industry; adopting policies if the Committee deems feasible.
- Avoid conflicts of interest and prohibited transactions

II. Committee Structure

- Are the Committee members aware of their fiduciary status
- Do Committee members participate in fiduciary training when appointed, and is annual ongoing fiduciary training provided by the contracted Investment consultant or designated investment management or compliance professional?
- Do Committee members participate in the Nevada Open Meeting Law (OML) and Nevada Boards and Commissions Training provided by the State of Nevada Attorney General's Office at time of appointment and reviewed or refreshed at least annually during tenure, and other annual training opportunities and support?
- Do Committee members meet and maintain the Committee requirements outlined in NRS 287.325 to carry out their fiduciary duties?
- Does the State of Nevada contract with or employ knowledgeable experts in Investment Management, Recordkeeping, and Plan Administration to ensure fiduciary compliance?
- Have all fiduciaries to the Plan been identified? Do all fiduciaries have control over the management or disposition of assets and/or Plan Design?
- Do the fiduciaries have discretionary authority over administration of the Plan?
- Does the Plan provide a platform for participants to receive investment advice for a fee (with intent that it be acted upon by choice and direction of the participants)
- Does the committee have a charter, if applicable?

III. Plan and Committee Procedures

- Has the Mission Statement of the Plan been established and reviewed at least annually, and are ongoing goals and objectives of the plan formally reviewed, discussed, amended (if needed), and documented on at least an annual basis?
- Are there formal policies and procedures established for the following:
  - Frequency of meetings (quarterly, etc.)
  - Monitoring of service providers and other professionals (E.g., frequency of vendor searches, contract management, contract evaluation, etc.).
  - Determining the prudency of investments
  - Determining the reasonableness of fees
  - Determining reasonableness of service contract terms and conditions
  - Appointing and/or replacing committee members
- Is there an Investment Policy Statement (IPS) established and adopted?
  - Is the IPS regularly consulted when making investment decisions?
  - Is the IPS regularly reviewed and updated as appropriate?
- Is there documentation of the minutes of each committee meeting?
- Does the Plan follow the State of Nevada's Records Retention requirements?

IV. Investment Management – Does the Committee engage in regular monitoring of the following:

- Investment Structure:
  - Is the investment structure appropriate for underlying participants?
  - Are the number of investment options appropriate?
  - Do the investment options span the risk return spectrum?
  - Can the participants understand the investment options?
  - Are there any voids in the current investment lineup?
- Qualified Default Investment Option (QDIA) (target date funds) Review:
  - Has a QDIA been adopted and ensure that an investment qualifying as a QDIA is appropriate as a single investment capable of meeting a worker's long-term retirement savings needs and the Plan's financial wellness goals and objectives
  - Review the Plans employee demographics of the Plan and the current allocation by age
  - Does the Committee regularly examine the asset allocation of the current QDIA to ensure it is appropriate for the generational employment demographic of the participating workforce of the Plan?
  - Regularly review the current QDIA versus comparable vehicles
- Conduct at least an annual IPS Review
- Engage in an Investment Fund Performance Analysis: (at least quarterly):
  - Review fund performance and risk measures vs. benchmarks and peer groups
  - Review plan level fund and contribution asset allocations

- Assess fund performance and attributes vs. Investment Policy Statement criteria
- Provide fund recommendations: Additions, Replacements, Watch List
- Conduct a Global Capital Market Review:
  - → Review of activity in domestic and foreign markets
  - → Review of returns for various domestic, foreign and fixed income asset classes to include observations and trends
- Conduct regular Fee Monitoring & Benchmarking (at least annually): versus plans in same industry and with similar number of participants and program demographics
  - → Review participant, record keeper/administrative and investment fees for transparency and competitiveness
  - → Are the fees deemed "reasonable"?
- Regularly review trends, developments, legal updates within the defined contribution environment as part of a compliance audit, review, or a provision of the Recordkeeping Services and/or Investment Consultant Contract(s).

V. Plan Administration and Compliance

- Are the plan documents and supporting documents (SPD, FICA Plan Doc, etc.):
  - Regularly reviewed to ensure compliance with its terms?
  - Regularly updated and amended to comply with legal and regulatory requirements?
  - Available for easy review by participants and/or beneficiaries?
- Are there written procedures in place for the following:
  - Preventing/correcting operational errors
  - Processing contributions timely
  - Monitoring various statutory limits
  - Conducting an annual financial audit
  - Processing and management of Plan loans
  - Processing and management of QDROs
  - Processing and management of Unforeseeable Emergency/Hardship distributions

VI. Plan Safeguards

- Although the Plan is NOT subject to ERISA Section 404(c), are the following safeguards considered or established if adopted:
  - Are participants provided with the following:
    - → The right to direct their own investments, if applicable
    - → Reasonable opportunity to provide investment direction to the record keeper on a timely basis
    - → A diversified range of investments to choose from
    - → Investment education
- Are plan expenses monitored and benchmarked against industry averages?

- Are vendors providing and updating 408(b)(2) disclosures
- Is a Qualified Default Investment Alternative ("QDIA") provided under the plan?
- Are QDIA notices distributed on a timely basis?
- Is a Fidelity bond required by the State of Nevada? If so, has it been purchased and regularly renewed?
- Is the plan covered by fiduciary liability insurance?
- Does the employer have cyber security insurance, and/or does it require it's contractors to maintain cyber security insurance?

VII. Communications

- Is there a written and adopted communication plan?
- Are participants provided with timely distribution of the following documents:
  - Summary Plan Document
  - Summary of Material Modifications
  - Annual Plan Report
- Are participants provided with all required notices on a timely basis (during the established on-boarding period and at least annually thereafter); including, but not limited to:
  - Enrollment materials
  - Quarterly benefit statements (Annual Benefits Statement for FICA Alternative Plan)
  - Annual and quarterly 404(a)(5) disclosures (if required)
  - 30-day notice for changes to investment fund lineup
  - Automatic contribution arrangement notice, (if applicable)
  - Blackout notices (if applicable)
  - Safe harbor notices (if applicable)
- Is the effectiveness of investment education materials being measured regularly?

Addendum B: Fee Policy Statement

NEVADA PUBLIC EMPLOYEES' DEFERRED COMPENSATION PROGRAM

FEE AND EXPENSE POLICY STATEMENT

STATE OF NEVADA

December 2020

Introduction and Purpose

The purpose of this Fee and Expense Policy Statement is to detail fees and expense-related procedures for the State of Nevada's 457(b) Deferred Compensation and 3121 FICA Alternative Programs. This document is reviewed at least annually by the Nevada Deferred Compensation ("NDC") Committee ("Committee") which serves as a Fiduciary to the Plans.

Participant Expenses

457 (b) Plan Administrative Fees: Effective January 1, 2020, a $10.25 administrative flat per-account charge ($41 per year) will be withdrawn quarterly for all participants with a total account balance of $1,000 or more, regardless of how they are invested. 457 (b) Plan Administrative Fees do not subsidize the 3121 FICA Alternative Plan.

3121 FICA Alternative Plan Administrative Fees: Effective January 1, 2020, a $0.55 administrative flat per-account charge ($2.20 per year) will be withdrawn quarterly for all participants. 3121 FICA Alternative Plan Administrative Fees do not subsidize the 457 (b) Plan.

Fund Management fees depend on the investment option chosen. NDC will strive to offer the lowest cost share classes of funds (on a NET basis). All revenue share, if applicable, is provided back to participants as appropriate. Please refer to the Contract Prospectus Summary for each individual fund fee information.

Payment of Excess Plan Expenses

State of Nevada is the Plans' Sponsor. All expenses incidental to the administration or protection of the Plans, and the management of the assets of the Plans, shall be paid from the assets of the Plans or by the Plan participants; unless the Plan Sponsor chooses to pay such expenses directly.

To the extent permitted by law, the Plans' Administrative Allowance Account ("Account") may be reimbursed from the Plans for any direct expenses properly and actually incurred in connection with the performance of services for the Plans.

Expenses may be paid or reimbursed from the Account only upon the review and approval of the Committee, or by such other appropriate fiduciary of the Plans.

Qualified Expenses

The expenses that may be paid from, or which may be reimbursed to the Plan Sponsor for its payment of, include, and are not limited to, the following:

(a) Ongoing Plan administrative expenses, such as record keeping, legal, auditing, annual reporting, claims processing and similar administrative expenses;

(b) Investment advisory, investment management, administrative investment or service fees and expenses;

(c) Costs incurred in preparing, printing and distributing plan-related documents and other Participant communication materials;

(d) Costs associated with benefit distributions and transactions;

(e) Expenses to provide investment assistance and education to Participants; and

(f) Costs for providing on-going education, including the costs of attending seminars and conferences, for members of the Committee, fiduciaries and staff with respect to the Plans as necessary or appropriate to assist in the discharge of their responsibilities to the Plans.

Participant Fees in Excess of Plans' Administration Service Provider Costs

The agreements entered into between the Plan Sponsor and Plan Administration Service Provider state that participants shall pay an explicit fee which shall be used to pay for various aspects of Plan Administration. This fee may exceed the amount retained by the Plan Administration Service Provider to pay for its services.

Fees collected in excess of those retained by the Plan Administration Service Provider and received by the Plan shall be held in an unallocated trust assets account maintained under the Plan, to be called the Administrative Allowance Account.

Thereafter funds accrued in this account shall be used exclusively for the benefit of Participants and their Beneficiaries, or to defray the reasonable expenses of administering and managing the Plan.

Allocation of Excess Plan Administration Fees

Excess revenue remaining in the Administrative Allowance Account may be allocated to Plan participants at the Committee's discretion. Such amounts shall be allocated to Plan participants based on their pro-rata share of Plan assets.

Amendment

This Fee Policy may be amended by a majority vote of the Committee at a properly noticed meeting called for that purpose.

On behalf of the Nevada Deferred Compensation Committee, this Fee and Expense Policy Statement is adopted by the Committee and effective on this date:

Signature: 

NDC Executive Officer

Name: Robert R. Boehmer

Date: 01/22/2024

Addendum C: Cybersecurity Policy Statement

NEVADA PUBLIC EMPLOYEES' DEFERRED COMPENSATION PROGRAM

CYBERSECURITY POLICY STATEMENT

January 2024

NEVADA PUBLIC EMPLOYEES' DEFERRED COMPENSATION PROGRAM

CYBERSECURITY POLICY STATEMENT

TABLE OF CONTENTS

I. Introduction and Purpose 1
II. Key Definitions..... 2
III. Tips for Keeping Accounts Safe and Secure 5
IV. Nevada Deferred Compensation Program Minimum Requirements..... 6
V. Recordkeeper Cybersecurity Policies and Procedures 7
VI. State of Nevada Cybersecurity Overview..... 15
VII. State of Nevada Cybersecurity Incident Response Overview..... 18
VIII Summary..... 22

I) Introduction and Purpose

Cybersecurity is defined as "measures taken to protect a computer, device or computer system (as on the internet) against unauthorized access or attack."[1]

For many individuals, their largest account is not their bank account but rather their retirement account. Accounts such as those within the State of Nevada Public Employees' Deferred Compensation Program ("NDC"). That is why it is critically important to protect these retirement accounts and their assets from outside threats.

The purpose of this Cybersecurity Policy is to define how NDC accounts are protected. It is important to note that Cybersecurity is a shared responsibility. Participating parties include:

- The Plans' recordkeeper – currently Voya Financial® ("Voya")
- The Plans' consultant – currently Hyas Group, LLC
- The Plans' audit firm – currently Casey Neilon
- The Plan Sponsor – State of Nevada
- Plan Fiduciaries – NDC Committee
- Key personnel – NDC executive director and staff
- Plan participants

This document provides an overview of the cybersecurity policies and procedures that currently apply to NDC.

It includes key cybersecurity definitions, an overview of recordkeeper cybersecurity requirements, an overview of the State of Nevada cybersecurity policy, and a review of what to do in the event of a cybersecurity incident.

The exhibits feature additional details regarding recordkeeper data security and a form to report a cybersecurity event.

The Committee and NDC Staff will review this document at least annually and update it as needed.

---

[1] https://www.merriam-webster.com/dictionary/cybersecurity

II) Key Definitions

Please note the same Plan definitions apply in this Cybersecurity Policy as are designated in the Plan Document for the State of Nevada Public Employees Deferred Compensation Program and in Nevada Revised Statutes (NRS) 287.250 et seq. Key definitions as related to cybersecurity are as follows:

"Account" means each separate account established and maintained for a Participant under the Plan, including, as applicable, each Before-Tax Deferral Account, Roth 457(b) Account, Rollover Account, Alternate Payee Account, and Beneficiary Account.

"Administrative Staff" refers to the appointed Executive Officer and any other administrative personnel under his or her authority or assigned to the Administration of the Plan under the authority of the State of Nevada Department of Administration Director.

"Affected Persons" means Client's and its Affiliate's former and current employees whose Personal Identifiable Information ("PII") may have been disclosed or compromised as a result of an Information Security Incident.

"**Affiliates**" means any entities that, now or in the future, control, are controlled by, or are under common control with Client. An entity will be deemed to control another entity if it has the power to direct or cause the direction of the management or policies of such entity, whether through ownership, voting securities, contract, or otherwise.

"Client" means the State of Nevada as the Plans' Sponsor. Client may be the entity, or an individual contact as designated by the Executive Officer.

"Committee" means the Deferred Compensation Committee of the State of Nevada as authorized under Nevada Revised Statute (NRS) 287.250 to 287.370. The Committee has all of the power and authority to formally take action and deliberate on Plan design and investment options on behalf of the Plan. The Committee may delegate administrative and managerial duties under this Plan to the appointed Executive Officer.

"Confidential Information" means (a) non-public information concerning the Disclosing Party; its affiliates; and their respective businesses, products, processes, and services, including technical, marketing, agent, customer, financial, personnel, and planning information; (b) PII; (c) trade secrets; and (d) any other information that is marked confidential or which, under the circumstances surrounding disclosure, the Non-Disclosing Party should know is treated as confidential by the Disclosing Party. Except with respect to PII, which will be treated as Confidential Information under all circumstances, Confidential Information will not include (a) information lawfully obtained or developed by the Non-Disclosing Party independently of the Disclosing Party's Confidential Information and without breach of any obligation of confidentiality; or (b) information that enters the public domain

without breach of any obligation of confidentiality. All Confidential Information will remain the property of the Disclosing Party.

"Employee" means any natural person or individual who receives compensation for services from the Employer, including (a) any elected or appointed officer or Employee of the Employer, (b) an officer or employee of an institution under management and control of Nevada System of Higher Education (NSHE), and (c) any employee who is included in a unit of employees covered by a negotiated bargaining agreement that specifically provides for participation in the Plan. An Employee shall not include an independent contractor, a consultant, or any other individual classified by the Employer as not eligible to participate in the Plan.

"Employer" means the State of Nevada and each Participating Employer, including but not limited to the Nevada System of Higher Education (NSHE), any authorized political subdivision of the State of Nevada, and any authorized agency or instrumentality of the State of Nevada.

"Executive Officer" means the State of Nevada Department of Administration division administrator for the Plan appointed pursuant to NRS 232.215. The Executive Officer serves as the primary contact and support for the Committee. As delegated by the Committee, the Executive Officer manages the day-to-day operation of the Plan and oversees and serves as the appointed certified contract manager of contracts and contractors of the Plan.

"Fraud" is a confirmed compromise of a participant's financial account by a fraudster using information within the fraudster's possession or control that results in wrongful financial or personal gain or illegal access to a financial account.

"Information Security Incident" means any breach of security or cybersecurity incident impacting Voya that has a reasonable likelihood of (a) resulting in the loss or unauthorized access, use or disclosure of Client PII; (b) materially affecting the normal operation of Voya; or (c) preventing Voya from complying with all of the privacy and security requirements set forth in this Agreement.

"Law" means all U.S. and non-U.S. laws, ordinances, rules, regulations, declarations, decrees, directives, legislative enactments and governmental authority orders and subpoenas.

"Participant" means an individual or Employee who is currently deferring Compensation, or who has previously deferred Compensation under the Plan by salary reduction and who has not received a distribution of his or her entire benefit under the Plan. Only individuals who perform services for the Employer as an Employee may defer Compensation under the Plan. This includes any Employee, former Employee, beneficiary, or alternate payee who is not deceased and who has an Account or Rollover Account under the Plan and as defined in Code Section 414(p)(8).

"Personal Identifiable Information (PII)" Personal Identifiable Information (PII) is a type of data that identifies the unique identity of an individual.

"Phishing" is a type of internet fraud that seeks to acquire a user's credentials by deception. It includes the theft of passwords, credit card numbers, bank account details, and other confidential information. Phishing messages usually take the form of fake notifications from banks, providers, e-pay systems, and other organizations. The phishing attempt will try to encourage a recipient, for one reason or another, to enter/update personal data. Common reasons given can include "suspicious login to the account," or "expiration of the password."

"Plan" means the Nevada Public Employees' Deferred Compensation Plan (NDC) and other participating jurisdictions, as the same may be amended from time to time.

"Recordkeeper" means a contracted third-party administrator that the Plan may contract with and delegates certain administrative authority to establish and securely keep track of Participant Accounts, including contributions, withdrawals, balances, transactions (e.g. fund transfers), and other activities authorized by the Committee and Administrative Staff.

"Security Breach" is a confirmed compromise of an information system within the authority or responsibility of the recordkeeper that results in: (a) the unauthorized acquisition, disclosure, modification, or use of unencrypted personal data, or encrypted personal data where the encryption key has also been compromised; and (b) a likely risk of identity theft or fraud against the data subject. A good faith but unauthorized or unintentional acquisition, disclosure, modification, or use of personal data by an employee or contractor of the recordkeeper or a party who has signed a confidentiality agreement with the recordkeeper does not constitute a Security Breach if the personal data is not subject to further unauthorized acquisition, disclosure, loss, modification, or use.

"Security Incident Response" Incident response is a planned approach to addressing and managing the reaction after a cyberattack or network security breach. The goal is to have clear procedures defined before an attack occurs to minimize damage, reduce disaster recovery time, and mitigate breach-related expenses.

III) Tips for Keeping Accounts Safe and Secure

The State of Nevada Public Employees' Deferred Compensation Program (NDC) and the Plans' contracted recordkeeper, Voya Financial®, recognize the importance of safeguarding participant accounts and personal information against the ongoing risk of fraud, cyber threats, and other unauthorized activity. Plan participants are their own first line of defense when it comes to protecting accounts and identity.

General password security

- Participants are strongly encouraged to use and regularly update a unique password for each website where they maintain an account.
- Participants should never use date of birth or Social Security numbers as their password.
- Participants should not allow social networking sites or web browsers to memorize passwords.
- Participants should not share their password or answers to security questions with anyone
- The strongest passwords are comprised of a chain of unrelated common words.

Fraudulent emails or phishing

- Participants should be suspicious of emails asking for confidential information and should never provide credentials.
- Participants should look out for red flags such as urgent requests, unknown email addresses, or discrepancies between actual and displayed hyperlinks.
- Participants should be aware that fraudulent emails can appear to come from a business that you are working with.
- Participants should always review the sender's name, email address, and URL to ensure they are from a legitimate source.
- Participants should know that any of NDC's contracted parties will never ask for personal information by email.

S.A.F.E. Guarantee

The Plans' recordkeeper, Voya, is committed to safeguarding participants' financial accounts and personal information from the risk of fraud, cyber threats, and unauthorized activity. As part of this effort, Voya has established the Voya S.A.F.E.® (Secure Accounts for Everyone) Guarantee.

If any assets are taken from workplace retirement plan accounts or Voya-administered Individual Retirement Accounts due to unauthorized activity and through no fault of the participant, Voya will restore the value of the account subject to satisfying a few key steps.

Voya believes that keeping participant accounts secure is a mutual responsibility.

IV) Nevada Deferred Compensation Program Minimum Requirements

NDC requires its recordkeeper to meet and maintain the following minimum requirements regarding cybersecurity:

- Multi-factor authentication
- Unique (non-SSN) login
- Minimum password length of eight characters
- End-to-end data encryption
- Off-site systems backups
- Annual data security audits (SOC-1)
- Annual penetration testing
- Commitment to 100% online account registration for NDC participants
- No personal information disclosure to unaffiliated third parties
- Provide complimentary third-party account monitoring services in the event of a breach

V) Recordkeeper Cybersecurity Policies and Procedures

Voya Financial® (Voya) currently serves as the contracted third-party administrator and meets the above requirements.

As recordkeeper, Voya establishes and securely keeps track of participant accounts, including contributions, withdrawals, balances, transactions (e.g. fund transfers), and other activities authorized by the Committee and administrative staff. The following information was provided by Voya as related to the safekeeping of participant data and accounts.

1. Data security

1.1. Security standards and controls

(a) Voya will establish and maintain:

(i) administrative, technical, and physical safeguards against the destruction, loss, or alteration of confidential information; and

(ii) appropriate security measures to protect confidential information, which measures meet or exceed the requirements of all applicable laws relating to personal information security.

(b) In addition, Voya will implement and maintain the following information security controls:

(i) privileged access rights will be restricted and controlled;

(ii) an inventory of assets relevant to the lifecycle of information will be maintained;

(iii) network security controls will include, at a minimum, firewall and intrusion prevention services;

(iv) detection, prevention, and recovery controls to protect against malware will be implemented;

(v) information about technical vulnerabilities of Voya's information systems will be obtained and evaluated in a timely fashion and appropriate measures taken to address the risk;

(vi) detailed event logs recording user activities, exceptions, faults, access attempts, operating system logs, and information security events will be produced, retained, and regularly reviewed as needed; and

(vii) development, testing, and operational environments will be separated to reduce the risks of unauthorized access or changes to the operational environment.

1.2. Information Security policies. Voya will implement and maintain written policies, standards, or procedures that address the following areas:

(a) information security;

(b) data governance and classification;

(c) access controls and identity management;
(d) asset management;
(e) business continuity and disaster recovery planning and resources;
(f) capacity and performance planning;
(g) systems operations and availability concerns;
(h) systems and network security;
(i) systems and application development, quality assurance, and change management;
(j) physical security and environmental controls;
(k) customer data privacy;
(l) patch management;
(m) maintenance, monitoring, and analysis of security audit logs;
(n) vendor and third party service provider management; and
(o) incident response, including clearly defined roles and decision making authority and a logging and monitoring framework to allow the isolation of an incident.

1.3. Subcontractors. Voya will implement and maintain policies and procedures to ensure the security of confidential information and related systems that are accessible to, or held by, third party service providers. Voya will not allow any third parties to access Voya's systems or store or process sensitive data, unless such third parties have entered into written contracts with Voya that require, at a minimum, the following:

(a) the use of encryption to protect sensitive PII in transit, and the use of encryption or other mitigating controls to protect sensitive PII at rest;
(b) prompt notice to be provided in the event of a cybersecurity incident;
(c) the ability of Voya or its agents to perform information security assessments; and
(d) representations and warranties concerning adequate information security.

1.4. Encryption standards, multifactor authentication, and protection of confidential information.

(a) Voya will implement and maintain cryptographic controls for the protection of confidential information, including the following:
    (i) use of an encryption standard equal to or better than the industry standards included in applicable National Institute for Standards and Technology Special Publications (or such higher encryption standard required by applicable Law) to protect confidential information at rest and in transit over untrusted networks;
    (ii) use of cryptographic techniques to provide evidence of the occurrence or nonoccurrence of an event or action;
    (iii) use of cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities, and resources; and

(iv) development and implementation of policies on the use, protection, and lifetime of cryptographic keys through their entire lifecycle.

(b) In addition to the controls described in clause (a) above, Voya will:

(i) implement multi-factor authentication for all remote access to Voya's networks;

(ii) ensure that no Client PII is (a) placed on unencrypted mobile media, CDs, DVDs, equipment, or laptops or (b) stored or transmitted outside the United States; and

(iii) ensure that media containing confidential information is protected against unauthorized access, misuse or corruption during transport.

1.5. Information Security roles and responsibilities. Voya will employ personnel adequate to manage Voya's information security risks and perform the core cybersecurity functions of identify, protect, detect, respond, and recover. Voya will designate a qualified employee to serve as its Chief Information Security Officer ("CISO") responsible for overseeing and implementing its information security program and enforcing its information security policies. Voya will define roles and responsibilities with respect to information security, including by identifying responsibilities for the protection of individual assets, for carrying out specific information security processes, and for information security risk management activities, including acceptance of residual risks. These responsibilities should be supplemented, where appropriate, with more detailed guidance for specific sites and information processing facilities.

1.6. Segregation of duties. Voya must segregate duties and areas of responsibility in order to reduce opportunities for unauthorized modification or misuse of Voya's assets and ensure that no single person can access, modify, or use assets without authorization or detection. Controls should be designed to separate the initiation of an event from its authorization. If segregation is not reasonably possible, other controls such as monitoring of activities, audit trails, and management supervision should be utilized. Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

1.7. Information Security awareness, education and training. Voya will provide regular information security education and training to all Voya personnel, as relevant for their job function. In addition, Voya will provide mandatory training to information security personnel and require key information security personnel to stay abreast of changing cybersecurity threats and countermeasures.

1.8. Vulnerability assessments. Voya will conduct monthly vulnerability assessments that meet the following criteria:

(a) all production servers and network devices must be scanned at least

monthly;

(b) all findings must be risk rated;

(c) all findings must be tracked based on risk; and

(d) tools used for scanning must have signatures updated at least monthly with the latest vulnerability. Voya will implement and maintain a formal process for tracking and resolving issues in a timely fashion.

1.9. Physical and environmental security. Voya will ensure that all sites are physically secure, including the following:

(a) sound perimeters with no gaps where a break-in could easily occur;

(b) exterior roof, walls, and flooring of solid construction and all external doors suitable protected against unauthorized access with control mechanisms such as locks, bars, alarms, etc.;

(c) all doors and windows to operational areas locked when unattended;

(d) equipment protected from power failures and other disruptions caused by failures in supporting utilities;

(e) closed-circuit television cameras at site entry/exit points; badge readings at all site entry points, or other means to prevent unauthorized access; and

(f) visitor sign-in/mandatory escort at site.

1.10. Information Security Incident notification

(a) In the event of any Information Security Incident, Voya will, at its sole expense: promptly (and in any event within 72 hours after Voya confirms an Information Security Incident) report such Information Security Incident to Client by sending an email to Client Contact Information, summarizing in reasonable detail the effect on Client, if known, and designating a single point of contact at Voya who will be

(i) available to Client for information and assistance related to the Information Security Incident; investigate such Information Security Incident, perform a root cause analysis, develop a corrective action plan, and take all necessary corrective actions;

(ii) mitigate, as expeditiously as possible, any harmful effect of such Information Security Incident and cooperate with Client in any reasonable and lawful efforts to prevent, mitigate, rectify, and remediate the effects of the Information Security Incident;

(iii) provide a written report to Client containing all information necessary for Client to determine compliance with all applicable laws, including the extent to which notification to affected persons or to government or regulatory authorities is required; and

(iv) cooperate with Client in providing any filings, communications, notices, press releases, or reports related to such Information Security Incident.

(b) In addition to the other indemnification obligations of Voya set forth in this Agreement, Voya will indemnify, defend and hold harmless Client from and

against any and all claims, suits, causes of action, liability, loss, costs and damages, including reasonable attorneys' fees, arising out of or relating to any Information Security Incident, which may include, without limitation:

(i) expenses incurred to provide notice to Affected Persons and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law;

(ii) expenses related to any reasonably anticipated and commercially recognized consumer data breach mitigation efforts, including, but not limited to, costs associated with the offering of credit monitoring or a similar identify theft protection or mitigation product for a period of at least twelve (12) months or such longer time as is required by applicable laws or any other similar protective measures designed to mitigate any damages to the Affected Persons; and

(iii) fines or penalties that Client pays to any governmental or regulatory authority under legal or regulatory order as a result of the Information Security Incident.

1.11. Risk assessments. Upon Client's request no more than once per year, Voya will complete an industry standard information security questionnaire and provide relevant Service Organization Control ("SOC") audit reports, when available. Voya's standard security requirements are set forth in Exhibit A. Voya represents and warrants that, as of the Effective Date, the statements in Exhibit A are true and correct in all material respects.

1.12. Penetration testing. If any Services to be provided by Voya include the hosting or support of one or more externally facing applications that can be used to access systems that store or process Client data, the terms of this Section will apply.

(a) At least once every 12 months during the Term and prior to any major changes being moved into production, Voya will conduct a Valid Penetration Test (as defined below) on each internet facing application described above. As used herein, a "Valid Penetration Test" means a series of tests performed by a team of certified professionals, which tests/mimic real-world attack scenarios on the information system under test and include, without limitation, the following:

(i) information-gathering steps and scanning for vulnerabilities;

(ii) manual testing of the system for logical flaws, configuration flaws, or programming flaws that impact the system's ability to ensure the confidentiality, integrity, or availability of Client's information assets;

(iii) system-compromise steps;

(iv) escalation-of-privilege steps; and

(v) assignment of a risk rating for each finding based on the level of potential risk exposure to Client's brand or information assets.

(vi) upon Client's request, Voya will provide to Client an executive summary of any material issues or vulnerabilities identified by the

most recent Valid Penetration Test along with the scope of systems tested. The report may be redacted to ensure confidentiality.

2. Privacy and PII

2.1. With respect to any PII, Voya will:

(a) comply with the Voya Privacy Notice at www.voya.com/privacy-notice;
(b) retain, use, process, and disclose all PII accessed, obtained, or produced by Voya only to perform its obligations under this Agreement and as specifically permitted by this Agreement, or as otherwise instructed by Client, and not for any other purpose;
(c) refrain from selling such PII or using such PII for any other purpose, including for its own commercial benefit;
(d) treat all PII as Confidential Information;
(e) comply with the provisions of this Agreement to return, store, or destroy the PII; and
(f) comply with all applicable Laws with respect to processing of PII.

Voya hereby certifies to Client that it understands the restrictions and obligations set forth above and will ensure that Voya and all Voya Personnel comply with the same.

2.2. As needed to comply with applicable Laws concerning the processing of PII or personal information security, or to the extent required by any changes in such Laws or the enactment of new Laws, the Parties agree to work cooperatively and in good faith to amend this Agreement in a mutually agreeable and timely manner, or to enter into further mutually agreeable agreements in an effort to comply with any such Laws applicable to the Parties. If the Parties cannot so agree, or if Voya cannot comply with the new or additional requirements, Client may terminate this Agreement upon written notice to Voya.

3. Confidential Information

3.1. Confidential Information. Either Party ("Disclosing Party") may disclose Confidential Information to the other Party (Non-Disclosing Party") in connection with this Agreement.

3.2. Use and disclosure of Confidential Information. The Non-Disclosing Party agrees that it will disclose the Disclosing Party's Confidential Information only to its employees, agents, consultants, and contractors who have a need to know and are bound by obligations of confidentiality no less restrictive than those contained in this Agreement. In addition, Voya agrees that it will use the Disclosing Party's Confidential Information only for the purposes of performing its obligations under

this Agreement. The Non-Disclosing Party will use all reasonable care in handling and securing the Disclosing Party's Confidential Information and will employ all security measures used for its own proprietary information of similar nature. These confidentiality obligations will not restrict any disclosure of Confidential Information required by Law or by order of a court, regulatory authority, or governmental agency; provided, that the Non-Disclosing Party will limit any such disclosure to the information actually required to be disclosed. Notwithstanding anything to the contrary, Client may fully comply with requests for information from regulators of Client and the Client Affiliates.

3.3. Treatment of Confidential Information following termination. Promptly following the termination or expiration of this Agreement, or earlier if requested by the Disclosing Party, the Non-Disclosing Party will return to the Disclosing Party any and all physical and electronic materials in the Non-Disclosing Party's possession or control containing the Disclosing Party's Confidential Information. The materials must be delivered via a secure method and upon such media as may be reasonably required by the Disclosing Party.

Alternatively, with the Disclosing Party's prior written consent, the Non-Disclosing Party may permanently destroy or delete the Disclosing Party's Confidential Information and, if requested, will promptly certify the destruction or deletion in writing to the Disclosing Party. Notwithstanding the foregoing, if the Non-Disclosing Party, due to requirements of applicable Law, must retain any of the Disclosing Party's Confidential Information, or is unable to permanently destroy or delete the Disclosing Party's Confidential Information as permitted above within 60 days after termination of this Agreement, the Non-Disclosing Party will so notify the Disclosing Party in writing, and the Parties will confirm any extended period needed for permanent destruction or deletion of the Disclosing Party's Confidential Information. All Confidential Information in the Non-Disclosing Party's possession or control will continue to be subject to the confidentiality provisions of this Agreement. The methods used to destroy and delete the Confidential Information must ensure that no Confidential Information remains readable and cannot be reconstructed so to be readable. Destruction and deletion must also comply with the following specific requirements:

Medium	**Destruction Method**
Hard copy	Shredding, pulverizing, burning, or other permanent destruction method
Electronic tangible media, such as disks and tapes	Destruction or erasure of the media

Hard drive or similar storage device	Storage frame metadata removal to hide the organizational structure that combines disks into usable volumes and physical destruction of the media with a Certificate of Destruction (COD)

3.4. Period of confidentiality. The restrictions on use, disclosure, and reproduction of Confidential Information set forth in this Section will, with respect to PII and Confidential Information that constitutes a "trade secret" (as that term is defined under applicable Law), be perpetual, and will, with respect to other Confidential Information, remain in full force and effect during the term of this Agreement and for three years following the termination or expiration of this Agreement.

3.5. Injunctive relief. The Parties agree that the breach, or threatened breach, of any of the confidentiality provisions of this Agreement may cause irreparable harm without adequate remedy at law. Upon any such breach or threatened breach, the Disclosing Party will be entitled to injunctive relief to prevent the Non-Disclosing Party from commencing or continuing any action constituting such breach, without having to post a bond or other security and without having to prove the inadequacy of other available remedies. Nothing in this Section will limit any other remedy available to either Party.

4. Cyber liability insurance. During the Term, Voya will, at its own cost and expense, obtain and maintain in full force and effect, with financially sound and reputable insurers, cyber liability insurance to cover Voya's obligations under this Addendum. Upon execution of the Agreement, Voya will provide Client with a certificate of insurance evidencing the following coverage and amount with such insurer:

Risk Covered: Network Security (a.k.a. Cyber/IT) Limits: $50,000,000

5. Disaster recovery and business continuity plan. Voya maintains, and will continue to maintain throughout the Term, (a) a written disaster recovery plan ("Disaster Recovery Plan"), which Disaster Recovery Plan is designed to maintain Client's access to services and prevent the unintended loss or destruction of Client data; and (b) a written business continuity plan ("BCP") that permits Voya to recover from a disaster and continue providing services to customers, including Client, within the recovery time objectives set forth in the BCP. Upon Client's reasonable request, Voya will provide Client with evidence of disaster recovery test date and result outcome.

VI) State of Nevada Cybersecurity Overview

In addition to recordkeeper cybersecurity policies noted, the State of Nevada has its own internal Information Security Policy. You may read the full Information Security Program Policy here.

The Nevada Information Security Program Policy defines a set of minimum-security requirements to protect state data and information technology (IT) systems that all state agencies within the Executive Branch of Nevada State Government must meet. This includes NDC.

Any state agency, based on the business needs and/or specific legal requirements, may exceed the security requirements put forth in this policy, but must, at a minimum, achieve the security levels required by this policy. The primary objective of Nevada Information Security Program Policy is to:

- effectively manage the risk of security exposure or compromise within state agency IT systems;
- communicate the responsibilities for the protection of state agency information;
- establish a secure processing base and a stable processing environment within state agencies and throughout the state;
- reduce to the extent possible the opportunity for errors to be entered into an IT system supporting state agency business processes;
- preserve management's options in the event of state data, information, or technology misuse, loss, or unauthorized access; and
- promote and increase the awareness of information security in all state agencies and with all state employees.

The following state and federal statutes require states to protect their information resources and data by establishing information security programs and imposing special requirements for protecting personal information.

- The Clinger-Cohen Act of 1996
- Federal Information Security Management Act of 2002
- Nevada Revised Statute (NRS) 242.101
- Nevada Revised Statute (NRS) 603A

State of Nevada Office of the Chief Information Officer (OCIO) has the statutory responsibility for establishing regulations and providing guidance to state agencies within the Executive Branch of Nevada State Government, for the protection of state information technology (IT) systems, and the data that those systems process, store, and transmit electronically. To support those responsibilities, OCIO established the Office of Information

Security (OIS) to develop appropriate security regulations and guidance, along with staff as subject matter experts to guide and assist state agencies in establishing agency security policies, standards, processes, and plans. [NRS 242.101]

To ensure the security concerns and needs of state agencies are included in the development of the State Information Security Program, a State Information Security Committee was established. This committee consists of representatives from state agencies with information technology backgrounds who have a vested interest in the development of the security policies, standards, and guidance.

As the State Information Security Program and the State Information Security Policy evolve, the policy will be subject to review and update, which will occur biennially, or when changes occur that signal the need to revise the State Information Security Policy. These changes may include the following:

- Changes in roles and responsibilities;
- Release of new executive, legislative, technical, or State guidance;
- Identification of changes in governing policies;
- Changes in vulnerabilities, risks, or threats; or
- Legislative Audit findings that stem from security audit.

The National Institute of Standards and Technology (NIST) Special Publications 800 Series documents and the NIST Cybersecurity Framework (CSF) provide continuing guidance for the ongoing development and revision of the security program policy. These publications focus on security requirements and best practices for the Federal government, which requires state compliance due to the state receiving federal funds for information systems, and the state agencies accessing, processing, storing, or transmitting federal data.

In 2019, NRS 603A was amended to identify the Center for Internet Security (CIS) Controls as a baseline security framework for the Executive Branch of Nevada State Government. In situations where neither the state nor the agency has established a policy or standard on a specific security control, the requirements of NIST 800-53 Security and Privacy Controls and 800-100 Information Security Handbook will be the de facto state standard.

This policy has been developed, revised, and approved by the State Information Security Committee and the State Chief Information Security Officer, and has received final approval by the State Chief Information Officer. Revisions to this document are subject to the review and approval of the State Information Security Committee and the State Chief Information Security Officer, with final approval of the State Chief Information Officer. When revisions are approved, a new version of the State Information Security Policy will be issued, and all affected state agencies will be informed of the changes.

Additionally, compliance with this policy is mandatory. It is the State Chief Information Officer's direction that all state agencies within the Executive Branch of Nevada State Government comply with the direction of this policy.

In cases where a state agency cannot comply with any section of the State Information Security Policy, justifications for the noncompliance must be documented using the Exception Request process provided in Appendix A of this document. The Exception Request must be submitted to OCIO, Office of Information Security, Chief Information Security Officer (CISO) for approval. Resulting risks from a deviation to policy must be documented in the appropriate Information Security Plan.

VII) State of Nevada Cybersecurity Incident Response Overview

The State of Nevada also maintains a policy for reporting and responding to information security incidents. The following section further explains the State of Nevada Incident Management Standards and provide details as to how the incident response is implemented. An incident response form is included in this Cybersecurity Policy as Exhibit B.

Document ID	Title	Revision	Effective Date	Pag
S.4.08.02	Information Security Incident Management	D	12/31/2020	1 of

1.0 PURPOSE

This standard establishes minimum requirements to ensure all information security incidents will be reported and responded to systematically, taking appropriate steps to minimize loss or theft of information, or disruption of services.

2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

- NRS 205.473 to 205.513, Unlawful Acts Regarding Computers and Information Systems
- NRS 242.181, Adherence by using agencies and elected officers of State to regulations; reporting of certain incidents
- NRS 281.195, Use of Computers State
- Information Security Program Policy, 100 Information Security Incident Report Form, S.4.08.02.1F

6.0 STANDARD

6.1 Information Security Incident Reporting

Any and all security incidents that may have, or have, affected, degraded, or violated either production systems; or Federal, State, or agency security policy, standards, or procedures shall be documented.

A. All information security incidents shall be documented by completing an Information Security Incident Report Form (S.4.08.02.1F) containing at a minimum:
   1. Description of incident
   2. Date and time
   3. Impact on the agency and/or IT resource
   4. Estimated financial impact
   5. Mitigation action taken
   6. Preventative Action Recommendations
   7. Name, title, and date of the person completing the report

B. All documented Information Security Incident Reports shall be provided to the Office of Information Security (OIS) within three (3) working days. If the incident is critical, as determined by the unit manager or designee, immediate notification of OIS must occur.

C. OIS shall review and maintain all Information Security Incident Reports and follow through with required actions or recommendations. Follow through actions must also be documented and attached to the original Information Security Incident Report.

D. OIS shall provide statistics on incidents to the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and State Information Security Committee at minimum quarterly.

6.2 Information Security Incident Response

A. When a security incident occurs, the initial incident response must follow these minimum response steps. There are two types of information security incidents, characterized incidents and uncharacterized incidents.
   1. When a **characterized** security incident occurs, the functional unit responsible for the affected systems will follow the unit's existing desk procedures to correct or mitigate the impact. If the incident or related outage exceeds two hours of production (six hours non-production system) downtime, the functional unit will create a report describing the root cause of the issue and the steps taken to resolve the incident, with submission to OIS who will track incidents and consolidate into the CIO and CISO report.
   2. When an **uncharacterized** security incident occurs, the functional unit will inform OIS after two hours of production (six hours non-production system) downtime and work to mitigate, isolate, identify the issue, and otherwise protect the forensic integrity of the situation while working to

resolve the incident. During this time the functional unit will take every care to preserve all available data for analysis and future investigation. Once the incident has been characterized the functional unit will submit a report to OIS.

B. If an incident remains uncharacterized for six hours the functional unit will submit a status report to OIS.

6.3 Cybersecurity Incident Response Team

At any time during an information security incident, characterized or uncharacterized, the CIO or CISO may create a Cybersecurity Incident Response Team (CSIRT).

C. The CISO shall coordinate the establishment of an incident response team, if necessary; identify the individuals who will participate in the incident response; and consult with the agency on whether technical resources available to the agency have the expertise required for the type of incident, or if external incident response resources are needed.
D. The function of this team is to ensure a systematic response to an incident, minimizing loss of information, minimizing disruption of services, and maximizing preservation of data, log files, and configuration information pertinent to the incident.
E. Post-incident actions include ensuring functional units update their desk procedures, configurations, and documentation as required to minimize future impacts of the same incident. The CSIRT Lead will follow-up with a finalized report to the CIO and CISO.

7.0 INCIDENT RESPONSE DEFINITIONS

Characterized Incident: An incident or event that is precisely defined and understood. Characterized incidents may have occurred previously. Documentation of characterized incidents should include corrective actions.

Uncharacterized Incident: An incident or event that is not understood. Un-characterized incidents have not occurred previously.

Information Security Incident: Any abnormal occurrence that negatively impacts the operation of state IT systems or information, or the ability of users to utilize state IT resources; and may include a loss of data confidentiality; disruption of data or system integrity; disruption or denial of availability; or a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Physical Security Incident: An occurrence which impacts or jeopardizes the controls in place to protect the physical structure or environment of a building,

office, vehicle, and all resources within; such as secure doors being propped open, vandalism, theft, suspicious vehicles located near the department's sensitive buildings, inappropriate location of IT equipment (i.e., lack of environmental or physical protection for the device), etc.

Administrative Security Incident: An occurrence to where administrative security controls are violated such as badges not being worn, sign in/out logs not completed, etc.

Desk Procedure: A set of documented steps to perform a specific function. An example is the set of actions required to update virus signature files on a desktop.

8.0 EXCEPTIONS

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

VIII) Summary

This Cybersecurity Policy Statement provided an overview of the policies and procedures that safeguard Nevada Deferred Compensation participant account data. With the increasing threats of cyberattacks, the Committee also receives training and information related to these policies on a regular basis.

This policy will be reviewed at least annually and updated as needed by the Committee and NDC staff.

Exhibit A: Voya Security Requirements

FC:	Foundation controls
FC-1:	Information asset management
FC-1.1	Voya implements and maintains an inventory list and assigns ownership for all computing assets including, but not limited to, hardware and software used in the accessing, storage, processing, or transmission of Client PII.
FC-1.2	Voya reviews and updates the inventory list of assets for correctness and completeness at least once every 12 months and updates the inventory list as changes are made to the computing assets.
FC-2:	Data privacy and confidentiality
FC-2.1	Voya will maintain an Information and Risk Management policy that is reviewed and approved by management at least every 2 years.
FC-2.2	Voya protects the privacy and confidentiality of all Client PII received, disclosed, created, or otherwise in Voya's possession by complying with the following requirements:
FC-2.2A	Such information is encrypted at rest on mobile devices (including mobile storage devices), portable computers, and in transit over untrusted networks with an encryption standard equal to or better than Advanced Encryption Standard (AES) 256 bit encryption or such higher encryption standard required by applicable law.
FC-2.2B	All hardcopy documents and removable media are physically protected from unauthorized disclosure by locking them in a lockable cabinet or safe when not in use and ensuring that appropriate shipping methods (tamper-proof packaging sent by special courier with signatures) are employed whenever the need to physically transport such documents and removable media arises.
FC-2.2C	All media is labeled and securely stored in accordance with Voya policies.
FC-2.2D	All electronic media is securely sanitized or destroyed when no longer required in accordance with industry standards.
FC-3:	Configuration management
FC-3.1	Voya implements and maintains accurate and complete configuration details (e.g., Infrastructure Build Standards) for all computing assets used in accessing, storing, processing, or transmitting Client PII.
FC-3.2	Voya reviews configuration details of the computing assets at least once every 12 months to validate that no unauthorized changes have been made to the assets.

FC-3.3	Voya updates the configuration details of all computing assets used to access, process, store, or transmit Client PII as configuration changes take place.
FC-4:	Operating procedures and responsibilities
FC-4.1	Voya implements and maintains operational procedures for information processing facilities and designates specific roles or personnel responsible for managing and maintaining the quality and security of such facilities, including, but not limited to, formal handover of activity, status updates, operational problems, escalation procedures, and reports on current responsibilities. Voya IT policies and standards document the policies and procedures for job scheduling processes and tools.
FC-4.2	Voya updates the operational procedures as changes take place and performs a comprehensive review and update of the procedures at least once every 2 years.
FC-5:	Security awareness and training
FC-5.1	Voya performs pre-employment background checks, including criminal history for 7 years, credit score and history (if applicable), credentials verification (if applicable), and educational background.
FC-5.2	Voya implements and maintains a documented security awareness program for all Voya Personnel which covers access to Client PII.
FC-5.3	Voya's security awareness program includes security requirements, acceptable use of computing assets, legal responsibilities, and business controls, as well as training in the correct use of information processing facilities and physical security controls.
FC-5.4	Voya ensures that all Voya Personnel complete security awareness training prior to being provided access to Client PII and at least annually thereafter. Voya provides mandatory annual training programs that include security awareness training to all Personnel.
UA:	**User access controls**
UA-1:	User access controls
UA-1.1	Voya implements and maintains identity management system(s) and authentication process(es) for all systems that access, process, store, or transmit Client PII.
UA-1.2	Voya ensures that the following user access controls are in place:
UA-1.2A	The "Least Privilege" concept is implemented ensuring no user has more privileges than they require in performing their assigned duties.
UA-1.2B	Users requiring elevated privileges as a normal part of their job responsibilities have a regular, non-privileged account to perform regular business functions.

UA-1.2C	All users have an individual account which cannot be shared.
UA-1.2D	Account Names/IDs are constructed not to reveal the privilege level of the account or position of the account holder.
UA-1.2E	System- or application-level service accounts are owned by a member of management or an IT system administration delegate and only have the privileges necessary to function as required by the application, system, or database the account has been created for.
UA-1.2F	Network access is disabled within 24 hours of termination. Automated processes disable access upon termination and initiate manager review on employee position changes, in accordance with Voya policies.
UA-2:	Access Control Management
UA-2.1	Voya maintains a comprehensive physical security program. Access to Voya facilities is restricted and logs are maintained for all access. Physical security and environmental controls are present in Voya buildings.
UA-2.2	Voya ensures that access to systems that access, process, store, or transmit Client PII is limited to only those personnel who have been specifically authorized to have access in accordance with the users' assigned job responsibilities.
UA-2.3	Voya ensures that accounts for systems that access, process, store, or transmit Client PII are controlled in the following manner:
UA-2.3A	Users must provide a unique ID and Password for access to systems. Access to applications/systems is limited to a need-to-know basis and is enforced through role-based access controls.
UA-2.3B	Accounts are protected on computing assets by screen-savers that are configured with an inactivity time-out of not more than 15 minutes.
UA-2.3C	Accounts are locked after no more than 10 consecutive failed logon attempts, depending upon the system and platform.
UA-2.3D	Accounts remain locked until unlocked by an Administrator or through an approved and secure end-user self-service process.
UA-2.3E	Accounts are reviewed on a periodic and regular basis (semi-annually for non-privileged and privileged accounts) to ensure that the account is still required, access is appropriate, and the account is assigned to the appropriate user.
UA2.4	Voya ensures that wireless mobile devices are secured against threats coming from these wireless networks and wireless connections are required to be encrypted.

UA-3:	User access management
UA-3.1	Voya ensures that passwords for all accounts on systems that access, process, store, or transmit Client PII are configured and managed in accordance with industry standards:
UA-4:	Information access restriction
UA-4.1	Voya implements information access restrictions on all systems used to access, process, store, or transmit Client Information.
UA-4.2	Voya ensures the following Information Access Restrictions are in place:
UA-4.2A	Access to underlying operating systems and application features that the user does not require access to in the performance of their assigned responsibilities are strictly controlled.
UA-4.2B	Access to source code and libraries are restricted to only those individuals who have been specifically approved to have access. A person who develops code changes cannot be the same person who migrates the code change into production.
UA-4.2C	Access between Development, Test, and Production environments are strictly controlled. The version management system provides segregation of code, data, and environments.
UA-4.2D	Temporary privileged access to production data is granted to authorized personnel based on job function for emergency support and only via access control and logging security tools.
PS:	**Platform security controls**
PS-1:	Computer System Security (Servers and Multi-user Systems only)
PS-1.1	Voya implements and manages a formal process for ensuring that all computer systems that access, process, store, or transmit Client PII are protected and configured as follows prior to and while remaining in a production status:
PS-1.1A	Systems are assigned to an asset owner within Voya's organization.
PS-1.1B	Systems are located in a data center or similarly controlled environment with appropriate physical security mechanisms and environmental controls to ensure systems are protected from theft, vandalism, unplanned outages, or other intentional or unintentional hazards.
PS-1.1C	All systems are configured to meet Voya standards, monitored to ensure a compliant state and patched as required to maintain a high degree of security. Issues found to be out of compliance are required to be tracked to closure.

PS-1.1D	Systems are configured with commercially available and licensed anti-virus software, which is set to perform active scans, perform scans of uploaded or downloaded data/files/web content, and is updated on at least on a daily basis.
PS-1.1E	System clocks are configured to synchronize with a reputable time source (e.g., NTP).
PS-1.1F	Systems display a warning banner to all individuals during the logon process that indicates only authorized users may access the system.
PS-1.1G	Systems that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.
PS-1.1H	All high and medium vulnerability and risk issues identified are remediated utilizing a risk-based approach and in alignment with application team code release schedules.
PS-1.1I	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor systems.
PS-2: Network security	
PS-2.1	To ensure systems accessing, processing, storing, or transmitting Client PII are protected from network related threats, Voya implements the following network security controls prior to connecting any network component to a production network and for the duration that the component remains in a production status.
PS-2.1A	Networks are constructed using a defense-in-depth architecture, are terminated at a firewall where there are connections to external networks and are routinely scanned for unapproved nodes and networks.
PS-2.1B	Business-to-Business (B2B) and Third-Party network connections (Trusted) to systems accessing, processing, storing, or transmitting Client PII are permitted only after a rigorous risk assessment and formal approval by Voya management. Network connections from un-trusted sources to internal resources are not permitted at any time.
PS-2.1C	Network components (switches, routers, load balancers, etc.) are located in a data center or a secure area or facility.
PS-2.1D	Voya systems are configured to provide only essential capabilities and restrict the use of any unneeded functions, ports, protocols, and services.
PS-2.1E	Intrusion detection/prevention technologies, firewalls, and proxy technologies are implemented, monitored, and managed to ensure only authorized and approved traffic is allowed within and between segments of the network.

PS-2.1F	Internal Voya wireless networks are configured with the most robust security standards available, including but not limited to, 802.11i/n, strong authentication, IP/MAC address filtering, firewall protection, and intrusion detection/prevention.
PS-2.1G	Wireless networks are not used to access Client Information unless the information is encrypted at either the file or transport level.
PS-2.1H	Network components that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.
PS-2.1I	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor network components.
PS-3: Generic application and database security	
PS-3.1	Voya implements and maintains an application security certification and assurance process that ensures that all applications that access, process, store, or transmit Client PII provide the following:
PS-3.1A	Application and database design ensures security, accuracy, completeness, timeliness, and authentication/authorization of inputs, processing, and outputs.
PS-3.1B	All data inputs are validated for invalid characters, out of range values, invalid command sequences, exceeding data limits, etc. prior to being accepted for production. Voya implements static source code analysis tools to validate data inputs.
PS-3.1C	Application source code developed in house by Voya is protected through the use of a source code repository that ensures version and access control. The version management system provides segregation of code, data, and environments.
PS-3.1D	Applications and databases are tested for security robustness and corrective measures are applied prior to the application being placed into a production environment. All systems are configured to meet Voya standards, monitored to ensure compliance state and patched as required to maintain a high degree of security.
PS-3.1E	Applications and databases are implemented into a production environment with minimal privileges and critical configuration files and storage subsystems are protected from unauthorized access.
PS-3.1F	Applications and databases that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.

PS-3.1G	Voya ensures that Consumer/Internet facing applications have been designed and implemented using multi-factor authentication architecture. Web sessions require the use of an HTTPS (encrypted) connection, as well as authorization to approved data and services.
PS-3.1H	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor applications and databases.
PS-4: Workstation and mobile devices security (end user devices)	
PS-4.1	Voya ensures that the following security controls have been implemented and are maintained to protect Client PII accessed, processed, stored, or transmitted on workstations and mobile devices.
PS-4.1A	Workstations are located in a physically secure environment with mechanisms in place to prevent unauthorized personnel from accessing data stored on the device, reconfiguring the BIOS or system components, or from booting the device from unauthorized media. Portable devices are configured for boot-up encryption.
PS-4.1B	Laptops/portable computers and other mobile devices are assigned to an owner who is responsible for physically securing the device at all times, and the owner of the device must receive adequate awareness training on mobile device physical security.
PS-4.1C	Portable devices are configured for boot-up encryption. All laptop hard drives are encrypted using AES 256. Any device deemed "remote" requires hard drive encryption.
PS-4.1D	All workstations, laptops/portable computers and other mobile devices (where applicable) are configured with commercially available and licensed anti-virus software, which is set to perform active scans, to perform scans of uploaded or downloaded data/files/web content, and is updated on at least a daily basis.
PS-4.1E	All workstations, laptops/portable computers and other mobile devices (where applicable) are configured with a commercially available and licensed operating system, patched according to manufacturer's recommendations, hardened according to best industry practices and standards and configured so that regular users do not have administrative privileges.
PS-4.1F	Laptops/portable computers and other mobile devices (where applicable) are configured with personal firewall technology.
PS-4.1G	Workstations, laptops/portable computers and other mobile devices (where applicable) display a warning banner to all individuals during the logon process that indicates that only authorized users may access the system or device.
PS-4.1H	Voya implements and maintains processes for recovering laptops/portable computers and mobile devices from terminated Voya Personnel.

PS-5: Backup and restore	
PS-5.1	Voya implements and maintains backup and restore procedures to ensure that all Client PII received, disclosed, created, or otherwise in the possession of Voya is appropriately protected against loss.
PS-5.2	Voya ensures that backups are securely stored and storage systems are physically and logically protected.
PS-5.3	Voya implements a backup and availability schedule to meet business and regulatory requirements.
PS-6: Remote network access controls	
PS-6.1	Voya implements and maintains a remote network access control strategy or process.
PS-6.2	Voya ensures the following remote network access controls are in place:
PS-6.2A	Users requiring remote access are appropriately authorized by Voya management.
PS-6.2B	Remote access connections are established through the use of Virtual Private Networking (VPN) or secure VDI mechanisms that provide transmission security, encryption, and connection timeout (e.g., split-tunneling disabled).
PS-6.2C	Only Voya approved and controlled (managed) computing devices are used when remotely accessing (where applicable) Voya's computing environments where Client PII is held. Any device deemed "remote" requires data encryption. Encrypted communications are required for all remote connections.
PS-6.2D	Users are thoroughly authenticated using multi-factor authentication prior to being provided remote access.
ITR: IT resilience controls	
ITR-1: Architecture	
ITR-1.1	Voya ensures that the architecture of computing environments where Client PII is accessed, processed, stored, or transmitted incorporates reasonable industry best practices for authentication/authorization, monitoring/management, network design, connectivity design, firewall and intrusion prevention technologies, and storage and backup capabilities.
ITR-2: Hardware and software infrastructure resilience	
ITR-2.1	Voya ensures all hardware and software components classified with an availability rating of "critical" used in the accessing, processing, storage, or transmission of Client PII is: • Identified and cataloged • Supported by the manufacturer of the component (or if developed in-house, follows Voya's SDLC Policy which includes quality/security)

	• Applications and systems classified as A4 may be designed with high availability features and have no single point of failure • Reviewed on a regular basis for capacity implications (at minimum once every 12months)
ITR-2.2	Voya maintains Business Continuity Plans to address business unit and departmental actions to be undertaken before, during and after an incident or disaster. Voya's Disaster Recovery Plan addresses the recovery and availability of systems and data.
ITR-3: Capacity assurance	
ITR-3.1	Voya ensures that computing environments used to access, process, store, or transmit Client PII are assessed for capacity and performance on a periodic basis (at minimum once every 12 months) and appropriate corrective actions are taken to make the environment sufficiently robust enough to perform its stated mission.
CM: Change management controls	
CM-1: Change management process	
CM-1.1	Voya implements and maintains a change control process to ensure that all changes to the environment where Client PII is accessed, processed, stored, or transmitted is strictly documented, assessed for impact, and approved by personnel authorized by Voya to provide approval for such changes, thoroughly tested, accepted by management, and tracked.
CM-1.2	Voya implements an emergency change control process to manage changes required in an emergency situation where a computing system is down or there are imminent threats/risks to critical systems involving Client PII.
CM-2: Separation of environments	
CM-2.1	Voya maintains physically and/or logically separate development, test, and production computing environments. Development, testing, and acceptance environments are separate from the production environment.
CM-2.2	Voya ensures that Client data used for development or testing purposes is completely depersonalized/desensitized of confidential values prior to entering a development or test environment. Data is depersonalized in non-production-controlled environments for testing purposes with required approvals. PII elements are required to be depersonalized in non-production environments.
SM: Security monitoring controls	
SM-1: Security event monitoring and incident management	
SM-1.1	Voya implements and maintains a security event monitoring process and associated mechanisms to ensure events on computing systems, networks, and applications that can impact the security level of that asset or the data residing

	therein are detected in as close to real-time as possible for those assets used to access, process, store, or transmit Client PII.
SM-1.2	Voya implements and maintains an incident management process to ensure that all events with a potential security impact are identified, investigated, contained, remediated, and reported to Client effectively and in a timely manner.
SM-1.3	Voya has implemented monitoring controls that provide real-time notifications of events related to loss of confidentiality, the integrity, or the availability of systems.
SM-1.4	Event logs (audit trails) are stored for analysis purposes for a minimum period of 3 years.
SM-2: Technical state compliance	
SM-2.1	Voya ensures computing environments that access, process, store, or transmit Client PII are continually in compliance with quality and security requirements including, but not limited to, authentication/authorization, monitoring/management, network design, connectivity design, firewall and intrusion prevention technologies, and storage and backup capabilities.
SM-2.2	Voya ensures IT Risk Management facilitates risk assessments of information technology processes and procedures in accordance with the annual IT Risk Assessment Plan approved by the IT/Privacy Risk Committee. Risk Assessment results are communicated to management for awareness and resolution or risk acceptance of findings based on management's risk appetite.
SM-3: Security and penetration testing	
SM-3.1	Voya implements and maintains vulnerability and penetration testing (Ethical Hacking) processes to ensure the computing environment where Client PII is accessed, processed, stored, or transmitted is continually protected from internal and external security threats.
SM-3.2	Voya implements and maintains a process for vulnerability scanning on at least a monthly basis and ensures issues are remediated, utilizing a risk based approach within a reasonable timeframe.
SM-3.3	Penetration testing (Ethical Hacking) of Internet facing systems or systems exposed to un- trusted networks is conducted prior to the system being deployed into a production status, after any significant changes, and then at least once every 12 months thereafter.

1111551_1221 © 2021 Voya Services Company. All rights reserved. CN1966532 _1223

Exhibit B

State of Nevada Security Incident Report Form

State of Nevada

Information Security Committee

INFORMATION SECURITY INCIDENT REPORT

SECTION 1	
Type of Incident:	
Start Date/Time:	**Ending Date/Time:**
Description of Incident:**	

SECTION 2
Impact/Damage Sustained:**
Estimate of Financial Impact:**
Mitigation Action Taken:**

SECTION 3 (Office of Information Security Use Only)
Corrective Action Taken:**
Additional Preventative Action Recommended:**

Reporter:	**Title:**	**Date:**
Previous Reports on this Incident Dated:		

*** Expand on additional paper as necessary*